RÉPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTÉRE DE L'ENSEIGEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

Mémoire
De fin d'études

En vue de l'obtention du Diplôme de Master Deux en Informatique

Option : ***Système Informatique***

Promotion: 2011/2012

Thème

Protection de la vie privée dans les réseaux sociaux

Proposé par:

M^R **Ouamrane**

Réalisé par :

M^elle **CHEBBAH SONIA**

M^elle **BOUBRIT ZOHRA**

Remerciements

En préambule à ce mémoire, on souhaitait adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette année universitaire.

On tient à remercier sincèrement Monsieur OUAMRANE, qui, en tant que promoteur, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'il a bien voulu nous consacrer et sans qui ce mémoire n'aurait jamais vu le jour.

Nos remerciements s'adressent également à Madame AIT ADDA, Madame AOUDJIT pour leurs générosités et la grande patience dont elles ont su faire preuve malgré ses charges académiques et professionnelles.

Enfin, on adresse nos plus sincères remerciements à tous nos proches et amis qui nous ont toujours soutenue et encouragée au cours de la réalisation de ce mémoire.

Je dédie ce mémoire de fin d’études

A Mon très cher ***père*** et ma très chère ***mère*** en témoignage de ma reconnaissance envers leur soutien, les sacrifies et tous les efforts qu’ils ont fait pour mon éducation ainsi que pour mes études ;

A mes deux chers frères ***MOULOUD*** et ***YACINE*** à qui je souhaite tout le bonheur et réussite ;

Aux deux personnes que j'aurais tant aimé qu'elles assistent à ma soutenance : ***ma grand-mère*** ainsi que ***mon grand-père*** paix à leur âme ;

A mes ***tentes*** et ***oncles*** ainsi que leur ***enfants*** ;

A tous ceux qui ont une relation de proche ou de loin avec la réalisation du présent rapport ;

ET à mon ami et binôme ***SONIA***.

Je dédie ce mémoire à toute ma famille, ma mère, mon père mes sœur kamelia et Sabrina, ma belle famille surtout á mon fiancé amine.

Je le dédie aussi à la mémoire de mon beau père Hocine, aussi a mes grand parents Saliha et Ali.

Je le dédie aussi à tous mes oncles et tantes, cousins et cousines.
Je ne saurai terminer sans citer mes amis.

Enfin je le dédie à tous ceux qui me connaissent, qui m'ont aidé à réaliser ce mémoire.

Qu'ils trouvent à travers ce travail ma sincère reconnaissance.

A Zola ma binôme.

Table des matières

Chapitre 2 : Sécurité Informatique

Chapitre 3 : Sécurité dans les réseaux sociaux

Chapitre 4 : Analyse et conception

Chapitre 5 : Outils de développement et Réalisation

Liste des figures

Chapitre 1 : Etat de l'art sur les réseaux sociaux

Chapitre 2 : Sécurité Informatique

Chapitre 3 : Sécurité dans les réseaux sociaux

Chapitre 4 : Analyse et conception

Chapitre 5 : Outils de développement et Réalisation

Liste des tableaux

Liste des algorithmes

Chapitre 5 : Outils de développement et Réalisation

Introduction Générale

Les sites de réseau social font partie du quotidien de bien des individus répartis un peu partout dans le monde. Sur ces sites, les utilisateurs dévoilent, comme bon leur semble, des informations relatives à leur vie privée. Le phénomène est certes fort intéressant, mais parallèlement à l'engouement qu'il suscite, il soulève des inquiétudes en matière de sécurité et de vie privée.

Ces sites de réseaux sociaux s'inscrivent dans ce qui est communément qualifié de Web 2.0. Cette appellation sert à désigner des outils qui permettent à l'internaute de mettre en ligne des données (vidéos, musiques, textes, images), de dialoguer avec d'autres internautes et de donner son opinion sur divers sujets.

La protection des renseignements personnels et de la vie privée suscitent des inquiétudes à l'heure ou la circulation de l'information peut se faire en un clic des souris. On craint pour la sécurité des personnes et le respect de leur vie privée, voire de leur liberté. Des informations peuvent être recueillies à des fins malveillantes. Dés que l'information est lancée sur Internet, il devient difficile d'en garder le contrôle.

Plusieurs sites très populaires présentent de nombreux défauts de sécurisation. Dans ce document nous nous sommes penchés sur la sécurité et protection de la vie privée dans les deux plus grands leaders des réseaux sociaux qui sont : ***Facebook*** et ***Twitter*** .

En jouant sur la corde curieuse et voyeuriste des habitants d'un campus, ***Facebook*** a réussi à se rendre additif et à récupérer les informations personnelles de tout le monde.

En misant sur la simplicité et la diffusion publique, ***Twitter*** a réussi à être indispensable pour ceux qui veulent aller vite ou qui souhaitent être transparents.

Les informations que nous donnons à ces deux réseaux constituent maintenant, avec la position dominante qu'ils occupent, l'alpha et l'oméga des réseaux sociaux. A ***Facebook***, nous donnons notre âge, nos amis, notre famille, nos intérêts, nos photos. A ***Twitter*** ce que l'on partage, publie, les personnes que l'on aime suivre sans être leur ami.

Et aux deux: notre position géographique.

Néanmoins, l'un des défauts les plus importants de ces deux dernier, est de ne proposer aucune authentification, qui crypte les données transmises au site. L'étude note toutefois que ces deux sites se rattrapent sur le surf qui est quant à lui sécurisé (mais activable de manière manuelle, c'est-à-dire en utilisant le protocole https).

Cependant, un nouveau genre de réseau social est apparu dans le but de remédier à failles existantes dans ses concurrents. Ce sont les ***réseaux sociaux décentralisés***.

Ces derniers, ont pour politique que chaque membre du réseau est à la fois client et serveur, et ceci dans le but de permettre aux internautes de garder le contrôle sur leurs données en gardant ces dernières locales sur leur propre poste. Mais cette méthode présente plus d'inconvénients que d'avantages, et cela en termes de cout et de gestion de sécurité.

Pour remédier aux failles de chaque réseau, la solution proposée sera basée sur le principe de ***cryptographie***, qui utilisera un algorithme de cryptage afin de permettre la circulation des données au sein des diverses réseaux sociaux d' une manière plus sécurisée, par conséquent une meilleure protection de la vie privée.

Tout d' abord, dans ce document, vous sera présenté des définitions de base sur les réseaux sociaux, afin de mieux comprendre leur fonctionnement.

Par la suite, nous avons étudié les différents aspects de la sécurité informatique, et les diverses moyens de protection existantes, en particulier, la ***cryptographie***.

Aussi, nous avons étudié trois différents réseaux sociaux qui sont : ***Facebook***, ***Twitter*** et les ***réseaux sociaux décentralisés***. Et cela en nous basant sur la protection de la vie privée au sein de ces derniers.

Enfin, dans les deux derniers chapitres, nous avons proposé une solution afin d' optimiser la protection de la vie privée, en utilisant de la cryptographie, et ceci, en proposant une application, qui vous sera illustrée et expliquer.

Les principales questions posées sont :

- ***Comment gérez-vous votre cyber identité ?***
- ***Quelle importance accordez-vous à votre e-réputation ?***
- ***Evitez-vous les réseaux sociaux ?***
- ***Utilisez-vous des pseudonymes ?***
- ***Ou au contraire, laissez-vous vos informations personnelles à la portée de tous ?***
- ***Acceptez-vous que des inconnus accèdent à vos pages ?***
- ***Comment va-t-on faire pour protéger des données personnelles sur des sites de réseaux sociaux ?***

Chapitre 1

Etat de l'art sur les réseaux sociaux

Chapitre 1 Etat de l'art sur les réseaux sociaux

Depuis quelques années, et plus précisément depuis 2005, le web que nous connaissions, celui du html et des sites personnels, subit de fortes mutations tant au niveau technologique que fonctionnel. Cette métamorphose a un nom : le Web 2.0 (Le terme a été inventé par Dale Dougherty de la société O'Reilly Media lors d'un brainstorming avec Craig Cline de MediaLive en octobre 2004).

Le Web2.0 peut être définit comme une partie de l'Internet 2.0 (regroupant tous les nouveaux services web mais aussi d'autres services comme la téléphonie ou la mobilité).

En parcourant différents ouvrages ou sites internet, des centaines de définitions et de concepts fleurissent au fil du temps. D'un côté, il s'agit d'une révolution technologique proposant sons, vidéos et images en temps réel, de l'autre interactivité plus grandes avec les sites web en passant par un sombre concept marketing que certains grands groupes voudraient vendre à l'internaute lambda. Néanmoins, une notion est toujours présente lorsque l'on parle du Web2.0 : l'utilisateur.

Lors de la première apparition de l'expression, plusieurs termes ont été émis pour définir le Web2.0 : « le Web en tant que plateforme ; les données comme « connaissances implicites » ; les effets de réseau entraînés par une « architecture de participation », l'innovation comme l'assemblage de systèmes et de sites distribués et indépendants ; des business model poids plume grâce à la syndication de contenus et de services ; la fin du cycle d'adoption des logiciels (« la version bêta perpétuelle »). »

L'expression intéressante ici est « les effets de réseau entraînés par une « architecture de participation ». Dans le Web1.0, l'internaute était seulement passif. A partir du Web2.0,

L'internaute, l'utilisateur devient actif : il crée son propre contenu, il partage des informations (photos, vidéos…), il se crée un réseau…

Depuis que l'homme existe, que ce soit dans la vie personnelle ou professionnelle, il se regroupe par centres d'intérêt pour former des réseaux. Maintenant, ces individus ont la possibilité de se regrouper en ligne via Internet en particulier sur les réseaux sociaux.

Ainsi, il est important de bien cerner l'usage de ces réseaux sur le Web et de pouvoir en définir les enjeux communautaires, sociologiques ou encore économiques. Pour cela, il est nécessaire de définir les réseaux sociaux, leur typologie et de savoir comment ils peuvent se former et se construire. Afin de mieux cerner le phénomène et d'en comprendre le port.

I. Définitions importantes

1. Donnée à caractère personnel [1]

En principe les données sont considérées comme à caractère personnel dès lors qu'elles permettent d'identifier directement ou indirectement des personnes physiques. Une personne est identifiée lorsque son nom apparaît dans un fichier. Une personne est identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification (ex. : n° d'immatriculation, adresse IP, numéro de téléphone, photographie...).

En ce sens, constituent également des données à caractère personnel toutes les informations dont le recoupement permet d'identifier une personne précise (ex. : une empreinte digitale, l'ADN, une date de naissance associée à une commune de résidence, ...). Les technologies de l'information et de la communication génèrent de nombreuses données personnelles (un paiement par carte bancaire, un appel passé par un téléphone portable, une connexion à internet) et aussi des "traces informatiques" facilement exploitables grâce aux progrès des logiciels, notamment les moteurs de recherche.

2. Social [1]

En peut l'exprimer comme la relation qui existe entre les vivants, dans divers domaines.
Cette notion se caractérise par vivre en société, relatif aux valeurs, critères ou comportement, réalité concrète engendré par une société divisé et hiérarchisée : ascension, différence, échelle, prestige, promotion, réussite sociale.
Aussi aux problèmes qui en sont issus : accord, antagonisme, cohésion, conflit, haine, lutte, pacte sociale…

3. Réseau social [2] [3]

Définir le reseau social,Cette mission est loin d'être aisée car sous le terme réseau social se cachent de nombreuses significations qu'il est difficile de résumer simplement. Une simple recherche sur Google des termes « réseau + social » en dit long sur l'étendu de cette notion : plus de 12 millions de résultats ! Et encore 500 000 résultats pour « réseaux + social + définition » !

Néanmoins, en analysant les différentes définitions on constate que l'on peut distinguer les réseaux sociaux dans leur dimension sociétale et sociologique et informatique des plateformes de réseautage social sur internet.
Pour les réseaux sociaux dans leur définition sociologique, la démarche adoptée est scientifique. La définition choisie : « *Un réseau social est un ensemble d'entités sociales telles que des individus ou des organisations sociales reliées entre elles par des liens crées lors de leurs interactions mutuelles, des réseaux sociaux peuvent être créés stratégiquement pour agrandir ou rendre plus efficient son propre réseau social (professionnel, amical,…) ».*

Du coté informatique « *Un réseau est un ensemble de nœuds (ou pôles) reliés entre eux par des liens (ou canaux). Les nœuds peuvent être des points massiques simples ou des sous-réseaux complexes. Les canaux sont à leur tour des flux de force, d'énergie ou d'information. L'étymologie du mot remonte au latin rete qui signifie « filet », donnant l'adjectif réticulé, caractérisant les objets ayant une structure de filet, notamment les réseaux* ».

Il existe plusieurs réseaux sociaux dans le monde, les plus utilisée sont facebook, twitter…

L'ingrédient fondamental du réseau social reste cependant la possibilité d'ajouter des amis (connaissances), et de gérer ainsi une liste de contacts.
L'émulation des réseaux sociaux fonctionne ensuite sur deux principes que l'on peut résumer ainsi :

- Les amis de mes amis sont mes amis.
- Les personnes qui partagent les mêmes centres d'intérêts que moi sont mes amis.

4. Vie privée [1]

Au sens classique ou historique, la vie privée été définie comme « le droit de vivre en paix ».

Au 21^{e} siècle, cependant, la vie privée a revêtu plusieurs dimensions .Pour certaines personnes, la vie privée signifie avoir droit á un espace privé, pouvoir effectuer des communications privée, être libre de toute surveillance et respecter le caractère sacré de la personne. (vie, 2003)

Il n'existe pas de définition juridique précise de la vie privée, rien qu'elle est l'ensemble des activités d'une personne qui relève de son intimité par opposition à la vie publique.

5. Sécurité [4] [5]

La sécurité est l'état d'esprit d'une personne qui se sent tranquille et confiante .c'est le sentiment, bien ou mal fondé, d'être à l' abri de tout danger et risque, il associe calme, confiance, quiétude, sérénité, tranquillité, assurance, sureté.
Les principes de la sécurité sont la disponibilité, l'intégrité, la confidentialité qui est la protection des données contre la divulgation, authentification et identification.

Concept permettant de s'assurer que l'information ne peut être lue que par les personnes autorisées.

Solution dans le monde réel :
– Utilisation d'enveloppes scellées
– Verrouillage avec clés
– Mesures de Sécurité physique

– Utilisation de l'encre invisible

6. **Confiance** [1]

La confiance renvoie à une attitude générale, rencontrée dans des circonstances multiples, où une personne détermine son comportement sur la base d'un sentiment puis d'un raisonnement.

II. Contexte de l'évolution d'Internet

1. Web traditionnel [6] [7]

Le Web 1.0 comprenait des pages statiques, dont le contenu était obtenu en prenant de la communication papier et en la transférant sous forme numérique dans des pages html qui n'étaient que rarement mises à jour, voire jamais
Ce mouvement n'a cependant pas totalement disparu. Pour preuve, on voit encore aujourd'hui des sites internet dits professionnels ne comportant qu'une plaquette scannée avec deux ou trois lignes de texte.

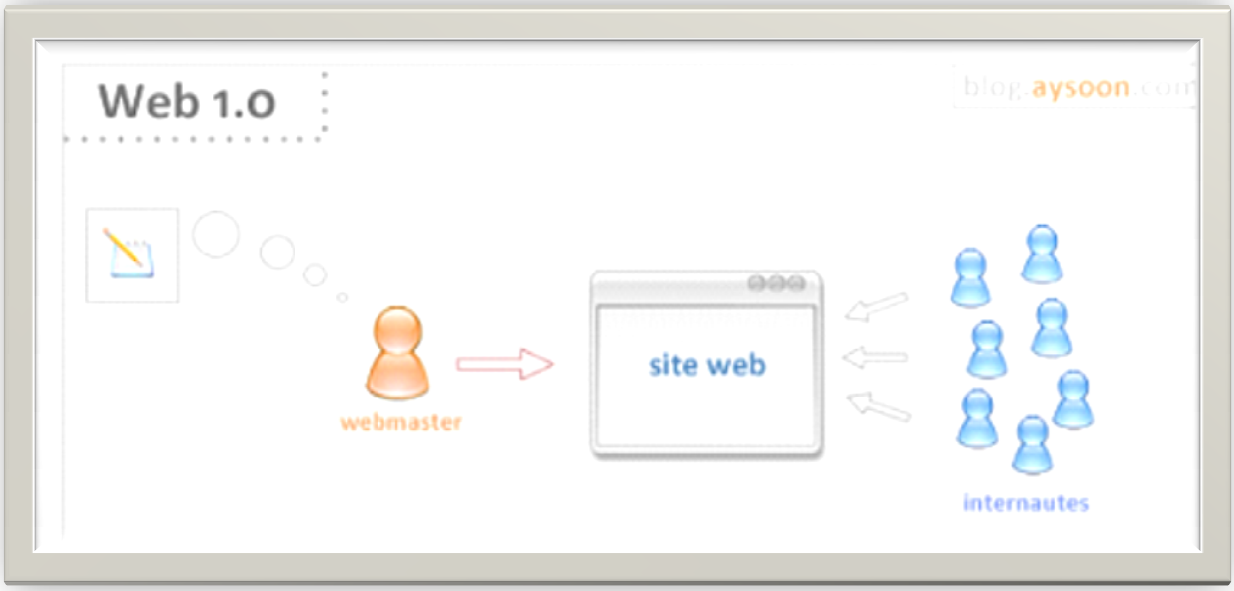


Figure 1: Représentation graphique du Web1.0

2. Web 2.0 ou web social [6] [7]

Le Web 2.0 est plus orienté partage de données. Il répond à la question principale que devrait se poser tout propriétaire de site internet à savoir la manière dont le contenu que ce dernier met en ligne peut être partagé au mieux avec d'autres utilisateurs.

L'internaute n'est alors plus un simple spectateur passif, mais devient un acteur jouant un rôle dans le site avec lequel il interagit. Dans cette optique sont apparus les réseaux sociaux et le phénomène de syndication : les fameux flux RSS[1].
Ainsi ces domaines XML[2], RSS et AJAX[3] : permettent le partage de l'information, en effet les documents sont reliés (blogs, photos, vidéo en ligne, WIKI), les utilisateurs ont d'avantage de pouvoir (leurs avis devient précieux) et les collaborations entre les sites marchands est mise en avant (phénomène de mashups[1]).
Cette version du web a vue une évolution qui est le web 3.0 caractérisée par une portabilité et une mobilité exceptionnelle.
C'est un web déstructuré. En effet, l'internaute n'a plus besoin d'aller sur Internet, c'est Internet qui vient à l'internaute.

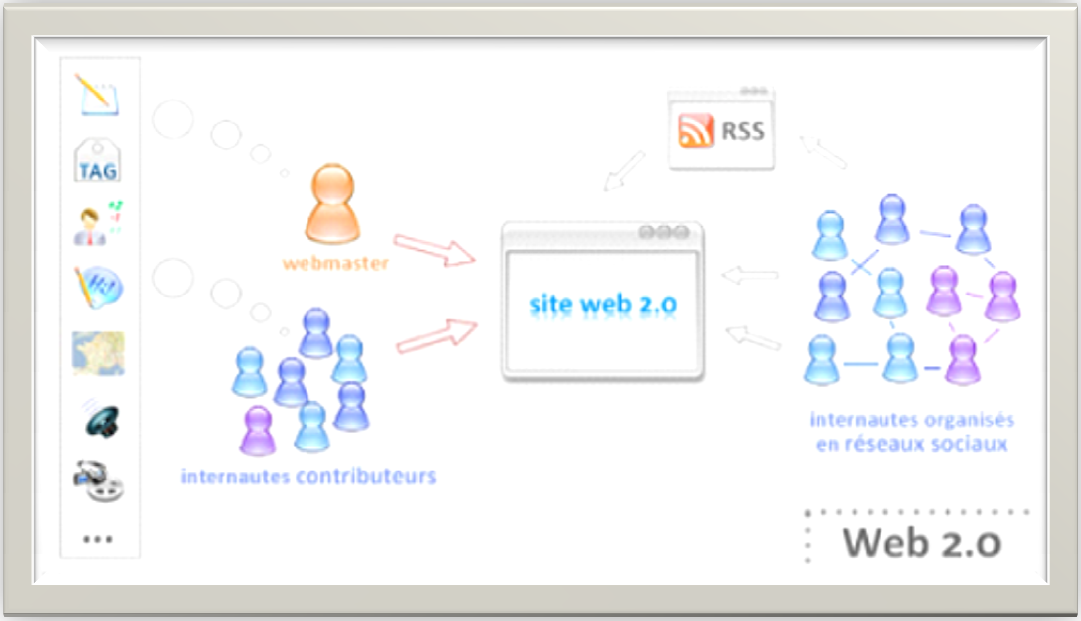


Figure 2 : Représentation graphique du Web 2.0

[1] Site internet ou application dont le contenu provient de la combinaison de plusieurs sources d'information.
[2] Extensible Markup Language, une spécification simple et un ensemble de codes qui permettent à des processus s'exécutant dans des environnements différents de faire des appels de méthodes à travers un réseau.
[3] Asynchronous JavaScript and XML, une solution informatique libre pour le développement d'applications Web.

3. Outils du web 2.0

Avec le Web 2.0, les nouveaux outils permettent aux internautes de participer en interagissant. La notion d'intelligence collective émerge. Par ailleurs, lors d'échanges d'une information sur le Web, celui qui la donne la détient toujours. Cela occasionne un enrichissement mutuel et l'on passe vers l'équation « 1+1=3 ». La collaboration dans les groupes fait émerger des résultats supérieurs à ceux obtenus par la somme des individus. D'un point de vue théorique, ceci s'explique par la loi de Metcalfe .

Concrètement, l'internaute dispose de plusieurs outils sur le Web. Le tableau comparatif qui suit résume leurs avantages respectifs selon les besoins.

Outil-Critères	Objectifs et caractéristiques	Mise à jour	Astuces	Outils
Blog	Partager dans un domaine donné. Outil de publication dynamique, simple à mettre à jour, interfaces facile d'emploi.	Par les membres de la communauté : Droit d'accès et d'écriture. Ensemble des lecteurs : Possibilité d'ajout de commentaires.	Faire participer ses partenaires pour alimenter régulièrement son blog sans s'épuiser.	TypePad, WordPress, etc.
Wiki	Créer une transversalité (structure projet). Travailler de façon collaborative et partager l'information de façon efficace.	Ajout et modification pour l'ensemble des utilisateurs. Possibilité de modération des informations publiées.	Planifier les tâches en fonction des rythmes et des cultures de chacun. Outil plus collectif que coopératif : pas de travail de reformulation par le collectif. Utile pour confronter et faire émerger des idées, permet les consensus.	Media Wiki, Blue Kiwi.
Newsletter	Fidéliser ses lecteurs, clients et prospects.	Publication au numéro. Fréquence variable selon les choix éditoriaux (par exemple mensuel).	Réaliser des Newsletters en interviewant des personnes, organiser des concours.	Http : // Yourmailinglist provider. com.
Forum	Rencontrer des personnes qui partagent les mêmes intérêts, resserrer les liens, enrichir ses connaissances dans les domaines.	Fréquente : selon les articles et les réponses publiés.	Co-animation des forums et listes de discussion.	

Tableau 3: Tableau comparatif des outils du web

III. La particularité du réseau social

La première personne à avoir représenté un réseau social est Jacob Levy Moreno au début des années 1930, son objectif étant de visualiser graphiquement un réseau social, il a représenté les personnes par des points et une relation entre deux personnes par des flèches .Cette représentation est depuis désignée par le terme sociogramme.
Apres cela cette représentation a été passée en revue par des mathématiciens pour devenir une représentation adoptée par toutes les sciences manipulant les réseaux sociaux.
Par la suite il ya eu Robin Dunbar et son fameux nombre de dunbar ,qui dessine la particularité des réseaux sociaux .

1. Nombre de Dunbar [8]

Le nombre de Dunbar est le nombre d'amis avec lesquels une personne peut entretenir une relation stable á un moment donné de sa vie. Cette limite est inhérente á la taille de notre néocortex, elle est estimée á 148 personnes ce qui montré dans la figure ci-dessous.

Ce nombre provient d'une étude publiée en 1993 par l'anthropologue britannique Robin Dunbar.

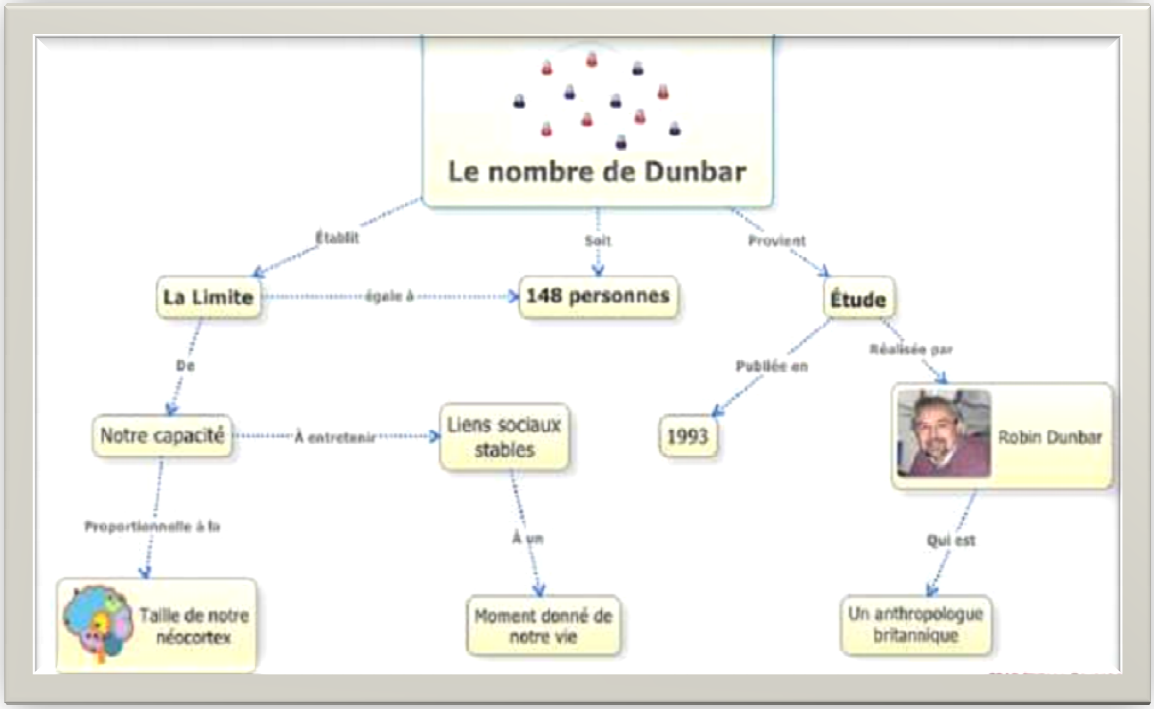
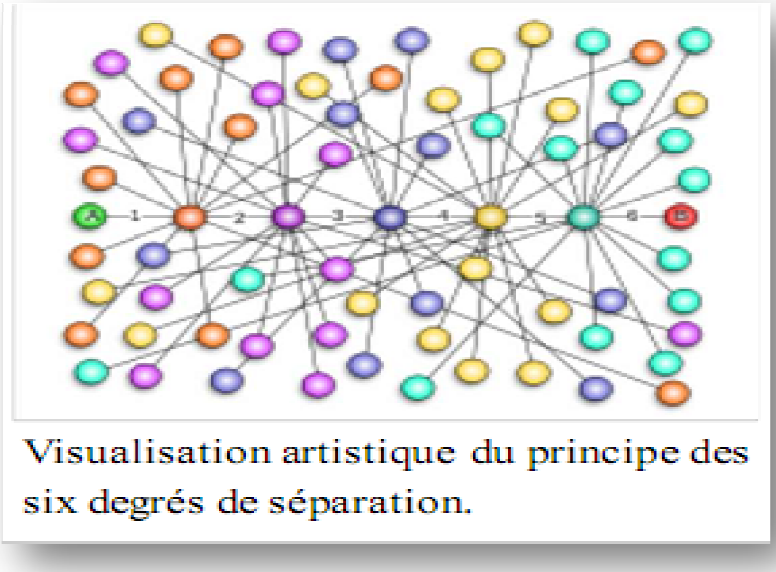


Figure 3 : Le schéma de Dunbar

2. Degrés de séparation

L'effet du petit monde est l'hypothèse que la longueur de la chaîne des connaissances sociales requise pour lier une personne arbitrairement choisie à n'importe quelle autre sur Terre est généralement courte. Le concept á engendré l'expression célèbre des « six degrés de séparation » après l'expérience du petit monde de 1967, réalisée par le psychologue Stanley Milgram .



Visualisation artistique du principe des six degrés de séparation.

Figure 4 : Six degrés de séparation

3. La loi de Reed

La loi de Reed affirme que la loi de *Metcalfe*[4] minimise la valeur des connexions ajoutées. Non seulement un membre est relié au réseau entier comme à un tout, mais également à beaucoup de sous-ensembles significatifs du tout.

[4] La Loi de Metcalfe est une loi théorique et empirique énoncée par Robert Metcalfe (fondateur de la société 3Com et à l'origine du protocole Ethernet).

Ces sous-ensembles ajoutent de la valeur à l'individu comme au réseau lui-même. En incluant des sous-ensembles dans le calcul de la valeur du réseau, la valeur augmente plus rapidement qu'en se cantonnant à ne prendre en compte que les noeuds.

Cette loi est particulièrement adaptée aux réseaux où individus, communautés et groupes plus ou moins formels sont considérés. Elle permet de rendre compte du web 2.0 et plus particulièrement dans sa dynamique sociale.

4. Classement des réseaux sociaux

Plusieurs catégories de réseaux sociaux existent. Aussi est-il tentant de classifier, de catégoriser les réseaux sociaux. On peut effectuer un classement des réseaux sociaux selon trois catégories:

- Réseaux ouverts.
- Réseaux sur invitation (il faut être invité par l'un de ses membres).
- Services en ligne de réseautage professionnels (favorisent les rencontres professionnelles, les offres de poste et la recherche de profils).

Mais d'autres classifications existent :

- Les networkings : les plus utilisés dans les milieux professionnels. Ils permettent des échanges entre professionnels sur des plateformes en évolution perpétuelles.
- Les bloglikes : ils ressemblent vaguement à des blogs. Ils sont souvent le refuge d'ados en mal de reconnaissance.
- Les spécialisés : ils regroupent des communautés autour d'un thème bien précis
- Le micro-blogging : chat public, summum du narcissisme, on y met tout ce qu'on y fait minute par minute, histoire de montrer aux autres qu'on est très actif.
- Les fourres-tout : ce sont les inclassables qui se servent du collaboratif ou du participatif pour alimenter leur service.

On peut y trouver, les sites de partage d'avis

- Les open-sources : ou plutôt les plateformes qui vous permettront de créer votre propre réseau social.

5. Une utilisation inégale par pays

Il n'y a pas encore de leader mondial incontesté. Chaque pays a ses préférences. Ainsi la carte ci-dessous permet de visualiser la fréquence d'utilisation des différents réseaux.

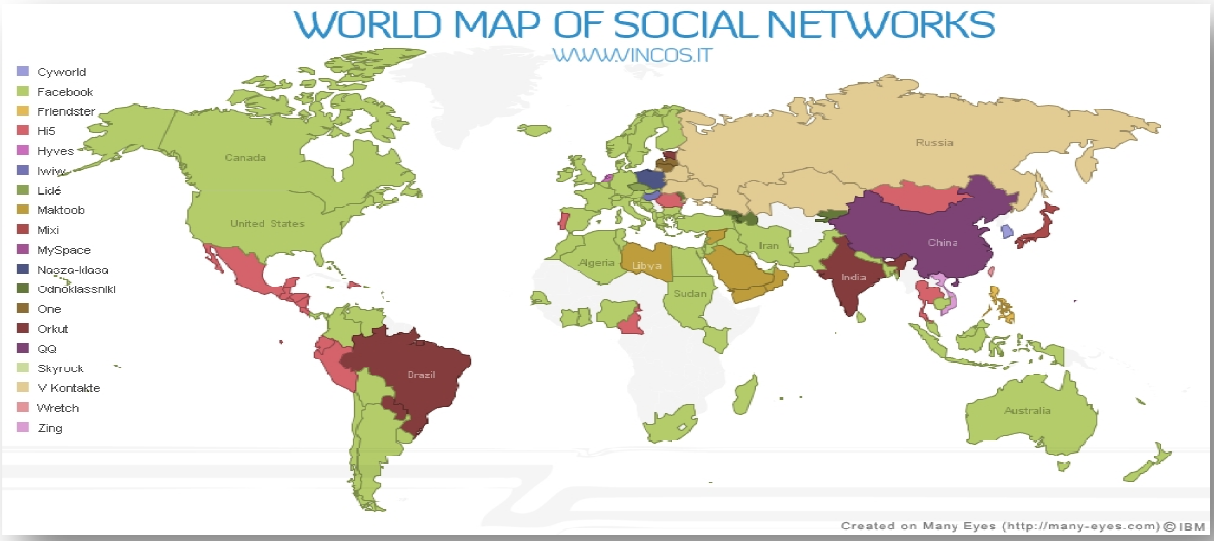


Figure 5 : Utilisation des réseaux sociaux dans le monde

IV. Présentations des réseaux sociaux

1. Twitter

Twitter est un outil de réseau social et de microblogage qui permet à l'utilisateur d'envoyer gratuitement des messages brefs, appelés tweets (« gazouillis »), par Internet, par messagerie instantanée ou par SMS.

twitter

Logo de Twitter

Création	2006
Personnages clés	Jack Dorsey, Biz Stone et Evan Williams
Slogan	« Discover what's happening right now, anywhere in the world Découvrez en temps réel ce qui se passe partout dans le monde »
Siège social	San Francisco, Californie (États-Unis)
Direction	Jack Dorsey (président), Evan Williams (CEO)
Activité	Internet
Produits	Service de microblog
Effectif	600 [1]
Site web	twitter.com (https://twitter.com/)

Figure 6: Identité de Twitter

2.1. Historique [9]

Twitter a été créé à San Francisco au sein de la startup Odeo Inc .fondée par Noah Glass et Evan Williams. Noah Glass commercialisait Twitt'Ver, une application permettant de publier des fichiers audio sur un blog au moyen d'un téléphone. Evan Williams est connu pour être entre autres le cofondateur de la société Pyra Labs, à l'origine de la plateforme de blogs Blogger, rachetée par Google en 2003. Odeo proposait une plateforme d'hébergement, de diffusion et d'enregistrement de podcasts.

À côté de ce service de podcasts dont le marché est très concurrentiel, Jack Dorsey, dispatcheur pour une compagnie de taxis, et Noah Glass, ancien répartiteur au 911, numéro centralisé des urgences américaines, furent chargés de développer un nouveau service .

L'idée de départ était de permettre aux utilisateurs de décrire ce qu'ils étaient en train de faire via SMS. Ouvert au public le 13 juillet 2006, la première version s'intitulait stat.us puis twittr, en référence au site de partage de photos Flickr puis Twitter, son nom actuel

Le 25 octobre 2006, les actifs de la société Odeo ont été rachetés par Obvious Corp Puis en avril 2007, une entité indépendante est créée avec comme nom Twitter, Inc. avec Jack Dorsey à sa tête jusqu'en octobre 2008 date à laquelle Evan Williams lui succédera. La société compte 29 employés en février 2009 et 300 en octobre 2010.

Entre temps, Twitter a remporté le prix 2007 South by Southwest Web Award dans la catégorie blog. Le 4 octobre 2010, Evan Williams, le cofondateur, annonce qu'il passe la main à Dick Costolo, ancien directeur d'exploitation.

Croquis préliminaire sur papier de Twitter (alors intitulé « stat.us »).

Figure 7 : Croquis de Twitter

- **Identité visuelle (logo)**

Figure 8 : Logo de Twitter

2.2. Présentation [10]

Twitter est un service de microblogage, permettant aux utilisateurs de bloguer grâce à des messages courts (140 caractères maximum, soit une ou deux phrases) par Internet, messagerie instantanée, téléphone portable.

Outre cette concision imposée, la principale différence entre Twitter et un blog traditionnel réside dans le fait que Twitter n'invite pas les lecteurs à commenter les messages postés.

Le slogan d'origine de Twitter, *What are you doing*?, le définissait comme un service permettant de raconter ce qu'on fait au moment où on le fait. Prenant acte de l'utilisation du service pour s'échanger des informations et des liens, Twitter le remplace par *What's happening*? (« Quoi de neuf ? » ou encore « Que se Passe-t-il ? » Dans la version française).

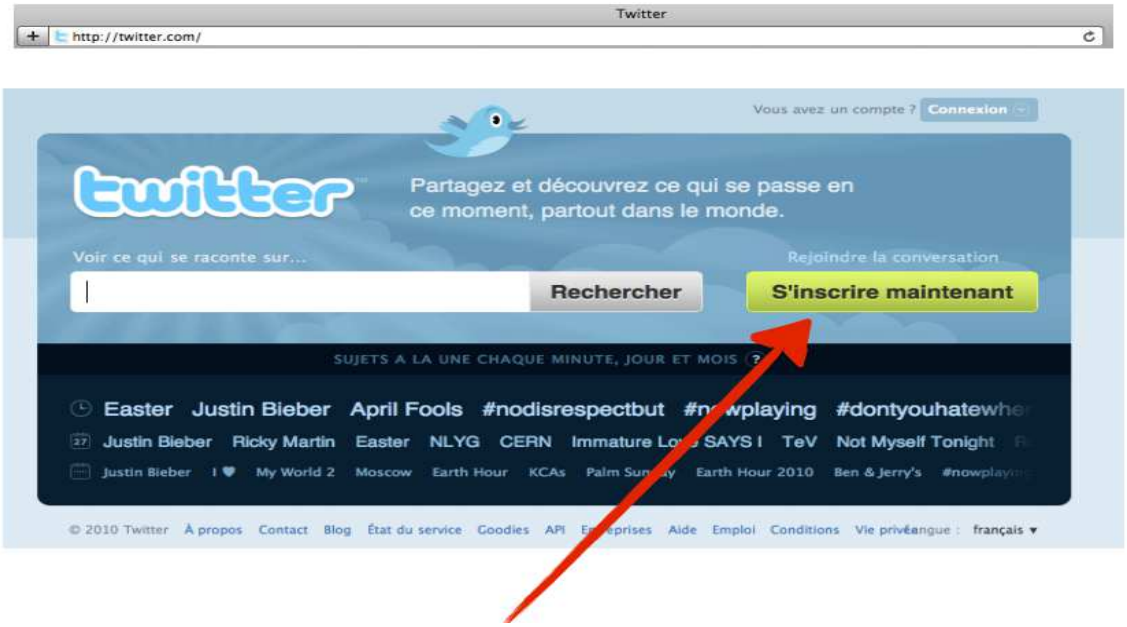
De tous les médias sociaux, Twitter est celui le plus abrupt, le plus difficile à appréhender quand on démarre. Contrairement à Facebook où l'on retrouve facilement ses amis, sa famille, contrairement à LinkedIn où l'on retrouve facilement ses collègues, ses clients, sur Twitter, on démarre avec une page blanche : pour le débutant, Twitter s'apparente souvent à une caverne magique dont on a du mal à trouver l'entrée.

2.3. Fonctionnalités de Twitter [11]

2.3.1. Devenir utilisateur Twitter

Créer un compte permet de publier rapidement de courts textes mais aussi des liens vers des photos que l'on vient de prendre et que l'on souhaite partager avec les personnes qui nous suivent.

Devenir un utilisateur enregistré offre la possibilité de réagir ou de publier à nouveau le message d'autres utilisateurs ou encore d'envoyer des messages privés.
Première étape pour créer un compte, se rendre sur le site internet de Twitter : http://twitter.com.



Cliquer sur le bouton «S'inscrire maintenant».

Figure 9 : Page d'accueil de twitter

2.3.2. Possibilité d'interagir dans le réseau

Vous pouvez alors écrire, «tweeter», en écrivant dans le cadre «Quoi de neuf ?» et en respectant les 140 caractères disponibles (le compteur à droite est là pour vous rappeler à l'ordre !)...

Figure 10 : Comment écrire sur Twitter

2.3.3. S'abonner à un compte

Se rendre tout d'abord sur le compte choisi en étant connecté et simplement cliquer sur «Suivre».

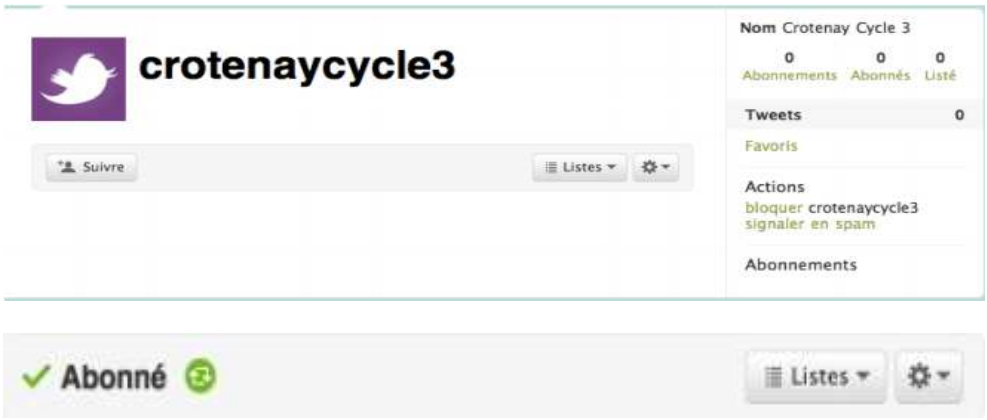


Figure 11 : Comment s'abonner à un compte

Le bouton suivre se transforme alors en «Abonné» : vous êtes désormais abonnés au compte choisi. Tous les tweets de cet utilisateur arriveront sur votre ligne du temps (sur votre page d'accueil).

Depuis la page d'un utilisateur, vous pouvez également classer directement ce compte dans vos listes personnelles avec le menu déroulant «Listes».

Le menu déroulant représenté par un engrenage vous permet plusieurs opérations :

- ✓ «Citer» l'utilisateur dans un nouveau message public que tous vos abonnés verront (mais aussi cet utilisateur même s'il ne fait pas partie de vos abonnés, vu que vous l'avez cité).
- ✓ «Ne plus suivre» : vous pouvez décider de ne plus être abonnés à cet utilisateur.
- ✓ «Bloquer» : l'utilisateur ne pourra pas vous suivre.
- ✓ «Signaler comme spam» signalera le compte aux services de Twitter comme étant susceptible d'être un spammeur (cf cet article de Wikipédia décrivant le spam).

Figure 12 : Menu déroulant

2.3.4. De nouvelles fonctionnalités dans Twitter

Twitter innove et va offrir de nouvelles fonctionnalités à l'ensemble des utilisateurs du réseau social. Pour l'instant, ces nouveautés ne sont accessibles qu'à un nombre limité de personnes, la nouvelle architecture proposera une navigation et des fonctions de recherche plus simples et plus rapides pour l'utilisateur. D'autre part, Twitter proposera aussi d'intégrer de nouveaux types de contenu comme la possibilité de placer des vidéos Youtube.

2. Facebook

La compagnie Facebook est située à Palo Alto en Californie. Le fondateur et directeur général est M. Mark Zuckerberg de l'Université de Harvard.

Facebook est actuellement le réseau social le plus populaire au monde (5ème site le plus visité).

Facebook, Inc.

Logo de Facebook

Création	4 février 2004
Fondateurs	Mark Zuckerberg Dustin Moskovitz Chris Hughes Eduardo Saverin
Siège social	Palo Alto, Californie (États-Unis)
Direction	Mark Zuckerberg (PDG) Sheryl Sandberg
Activité	Réseau social
Produits	Timeline, Ticker, Facebook Music, Facebook Lieux, Facebook Games, Instagram
Effectif	+ de 3 000 (2011)[1]
Site web	facebook.com (https://www.facebook.com/)
Chiffre d'affaires	3 710 M USD (2011) ▲
Résultat net	▲ 500 M USD[2, 3] (2010)

Figure 13 : Identité de Facebook

2.1. Historique

Le nom du site s'inspire des albums photo (« trombinoscopes » ou « *facebooks* » en anglais) regroupant les photos prises de tous les élèves au cours de l'année scolaire et distribuées à la fin de celle-ci aux étudiants. Facebook est né à l'université Harvard : c'était à l'origine le réseau social fermé des étudiants de cette université, avant de devenir accessible aux autres universités américaines. La vérification de la provenance de l'utilisateur se faisait alors par une vérification de l'adresse électronique de l'étudiant. Le site est ouvert à tous depuis septembre 2006.

- Logo visuelle de Facebook :

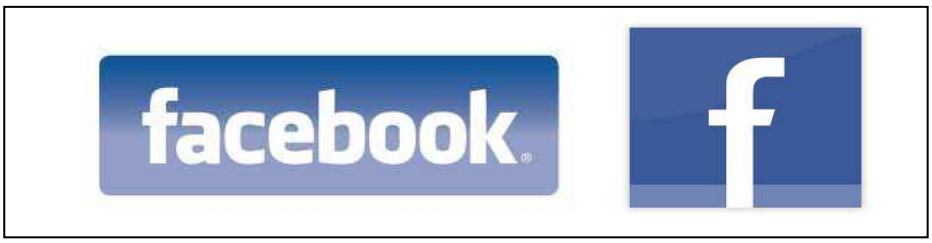


Figure 14 : loge de Facebook

2.2. Présentation

Facebook est un réseau social sur Internet permettant à toute personne possédant un compte de créer son profil et d'y publier des informations, dont elle peut contrôler la visibilité par les autres personnes, possédant ou non un compte. L'usage de ce réseau s'étend du simple partage d'informations d'ordre privé (par le biais de photographies, liens, textes, etc) à la constitution de pages et de groupes visant à faire connaitre des institutions, des entreprises ou des causes variées. L'intégralité des informations publiées sur ces deux supports, à l'inverse du profil, peut être consultée par n'importe quel internaute sans qu'il soit nécessaire d'ouvrir un compte.

2.3. Fonctionnalité de Facebook

Facebook propose à ses utilisateurs des fonctionnalités optionnelles appelées « applications », représentées par de petites boîtes superposées sur plusieurs colonnes qui apparaissent à l'affichage de la page de profil de l'utilisateur. Ces applications modifient la page de l'utilisateur et lui permettent de présenter ou échanger des informations aux personnes qui visiteraient sa page. L'utilisateur trouvera par exemple : une liste d'amis, une liste des amis qu'il a en commun avec d'autres amis, une liste des réseaux auxquels l'utilisateur et ses amis appartiennent, une liste des groupes auxquels l'utilisateur appartient, une boîte pour accéder aux photos associées au compte de l'utilisateur, un « mini-feed » résumant les derniers évènements concernant l'utilisateur ou ses amis, sur Facebook et un « mur » permettant aux amis de l'utilisateur de laisser de petits messages auxquels l'utilisateur peut répondre.

Par ailleurs une fonction de messagerie instantanée, disponible depuis avril 2008, permet de signaler à ses amis sa présence en ligne et, si nécessaire, de discuter dans un « salon » privé (l'application ne permettant pas, en octobre 2010, de réunir plus de deux personnes dans un même salon). Depuis février 2010, le chat de Facebook utilise le protocole de communication XMPP, afin de permettre aux utilisateurs de s'y connecter avec n'importe quel client de messagerie instantanée compatible avec ce protocole.

Le choix des applications à afficher est laissé à l'utilisateur, qui peut en ajouter après avoir consulté le catalogue, ou bien en supprimer, changer leur agencement sur la page, ou en

cacher certaines au public. Les applications permettent aussi aux membres de Facebook de jouer gratuitement à des jeux.

2.3.1. Devenir utilisateur Facebook

Pour ceux qui n'ont pas encore de compte Facebook, explication dans cette vidéo http://www.youtube.com/watch?v=OWxAWQchp1M ou ce tutoriel http://www.memoclic.com/1215-facebook/7473-facebook-creation-compte-reseau-social.html

Vous devez posséder une adresse email valide pour votre inscription car vous devrez confirmer celle-ci par le biais d'un email.
Lors de l'inscription il est préférable de donner uniquement les informations nécessaires illustrées ci-contre.

Page 15 : Page d'inscription à Facebook

Votre page d'accueil après inscription ressemble à ceci :

Page 16: Modifier son profil sur Facebook

Avant même de compléter votre profil en cliquant sur Afficher et modifier votre profil, il est nécessaire d'en paramétrer les options de confidentialité.

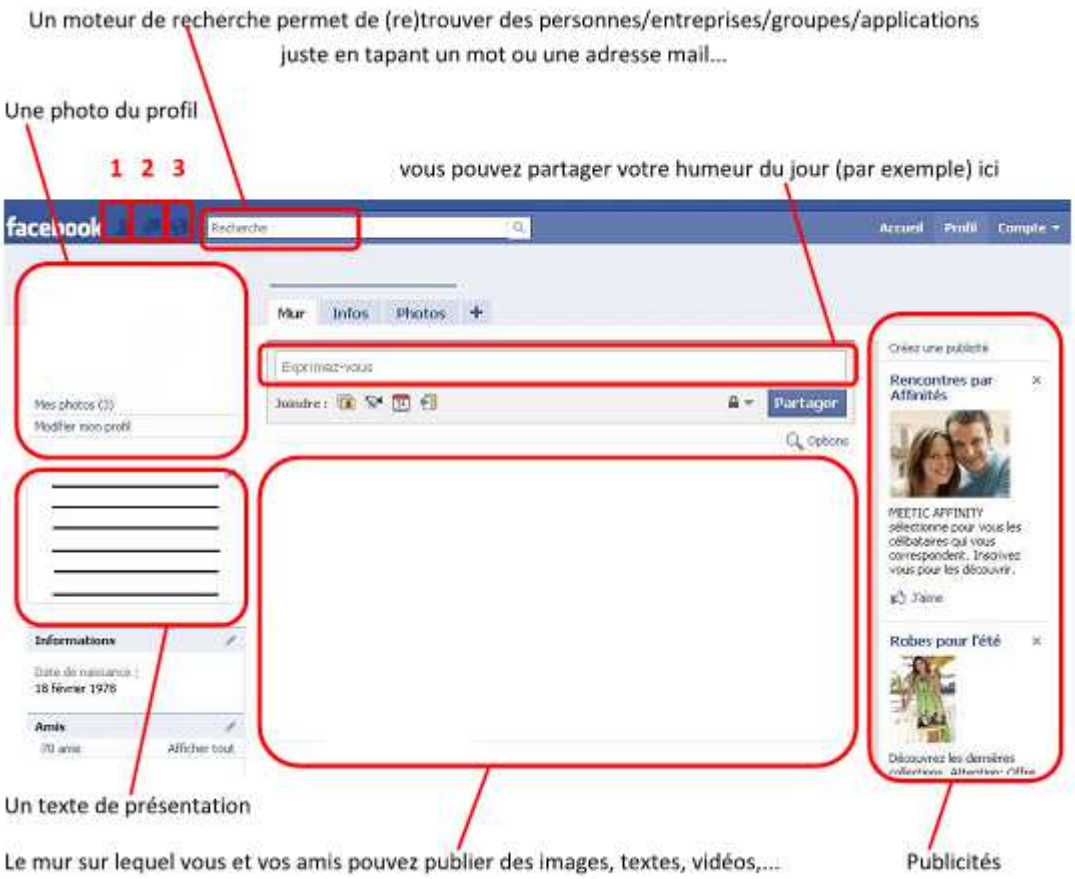
Le profil, accessible aussi par la barre horizontale de couleur bleu située tout en haut de la page Facebook, est la page que vos amis peuvent consulter lorsqu'ils cliquent sur votre nom et qui contient toutes les informations que vous souhaitez publier.

Deux choses sont importantes,

- ✓ réfléchir aux informations que vous allez publier
- ✓ et avant même de les publier, pensez à paramétrer les options de confidentialité du module Profil.

Vous pouvez trouver réponses à toutes vos questions sur la page profil à cette adresse http://www.facebook.com/help.php?page=402 de la rubrique d'aide.

Exemple : une page d'un nouveau profil, pas encore rempli.



1- Signal une invitation d'amis
2- Boite de réception
3- Notification ou actualités

Page 17: Exemple d'un nouveau profil Facebook

Vous avez la possibilité de paramétrer la confidentialité de 4 modules illustrés ci-dessous

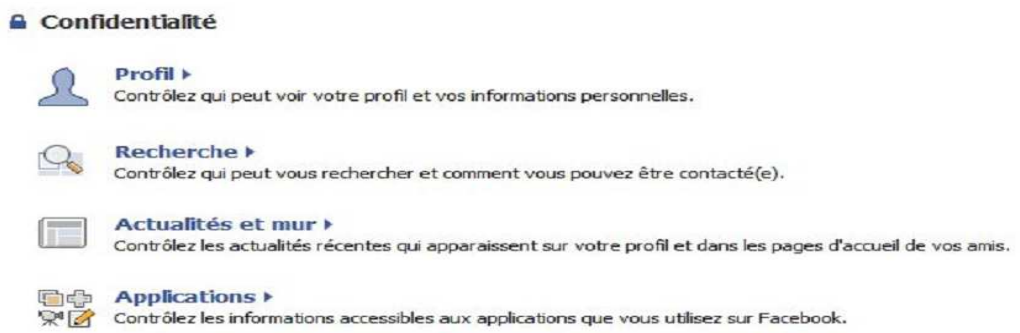


Figure 38 : Parametres de Confidentialités

2.3.2. Possibilité d'interagir avec le réseau

Facebook permet a ces utilisateurs d'entrer des informations personnelle et d'interagir avec d'autre utilisateurs, les informations susceptibles de d'être mises a disposition du réseau concernant l'état civil, les études et les centres d'intéres.ces informations permettent de retrouver les utilisateurs partageant les même intérêts .ces dernier peuvent former des groupes et y'inviter d'autres personnes, l'interaction inclues le partages de tout document.

- **Ecrire sur le mur**

le mur de Facebook contient les phrases de statuts et les liens publiés avec l'outil de publication , également les commentaires sur un message d'un ami ,aussi il existe aussi le Botton j'aime ou je n'aime pas. Il faut avoir confiance en ses amis… pour les laisser écrire des messages qui peuvent être vus par d'autres. Ce dernier peut être vu par tous les amis ou quelque uns, ou bien rendre le mur invisible donc privé.

- **Envoi de message**

Les messages des internautes de Facebook utilisent le protocole de communications XMPP.

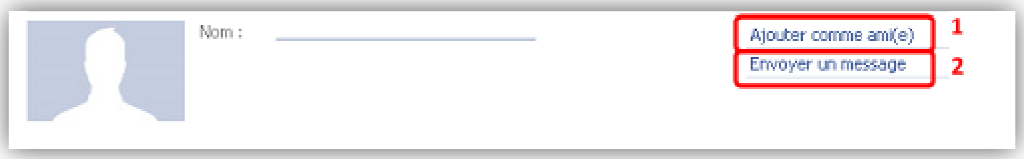


Figure 19:Interface de communication

- **Publicité ciblée**

La force de la publicité dans Facebook réside dans le contenue déposés

Figure 20 : Divers activités de facebook

2.3.3. Créer une page personnel [12]

La création d'une page Facebook peut répondre à plusieurs objectifs. Dans tous les cas, l'entreprise doit bien réfléchir à ce qu'elle veut faire de sa page Facebook. Parmi les objectifs les plus courants que se fixent les entreprises sont :

- Recruter sur Facebook.
- Trouver des prospects et des partenaires.
- Faire de la publicité.
- Développer son « capital social ».

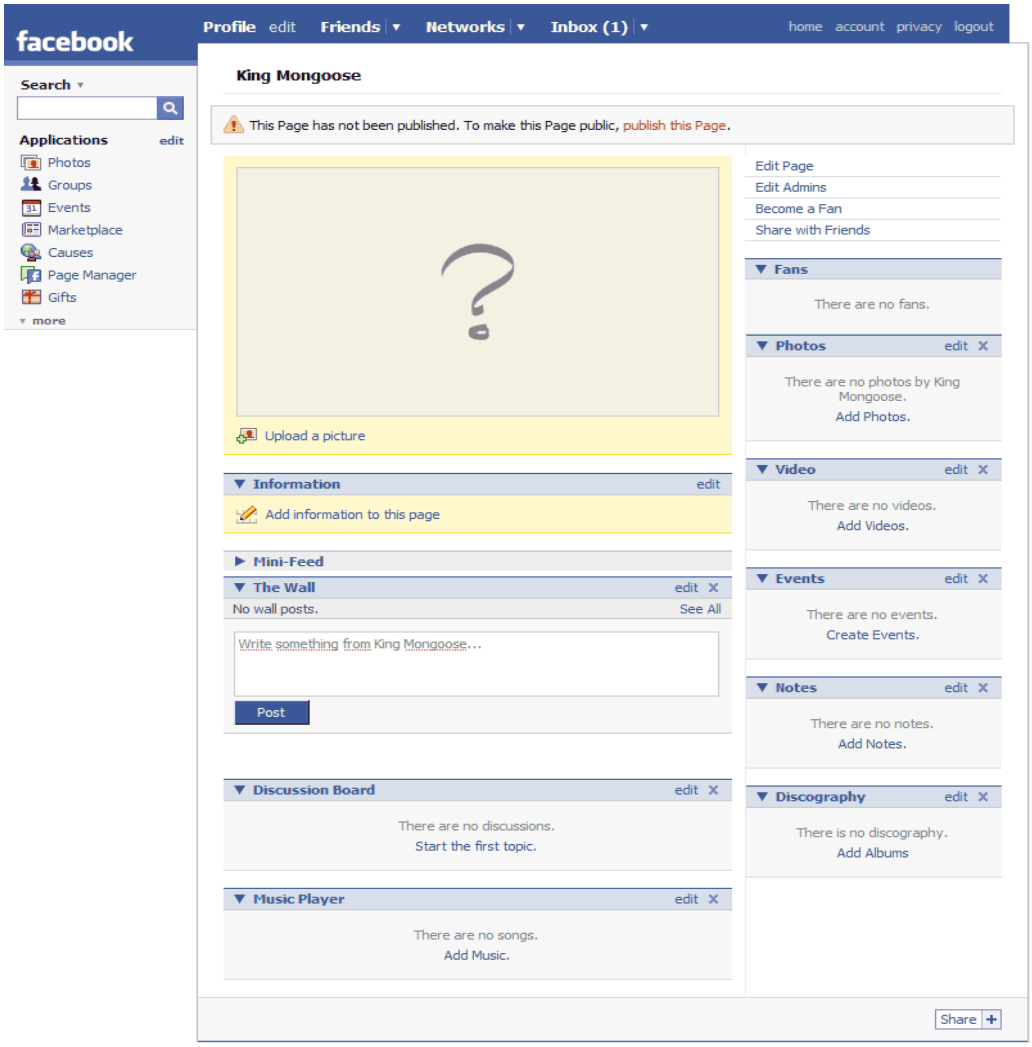


Figure 41 : Page Facebook

2.3.4. nouvelles fonctionnalités dans Facebook

La possibilité de :

Partage :

1. Tagger les gens en cliquant sur un bouton.
2. Dire ou tu es en cliquant sur un autre bouton.
3. Le plus cool des tous c'est la gestion de vos statuts.

Profil :

1. Revoir les tags avant qu'ils soient partagés sur Facebook (refuser ou valider le tag).
2. Possibilité de choisir avec qui vous voulez partager.
3. La possibilité de gérer vos statuts même s'ils sont déjà partagés vous pouvez les rectifier.

Dans ce chapitre, nous avons présenté les réseaux informatiques et donné leur classification Suivant la distance. Comme nous nous sommes intéressés au Web, à ses ressources et aux différents termes s'y rapportant, au final nous avons parlé des réseaux sociaux tel que Facebook dont ces moindre détailles inscription, utilisations....

Chapitre 2

Sécurité Informatique

Un réseau informatique est un ensemble d'éléments matériels reliés entre eux dans le but de permettre aux utilisateurs de partager des ressources et d'échanger des informations. Cet échange entre différentes entités fait sujet de cybers attaques, ce qui a poussé la recherche informatique à découvrir les diverses failles pouvant touchées la sécurité des réseaux de manière générale, et des réseaux sociaux plus précisément dans le seul but de les combattre en instaurant des politiques de protection.

I. Généralités sur la sécurité informatique

1. Qu'est ce que la sécurité informatique ? [13][14]

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

La sécurité informatique utilise un vocabulaire bien défini, par conséquent il est nécessaire de définir certains termes :

1.1. Les vulnérabilités [13]

Ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.

1.2. Les contre-mesures [13]

Ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).

1.3. Les menaces [14]

L'ensemble des actions de l'environnement d'un système pouvant entraîner des pertes financières. Elles peuvent provenir d'adversaires déterminés capables de monter une attaque exploitant une vulnérabilité.

- **Menaces relevant de problèmes non spécifiques à l'informatique**
  - ✓ Risques matériels accidentels: techniques de protection assez bien maîtrisées (incendie, explosion, inondation, tempête, foudre)
  - ✓ Vol et sabotage de matériels : vol d'équipements matériels, destruction d'équipements, destruction de supports de sauvegarde

- **Les pannes et les erreurs (non intentionnelles)**
  - ✓ Pannes/dysfonctionnements du matériel,
  - ✓ Pannes/dysfonctionnements du logiciel de base,
  - ✓ Erreurs d'exploitation : oubli de sauvegarde, écrasement de fichiers
  - ✓ Erreurs de manipulation des informations : erreur de saisie, erreur de transmission, erreur d'utilisation,
  - ✓ Erreurs de conception des applications,
  - ✓ Erreurs d'implantation.

- **Les menaces intentionnelles**

  L'ensemble des actions malveillantes(qui constituent la plus grosse partie du risque).

Qui devraient être l'objet principal des mesures de protection.

1.4. Les attaques (exploits) [14]

Elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.

1.4.1. Types des attaques

a. Attaques passives [13]

- ✓ Détournement des données (l'écoute, les indiscrétions)

Exemples: espionnage industriel

- ✓ Espionnage commercial
- ✓ Violations déontologiques
- ✓ Détournement des logiciels

Exemple: copies illicites

b. Attaques actives [13]

- ✓ Modifications des informations

Exemple : la fraude financière informatique, le sabotage des informations (logique)

- ✓ Modification des logiciels

Exemples: Bombes logiques, virus, ver

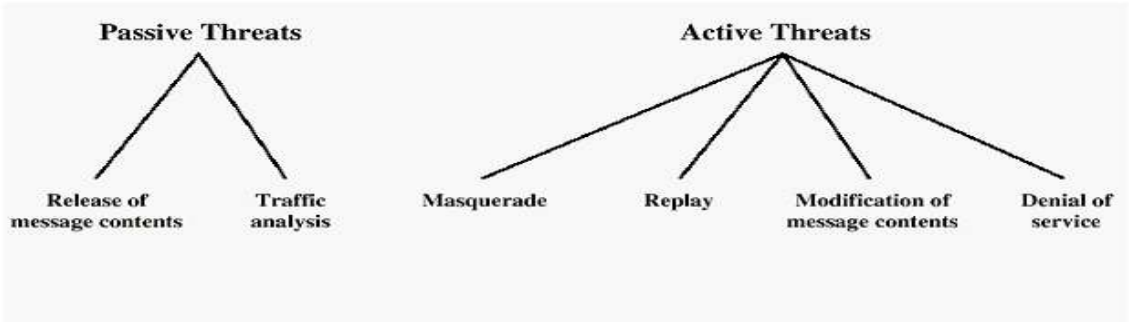


Figure 1 : Attaque passive et attaque active

1.4.2. Buts des attaques [14]

- ✓ *Interruption:* vise la disponibilité des informations
- ✓ *Interception:* vise la confidentialité des informations
- ✓ *Modification*: vise l'intégrité des informations
- ✓ *Fabrication*: vise l'authenticité des informations

1.4.3. Profils et capacités des attaquants [15]

Les attaquants peuvent être classés non-seulement par leurs connaissances (newbies, experts, etc...) mais également suivant leurs capacités d'attaques dans une situation bien définie. Ainsi, on dénombrera les capacités suivantes :

- ✓ Transmission de messages sans capacité d'écoute (IP spoofing...)
- ✓ Ecoute et transmission de messages
- ✓ Ecoute et perturbation des communications (blocage de paquets, DoS et DDoS...)
- ✓ Ecoute, perturbation et transmissions de messages
- ✓ Ecoute et relai de messages (attaques type man-in-the-middle)

Une autre caractéristique des attaquants va être leur emprise unidirectionnelle ou bi directionnelle sur les communications, du fait de la nature asymétrique de celles-ci. En effet, la plupart des canaux de transmissions sur Internet ou sur tout autre réseau hétérogène sont unidirectionnels et empruntent des chemins différents suivant les règles de routage. Ainsi, de nombreux protocoles de sécurité sont également unidirectionnels et il faut établir plusieurs canaux pour permettre un échange en "duplex". Ces canaux qui sont au nombre de 2 minimum, sont la plupart du temps gérés de façon totalement indépendante par les protocoles de sécurité. C'est le cas pour SSL/TLS mais également pour IPSec dont les associations de sécurité (SA) sont

unidirectionnelles et indépendantes, chacune définissant son propre jeu de clés, algorithmes, etc...

2. Services principaux de la sécurité informatique [15]

Pour remédier aux failles et pour contrer les attaques, la sécurité informatique se base sur un certain nombre de services qui permettent de mettre en place une réponse appropriée à chaque menace. A ce niveau, aucune technique n'est encore envisagée; il ne s'agit que d'un niveau d'abstraction visant à obtenir une granularité minimale pour déployer une politique de sécurité de façon optimale (les aspects pratiques tels qu'analyses de risques, solutions technologiques et coûts viendront par la suite. Décrivons les principaux services de sécurité :

- ✓ *Confidentialité*
- ✓ *Authentification* (entité, origine des données)
- ✓ *Intégrité*
  - ❖ Machines (tamper-résistance, tamper-proofness, exécution sécurisée...)
  - ❖ Données (avec possibilité de récupération)
  - ❖ Flux :
    - → Mode non-connecté, au niveau paquet (échanges de type requête-réponse, comme UDP)
    - → Mode orienté-connexion (ensemble de l'échange, comme TCP)
    - → Intégrité de séquences partielles (VoIP, applications, etc... permet d'éviter les DoS par exemple)
- ✓ *Contrôle d'accès* (autorisation, à différentier de l'authentification)
- ✓ *Non-répudiation* (avec preuve d'émission ou avec preuve de réception)

Notez que le chiffrement, les signatures digitales et autres techniques correspondent au niveau d'abstraction inférieur, décrit comme l'ensemble des mécanismes de sécurité permettant de réaliser les services décrits ci-dessus.

Plusieurs mécanismes peuvent par exemple réaliser le service d'authentification (schémas d'authentification, chiffrement, signatures digitales...).

Néanmoins, ces mécanismes de sécurité ne correspondent pas encore aux solutions finales qui seront réellement implémentées.

Il faudra pour cela effectuer un dernier raffinement, consistant à choisir les algorithmes symétriques, les algorithmes asymétriques, la taille des clés, etc....

3. Les objectifs de la sécurité informatique

La sécurité informatique à plusieurs objectifs, bien sûr liés aux types de menaces ainsi qu'aux types de ressources, etc... Néanmoins, les points principaux sont les suivants :

- ✓ Empêcher la divulgation non-autorisée de données
- ✓ Empêcher la modification non-autorisée de données
- ✓ Empêcher l'utilisation non-autorisée de ressources réseau ou informatiques de façon générale

II. La sécurité dans les réseaux

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet.
La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenu un point primordial dans la mise en place de réseaux informatiques.

1. Politiques de sécurité [16]

- ➢ Sécuriser les communications
  - ✓ Cryptographie (systèmes à clés…)
  - ✓ Brouillage, saturation…
  - ✓ Routage sécurisé (spécification de chemins autorisés)
  - ✓ Analyseur de sécurité

- ➢ Contrôler l'accès aux frontières du domaine
  - ✓ Fire-Wall (sites de confiance et autres, authentification)
  - ✓ Blocage des ports
  - ✓ Ecoute des flux entrants et sortants pour repérer les attaques/intrus (bande passante)
  - ✓ Piratage par logiciels espions « spywares »

- ➢ Audits : traces (pannes, attaques…)

2. Attaques de sécurité [17]

Les attaques portées à la sécurité d'un ordinateur ou d'un réseau sont mieux caractérisées en considérant le système en tant que fournisseur d'information.

En général, il existe un flot d'information issu d'une source, un fichier ou une zone de la mémoire centrale, vers une destination, un autre fichier ou utilisateur.

Il existe quatre catégories d'attaques : interruption, interception, modification, fabrication.

- *Interruption*

Un atout du système est détruit ou devient indisponible ou inutilisable.
C'est une attaque portée à la disponibilité. La destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont des exemples.

- *Interception*

Une tierce partie non autorisée obtient un accès à un atout. C'est une attaque portée à la confidentialité.
Il peut s'agir d'une personne, d'un programme ou d'un ordinateur.
Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes en sont des exemples.

- *Modification*

Une tierce partie non autorisée obtient accès à un atout et le modifie de façon (presque) indétectable.
Il s'agit d'une attaque portée à l'intégrité. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques.

- *Fabrication*

Une tierce partie non autorisée insère des contrefaçons dans le système. C'est une attaque portée à l'authenticité.
Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier.

3. Historiques des attaques [18]

- ✓ 1975 : Jon Postel pressent le SPAM
- ✓ 1983 : blagues de potaches
- ✓ 1983 : Wargames
- ✓ 1986 : Cukoo's egg
- ✓ 2 Novembre 1988 : Ver de Morris
- ✓ 2001 : Code Rouge
- ✓ 24 janvier 2003 : Slammer
- ✓ 2004 : Location de zombies
- ✓ 2009 : Conficker :
- ✓ 2010 : Opération Aurora (Google)
- ✓ 2010 : BotNet Mariposa
- ✓ 2010 : Ver stuxnet

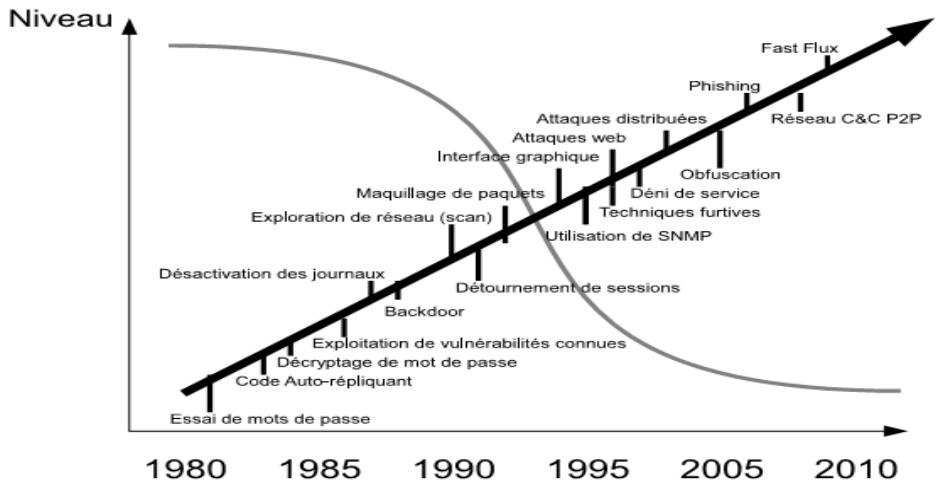


Figure 2 : Niveau des attaques

4. Les mécanismes de sécurisation

4.1. **Authentification** [16]

L'authentification est le premier rempart aux attaques informatique, il s'agit la plupart du temps du couple « Nom d'utilisateur/Mot de passe » (Login/Password).

Cette première méthode constitue une sécurité relativement fiable lorsqu'elle est bien utilisée: mot de passe correct, confidentialité assurée, fichier protégé,. . .
Elle pose tout de même certains problèmes comme par exemple le cas ou un utilisateur a besoin de se connecter sur plusieurs stations différentes.
Il va alors rapidement trouver cette méthode d'authentification relativement lourde.
Il éxiste plusieurs méthodes d'authentification, comme par exemple Kerberos (gestion de tickets), SSL (Secure Socket Layer), S-HTTP (Secure HTTP), les signatures digitales (Digital Signature) et les certifications. . .

4.2. **Firewalls** [16]

En informatique, un Firewall est un périphérique ou un ordinateur qui protège la partie privée d'un réseau de la partie publique. C'est en réalité l'élément qui permet de distinguer la partie privée du réseau de celle que l'on nommera publique (Internet,. . .), lui seul peut donc en atteindre les deux extrémités.

Il permet donc de protéger le réseau privé d'éventuelles attaques provenant d'Internet et peut également contrôler certaines actions effectuées de l'intérieur du réseau privé.

4.3. Cryptographie

Le but est de donner les grandes lignes des principaux algorithmes de cryptage, ainsi que de fournir un ordre d'idée sur leur niveaux de sécurité et leurs temps d'exécution. Nous pourrons ainsi effectuer une comparaison entre chacun d'eux en terme de coût machine et d'efficacité. La principale distinction se fera entre les codages de types symétriques et ceux de types asymétriques ou à clé privé.

IV. La cryptographie [19]

Quand Jules César envoyait des messages à ses généraux, il ne faisait pas confiance à ses messagers. Aussi remplaçait-il chaque A dans ses messages par un D, chaque B par un E, et ainsi de suite à travers l'alphabet. Seul quelqu'un qui connaissait la règle « décalé de 3 » pouvait déchiffrer ses messages.

1. Terminologie [20]

La cryptographie possède plusieurs éléments qui sont utilisées afin de mener á bien cette méthode de sécurité :

- *Texte clair* : le texte que l'on souhaite transmettre avant toute modification. Ca peut aussi bien être un texte dans une langue quelconque qu'une donnée autre (image, vidéo, son, ...).
- *Texte chiffré* : c'est le texte obtenu après avoir appliqué l'algorithme de chiffrement sur le texte clair.
- *Chiffre* : un chiffre est un algorithme permettant de substituer à chaque caractère du message clair un autre caractère.
- *Clef* : la clef est un paramètre permettant de calculer le message chiffré et/ou le message clair.

La terminologie de la cryptographie :

- ***Cryptanalyse*** : la Science permettant d'étudier les systèmes cryptographiques en vue de les tester ou de les casser.
- ***Cryptologie*** : la science qui regroupe la • Cryptologie : la science qui regroupe la cryptographie et la cryptanalyse.

2. Historique

La cryptographie a évolué en trois périodes historiques :

- La cryptographie mécanique. Il s'agit de la cryptographie qui utilise des moyens mécaniques pour chiffrer un message. Cette cryptographie s'étend de l'antiquité jusqu'à la fin de la seconde guerre mondiale environ. De nos jours, elle n'a plus cours.
- La cryptographie mathématique. Il s'agit de la cryptographie qui utilise les mathématiques pour chiffrer un message. Cette cryptographie a commencé aux environs de la fin de la deuxième guerre mondiale et c'est celle que l'on utilise de nos jours.
- La cryptographie quantique. Il s'agit de la cryptographie dont les bases reposent sur la physique quantique.

3. Qu’est-ce que la Cryptographie ?

La cryptographie traditionnelle est l’étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c’est ce qu’on appelle le chiffrement, qui, à partir d’un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l’action qui permet de reconstruire le texte en clair à partir du texte chiffré.
Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées algorithmes cryptographiques, qui dépendent d’un paramètre appelé clef.

4. Qu’est-ce que la cryptanalyse ?

À l’inverse de la cryptographie, la cryptanalyse est l’étude des procédés cryptographiques dans le but de trouver des faiblesses et, en particulier, de pouvoir décrypter des textes chiffrés. Le décryptement est l’action consistant à retrouver le texte en clair sans connaître la clef de déchiffrement.

5. Chiffrement et Déchiffrement

Les données qui peuvent être lues et comprises sans mesures spéciales sont appelées texte clair (ou libellé). Le procédé qui consiste à dissimuler du texte clair de façon à cacher sa substance est appelée chiffrement (dans le langage courant on parle plutôt de cryptage et de ses dérivés : crypter, décrypter). Chiffrer du texte clair produit un charabia illisible appelé texte chiffré (ou cryptogramme). Vous utilisez le chiffrement pour garantir que l’information est cachée à quiconque elle n’est destinée, même ceux qui peuvent lire les données chiffrées. Le processus de retour du texte chiffré à son texte clair original est appelé déchiffrement.

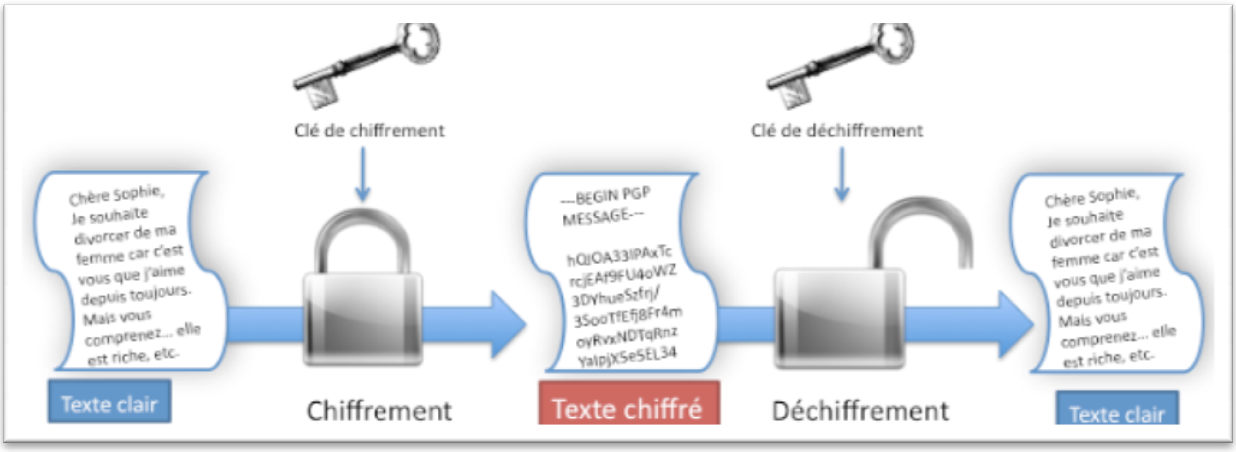


Figure 3 : Chiffrement et Déchiffrement

6. Cryptographie Symétrique

C'est le type le plus classique de cryptage. Le même mot de passe est utilisé pour crypter et décrypter le message. S'il existe plusieurs algorithmes différents, ceux que nous présentons ci-dessous sont considérés comme des standards car ils ont été révisés par la communauté internet internationale et que leurs forces et faiblesses sont bien documentées.
Il existe deux types de cryptographie symétrique :

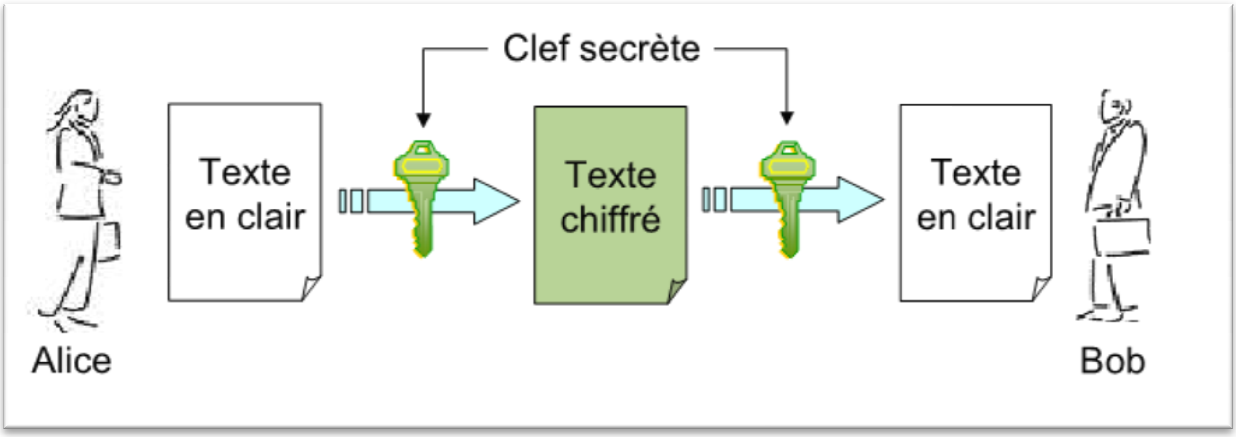


Figure 4 : Cryptographie symetrique

6.1. Le chiffrement par flot

Dans ce type de chiffrement, le cryptage est effectué bit-à-bit sans attendre la réception complète des données à crypter.

6.2. Le chiffrement par bloc

Quatre modes de chiffrement par bloc sont utilisés : Electronic CodeBook (ECB), Cipher Block Chaining (CBC), Cipher FeedBack (CFB) ou Output FeedBack (OFB).
Le cryptage en blocs est au contraire beaucoup plus utilisé et permet une meilleure sécurité. Les algorithmes concernés sont également plus connus DES, AES,…
Leur nom leur vient du fait qu'ils s'appliquent à des blocs de données et non à des flux de bits. Ces blocs sont habituellement de 64 bits mais cela dépend entièrement de l'algorithme utilisé et de son implémentation. De même, la taille de la clé varie suivant l'algorithme et suivant le niveau de sécurité requis.

- ***Avantage :***
  - Assure la confidentialité des données

- ***Inconvénients :***
  - Souffre d'un problème de distribution de clés
  - Problème de Gestion des clés.

6.3 Algorithmes de cryptage symétrique

6.3.1 DES (Data Encryption Standard)

6.3.1.1 Historique

Créé dans les années 70 (public en 1981), l'algorithme DES a été l'algorithme de cryptographie le plus usité jusqu'à ces dernières années. Il a été récertifié depuis et est encore aujourd'hui utilisé .Sa plus récente version date de 1994.

L'algorithme DES est un algorithme de cryptographie en bloc. Il opère généralement sur des blocs de *64 bits* et utilise une clé de *56 bits* qui sera transformée en 16 sous-clés de 48 bits chacune.

6.3.1.2 Performances

Au cours des 25 dernières années, l'algorithme DES s'est révélé être un algorithme solide. La seule attaque connue à ce jour est purement académique, et n'a aucune conséquence sur la sécurité pratique de l'algorithme. Malheureusement, sa faiblesse réside dans la longueur de sa clé, qui n'est que de 56 bits.

6.3.1.3 Modes d'utilisation

DES étant un algorithme de chiffrement par bloc, il peut être appliqué de plusieurs façons. En réalité, 4 modes d'utilisation de DES ont été proposés : ECB (Electronic CodeBook mode), CFB (Cipher FeedBack mode), CBC (Cipher Block Chaining mode) et OFB (Output FeedBack mode).

ECB correspond au mode le plus simple : étant donné un texte clair *x*1*x*2..., chaque bloc de 64 bits est chiffré avec l'algorithme DES, donnant un texte chiffré *y*1*y*2... Ce système présente un inconvénient flagrant : 2 blocs identiques seront codés de la même manière, et auront donc le même bloc chiffré. Il est donc possible de recenser tous les cryptés possibles puis par recoupements et analyses statistiques de recomposer une partie du message original sans avoir tenté de casser la clé de chiffrement.

Ces modes sont donc particulièrement adaptés au problèmes d'authentification et sont utilisés dans les MAC (Message Authentification Code). Un MAC est une section de message, ajoutée au texte clair (ou au texte chiffré), afin de garantir l'intégrité du message envoyé.

6.3.2 IDEA (International Data Encryption Algorithm)

6.3.1.1 Historique

Plus récent que le DES, l'IDEA, contrairement aux autres algorithmes de codage, a été breveté par la société suisse Ascom. L'utilisation non commerciale de cet algorithme, essentiellement utilisé dans le système PGP, est cependant permise sous réserve d'une autorisation d'Ascom.

L'IDEA opère sur des blocs de *64 bits* et utilise généralement une clé de *128 bits* qui sera transformée en 52 blocs de 16 bits.
Les algorithmes de cryptage et de décryptage sont les mêmes.
Le bloc d'entrée de 64 bits est divisé en 4 blocs de 16 bits A ,B, C, et D qui deviennent les blocs d'entrée de l'algorithme.

6.3.1.2 Performances

Cet algorithme est considéré comme étant assez nettement supérieur au DES en terme de sécurité. Sa vitesse d'exécution reste comparable avec le DES. Ses implémentations hardware sont simplement légèrement plus rapides.

6.3.3 Blowfish

6.3.1.1 Historique

Créé en 1994, Blowfish est un algorithme de chiffrement par blocs basé sur le DES, mais avec des clés plus longues et plus d'aléas lors du codage : on n'utilise plus des tables fixées, mais des tables à chaque fois différentes, déterminées par le mot-de-passe.

Blowfish effectue un codage par blocs de 64 bits, et utilise une clé de longueur variable.
L'algorithme est scindé en deux parties : une partie expansion de la clé et une partie encodage des données. La partie expansion de la clé consiste à convertir la clé de départ (maximum 448 bits) en plusieurs sous-clé totalisant 4168 bytes.
Le chiffrement des données s'effectue au cours de 16 itérations. Chacune d'elle est constituée d'une permutation dépendante de la clé, et d'une substitution dépendante de la clé et des données.
Toutes les opérations sont des Xor et des additions sur des mots de 32 bits.

6.3.1.2 Performances

Blowfish est un algorithme très performant en terme de sécurité en apparence, et très rapide. Il est encore relativement neuf et n'est pas très répandu. On manque donc d'information pour dire si cet algorithme est véritablement performant.

6.3.4 RC4

6.3.1.1 Historique

RC4 est un algorithme de chiffrement en continu à clé de longueur variable développé en 1987 par Ron Rivest pour RSA.
Il est longtemps resté secret avant d'être publié, et est maintenant beaucoup utilisé, en particulier dans le protocole SSL.
La structure du RC4 se compose de 2 parties distinctes.
La première, key scheduling algorithm, génère une table d'état *S* à partir des données secrètes, à savoir 64 bits.
La deuxième partie de l'algorithme RC4 est le générateur de données en sortie, qui utilise la table *S* et 2 compteurs, *i* et *j*.

6.3.1.2 Performances

Le chiffrement RC4 est extrêmement rapide, sûrement le plus rapide des chiffrements utilisés à l'heure actuelle.
Cependant, il comporte quelques failles de sécurité qui sont exploitables de façon plus efficace qu'une recherche exhaustive de clé.

6.4 Algorithmes de cryptage asymétrique

Le principe d'un code asymétrique (aussi appelé à clé publique) est que, contrairement au code symétrique, les deux interlocuteurs ne partagent pas la même clé. En effet, la personne qui veut envoyer un message utilise la clé publique de son correspondant. Celui-ci déchiffrera alors ce message à partir de sa clé privée que lui seul connait.

On voit ici que contrairement à un codage symétrique, le chiffrement et le déchiffrement se font par des opérations complètement différentes.

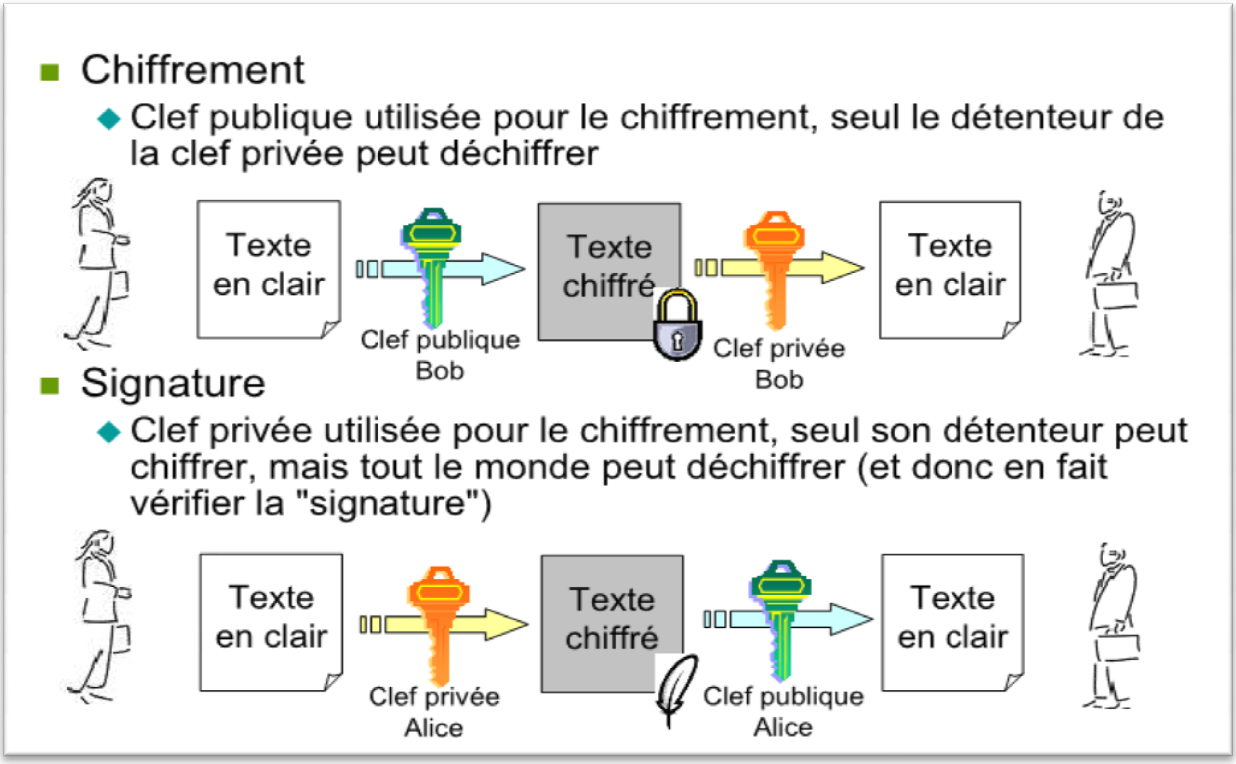


Figure 5 : Cryptographie asymetrique

6.4.1. RSA (Rivest-Shamir-Adleman)

6.4.1.1. Historique

R.S.A. signifie Rivest-Shamir-Adleman, en l'honneur de ses inventeurs : Ron Rivest, Adi Shamir et Leonard Adleman qui l'ont créé en 1977.

Tout le principe de RSA repose sur le fait qu'il est très difficile et donc très long de décomposer un très grand nombre en deux grands facteurs premiers, sauf cas particuliers.

6.4.1.2. Performances

La cryptographie à clé publique possède un avantage majeur sur la cryptographie à clé secrète.

Il est également à noter que la sécurité du cryptage RSA repose sur la puissance des ordinateurs et sur les connaissances actuelles en arithmétique. Tout progrès dans un domaine comme dans l'autre peut obliger à allonger la clé, ou à chercher une autre fonction qui soit facilement applicable dans un sens, et quasiment impraticable dans l'autre.

6.4.2. Systèmes de signature

Un codage asymétrique, quel qu'il soit, peut être très avantageux du fait que la clé privée ne soit détenue que par le receveur du message. Cela assure notamment que la clé privée ne puisse être divulguée, car elle n'est connue de personne d'autre que son utilisateur. Cependant, un problème apparaît rapidement : étant donné que la clé de chiffrement est publique, comment authentifier l'expéditeur. C'est là qu'intervient le système de signature. En effet, si la personne qui envoie le message y ajoute une signature qui lui est propre, il n'y a plus aucun doute sur son identité.

Dans la réalité, la plupart du temps, l'expéditeur chiffrera un nombre particulier d'une façon qui lui est propre, afin d'assurer le destinataire de l'intégrité du message qu'il reçoit, L'authentification d'un message, et la non-répudiation.
Les signatures électroniques sont obtenues par des fonctions de hachage.

- Des fonctions de hachage utilisées usuellement pour la signature sont :
  - → MD2 ;
  - → MD4 ;
  - → MD5 (128 bits) ;
  - → SHA ;
  - → SHA (160 bits).

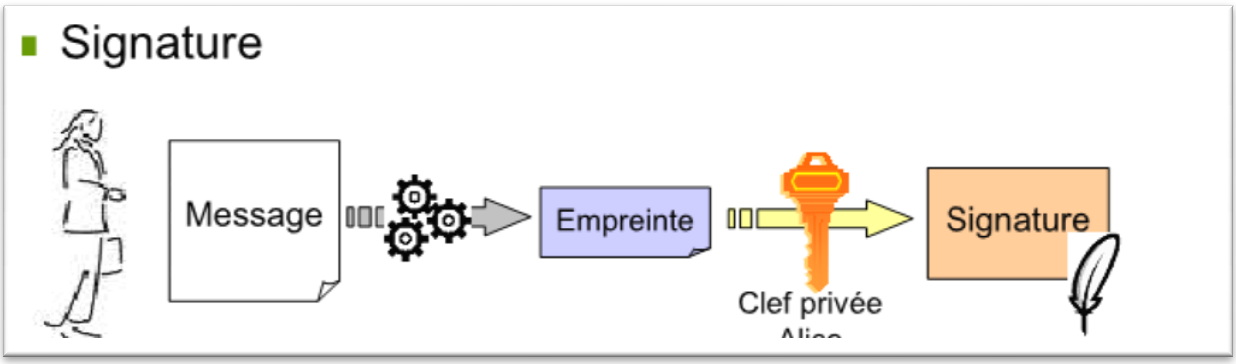


Figure 6 : Système de signature

7. Symétrique / Asymétrique : Petit Comparatif

D'après la section précédente on a déduit que la cryptographie à clé publique apportait une solution mais qui avait plus de tourments que la cryptographie à clé secrète.

En effet la cryptographie symétrique est utilisée pour deux raisons fondamentales,
D'une part, une raison pratique, la plupart des systèmes de chiffrement à clé publique sont très lents. Le RSA est par exemple plusieurs centaines de fois plus lent que l'AES en programmation logicielle et est complètement hors du coup en implantation matérielle.
A notre époque où la vitesse de transmission de l'information constitue un enjeu crucial, l'algorithme de chiffrement ne doit pas être un facteur limitant.
D'autre part, du point de vue de la sécurité se posent des problèmes relatifs à la structure même des systèmes de chiffrement à clé publique.

8. Sécurisation des applications

Divers types d'applications déployées en mode client-serveur á travers l'internet peuvent être sécurisées par l'emploi de systèmes cryptographiques symétrique ou asymétriques :

- → messagerie électronique.
- → Accès a des serveurs web.
- → Accès a des bases de données.

De nos jours, compte tenu de l'évolution historique de l'internet ,l'objectif est de sécuriser la vie privée des utilisateurs.

- Comparaison des forces relatives des algorithmes de cryptage -

Type	Degré de sécurité *	Implémentation	Vitesse
Idea	de type militaire	128 bit Secret partagé	Rapide
Blowfish	de type militaire	256 to 448 bit Secret partagé	Très rapide
DES	Bas	40 to 56 bit Secret partagé	Rapide
RSA	de type militaire	2048 bit Clé publique	Très lent
MD5	Elevé	128 bit Message Digest	Lent
SHA	Elevé	160 bit Message Digest	Lent

*** dépend de la longueur de la clé, évalué en fonction de la longueur maximale de la clé**

Tableau 4:Tableau comparatif d'algorithmes de cryptage

Une solution tout à fait intéressante et acceptable est le compromis élaboré par Zimmermann pour concevoir PGP.
Le principe du chiffrement est le suivant : supposons que l'émetteur A et le destinataire B souhaitent communiquer de manière intègre, en utilisant un algorithme à clé secrète (en l'occurrence, pour PGP, c'est l'algorithme IDEA). Ils se mettent d'accord sur la clé secrète par un protocole d'échange de clés. Ce genre de protocole utilise des propriétés de cryptographie à clé publique.

Ensuite ils communiquent en utilisant l'algorithme IDEA qui est à clé privée. Une fois que leur conversation est terminée, ils jettent la clé de session.
La même façon de procéder peut être utilisée avec un codage AES, au lieu d'un codage IDEA.

Un tel système combine alors les avantages des deux types de cryptographie : non partage des clés et intégrité des messages, ainsi que rapidité et sécurité d'exécution.

Après la présentation de ces différents algorithmes de codage, nous pouvons dire qu'il est nécessaire de distinguer les deux cas symétriques et asymétriques. En effet, chacun d'eux a ses particularités et n'auront pas les mêmes applications.
Dans les cas où les deux interlocuteurs sont sûrs, il est préférable d'utiliser un chiffrement symétrique. Parmi les chiffrements symétriques, le chiffrement *AES*, très récent, s'avère être le plus efficace. Il est d'ailleurs très employé depuis son officialisation.
Dans le cas où il est préférable que les deux interlocuteurs ne possèdent pas la même clé, pour quelque raison que se soit, un codage asymétrique comme le *RSA* s'avère plus approprié.

IV. Introduction à la sécurité dans les réseaux sociaux

Dans une société comme la notre, où l'accès à Internet est facile et où l'information est diffusée 24H/24, où les communications sont instantanées, les relations sociales pâtissent souvent de l'attrait pour les technologies. Les mises en garde sont en effet nombreuses contre l'adoption des nouvelles technologies qui risquent d'empiéter sur la vie privée et de réduire encore plus notre attention.

De nombreux habitués d'Internet sont conscients de la dépendance que crée la toile et de l'anxiété que peut générer l'usage des réseaux sociaux : la crainte par exemple de passer à côté de mises à jour essentielles.

Mais les internautes ignorent encore les règles élémentaires de sécurité.

Une enquête commandée par ESET révèle un gouffre entre les préoccupations des utilisateurs de réseaux sociaux et leurs comportements.

1. Qu’est ce que ESET ? [21]

Fondée en 1992, la société ESET est spécialisée dans la conception et le développement de logiciels de sécurité offrant une protection globale contre les menaces évolutives qui sévissent dans les environnements informatiques.
Pionnier en matière de détection proactive des menaces, ESET est aujourd'hui le leader dans ce domaine.
ESET a développé un vaste réseau mondial de partenariats, y compris avec des entreprises telles que Canon, Dell et Microsoft.
ESET possède des bureaux à Bratislava (Slovaquie), Bristol (Royaume-Unis), Buenos Aires(Argentine), San Diego (USA), Prague (République Tchèque), et est représentée dans plus de 110 pays.

2. Etude menée [21]

Alors que le débat sur la sécurité des réseaux sociaux bat son plein, ESET, a demandé à Harris Interactive, institut d’études de marché, d’interroger un échantillon représentatif d’américains

de plus de 18 ans, dont 1476 possèdent des comptes de réseaux sociaux afin de connaitre leur option sur la sécurité d'Internet et les conséquences que peuvent avoir leurs comportements.

Le résultat souligne un étonnant décalage entre les préoccupations des utilisateurs concernant la confidentialité, la sécurité et leurs actions sur les sites de réseaux sociaux.

- **Quand avez-vous changé le mot de passe de votre compte de réseau social pour la dernière fois ?**

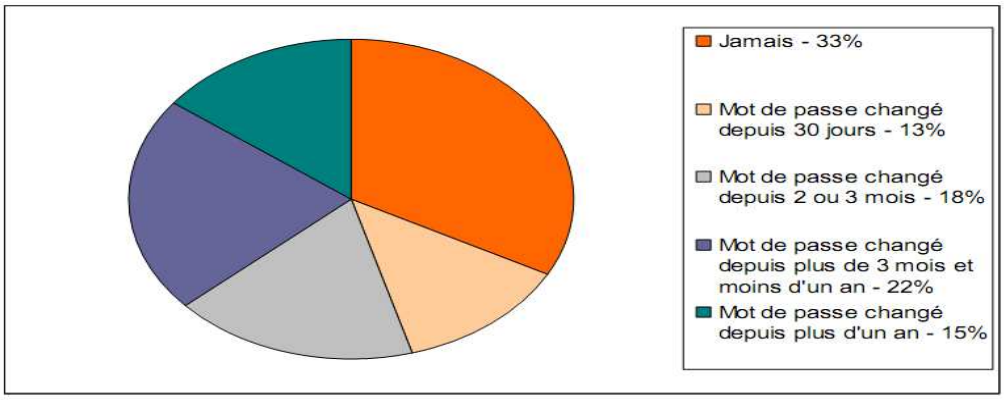


Figure 7: Cendage sur la date de modification du mot de passe dans un réseau social

L'étude révéle ainsi que 69% des utilisateurs de réseaux sociaux sont sensibles à la sécurité de ces sites, même si un tiers d'entre eux n'a jamais changé de mot de passe et que 15% l'ont modifié depuis un an.

De plus, un utilisateur sur dix a signalé que certains internautes avaient accédé à leur compte, sans autorisation, pour diffuser des liens malveillants et des commentaires malsains.

Ceci est d'autant plus inquiétant que l'accès non autorisé peut menacer la sécurité des données du titulaire du compte ainsi que celle de ses contacts.

- **En général, combien de fois mettez-vous à jour vos paramètres de confidentialité sur vos comptes de réseaux sociaux ?**

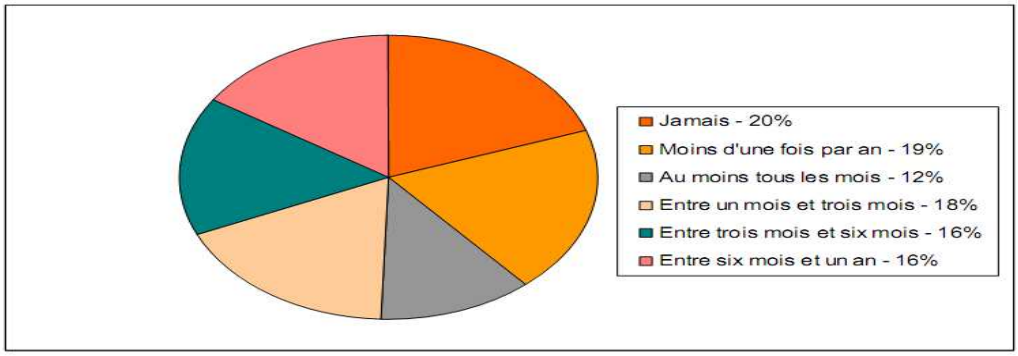


Figure 8: Cendage sur la mise à jour des paramètres de confidentialités

Le sondage dévoile également que 67% des utilisateurs de sites de socialisation sont soucieux de contrôler au mieux la confidentialité de leurs informations personnelles, et pourtant seulement 55% d'entre eux mettent à jour les paramètres de confidentialités moins d'une fois tous les six mois, voire jamais.

- **Quelqu'un a-t-il eu un accès non autorisé sur votre compte de réseau social pour diffuser des liens et des commentaires ?**

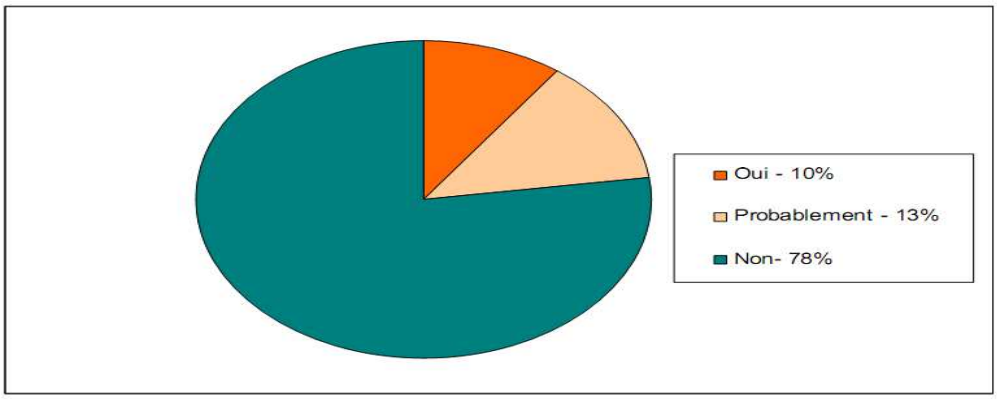


Figure 9: Cendage sur les accès non autorisé dans un réseau social

D'autres éléments tous aussi importants sont apparus lors de cette enquête :

- 37% des internautes craignent qu'un internaute vole et usurpe leur identité en ligne ;
- 95% des internautes acceptent parfois ou toujours toute demande de connexion provenant d'un ami ou d'un contact ;
- 71% des internautes appréhendent que leurs informations personnelles saisies sur les sites de réseaux sociaux soient vendues ou partagées à leur insu ;
- 17% s'inquiètent de l'utilisation des sites de réseaux sociaux pour leurs enfants.

- Parmi ces énoncés sur les réseaux sociaux, lesquels vous préoccupent le plus ?

Réponses multiples possibles.

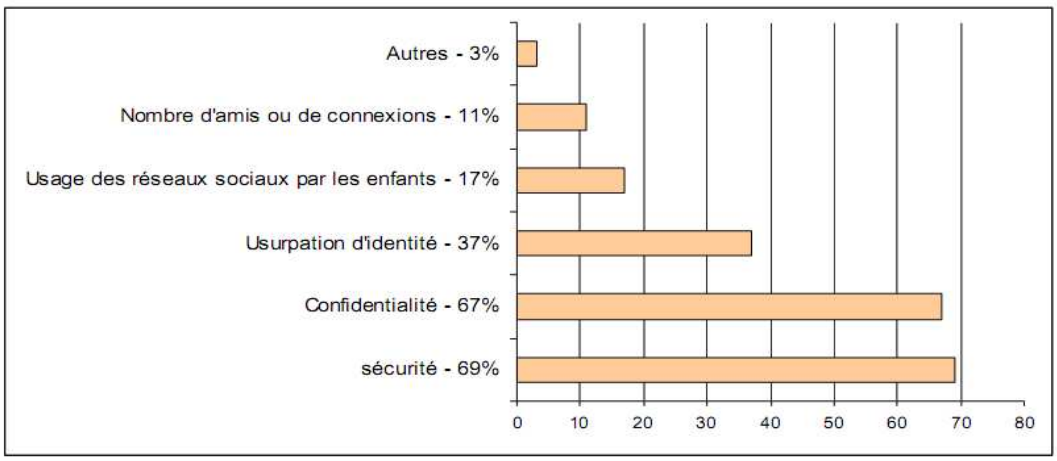


Figure 10: Cendage sur les risques qui préoccupent le plus les utilisateurs des réseaux sociaux

De nombreux utilisateurs estiment qu'il est difficile de contrôler la sécurité des réseaux sociaux et leur vie privée, et tout cela commence par leur profil d'utilisateur qui offre un accès direct à leurs informations.

Remarque :
Cette enquête a été menée en ligne aux Etats-Unis par Harris Interactive pour le compte d'ESET du 31 mai au 2 juin 2011 parmi 2027 adultes âgés de 18 ans et plus, dont 1476 ont des comptes de réseaux sociaux.

3. Qu'est ce qu'un profil utilisateur [22]

Définition 1 : **« Un profil utilisateur** est une source de connaissance qui contient des acquisitions sur tous les aspects de l'utilisateur qui peuvent être utiles pour le comportement du système. Le profil est souvent renseigné par l'utilisateur lui-même.

Outre les informations d'identification de base telles que l'identifiant ou l'état civil, le profil peut regrouper des informations très diverses selon les besoins. »

Définition 2 : Le profil utilisateur est un ensemble de données que l'on est obligé d'indiquer pour pouvoir utiliser des services proposés en ligne comme de disposer de pages web personnelles permettant de poster des articles, des messages, des commentaires, des images, des vidéos,... tout en créant un réseau de contacts.

Les profils utilisateurs sont utilisés en informatique dans de nombreux domaines. Ils permettent de fournir des services personnalisés, des offres adaptées, ...

- ✓ Systèmes d'exploitation où il s'agit typiquement du compte utilisateur,
- ✓ Logiciels, en général pour stocker les préférences en bureautique, dans les systèmes d'apprentissage, ...
- ✓ Applications web, comme le compte personnel sur un site web
- ✓ Filtrage, comme dans les moteurs de recherche ou les journaux personnalisés

On peut non seulement proposer des adaptations à l'individu de par son profil, mais aussi faire bénéficier le groupe des informations individuelles et vice-versa.

Avoir des profils en ligne implique de fait une « cyber » activité de dépôt et de partage d'informations personnelles et professionnelles, le tout constituant les traces « bâtisseuses » d'une identité numérique.

On se crée des profils sans cesse au cours de nos navigations web et particulièrement sur les réseaux sociaux.

Nous sommes donc visibles de nos proches, famille, amis, connaissances et aussi du monde entier.

La création d'un profil n'est pas un geste anodin. Elle nécessite réflexion et vigilance notamment pour des sites de partages et d'échanges d'informations.

Les réseaux sociaux constituent un véritable phénomène de société et une véritable manière de communiquer. Les possibilités sont gigantesques de dépôt et partage de photos aux jeux collaboratifs, en passant par l'organisation de soirées ou le lancement d'une action de solidarité, s'exprimer et créer, maintenir des relations ou s'informer.

Le revers de la médaille, pour être utile, le réseau social doit stocker le plus possible d'informations personnelles, professionnelles voire confidentielles.

Mais chaque utilisateur doit être vigilant en ce qui concerne son profil et les informations qu'il fournit ainsi qu'aux différentes manières des les sécurisées.

4. Risques pour l'utilisateur [23]

- ➢ *Publication d'informations privées*

Sur leurs profils, les utilisateurs de réseaux sociaux peuvent indiquer leurs adresses de courrier électronique, leurs numéros de téléphone, leurs loisirs, leurs préférences et autres informations personnelles.

Ces données peuvent être exploitées par des entreprises pour bombarder les utilisateurs de publicité ciblée.

À l'ouverture du compte, les paramètres de confidentialité standard ne sont pas suffisants et l'ensemble des données peut être visualisé par tous les utilisateurs du réseau social.

Certains passages des profils peuvent même être partiellement retrouvés par des moteurs de recherche, ce qui les rend accessibles à tous les internautes du monde entier.

Informations, textes et en particulier photos sont souvent archivés par les utilisateurs en dehors des réseaux sociaux sur leurs propres ordinateurs. De cette manière, les données peuvent à tout moment apparaître sur d'autres pages Web ou être exploitées à d'autres fins, même après avoir été supprimé du profil.

- *Vol d'identité*

Les cybers pirates tentent de plus en plus de craquer des comptes utilisateurs pour commettre leurs méfaits sous l'identité de quelqu'un d'autre.

Une fois qu'ils ont pris possession d'un compte, ils mettent souvent en scène une situation d'urgence et demandent aux amis du réseau de les aider financièrement.

Les informations lues en accédant au profil de l'utilisateur peuvent les aider à renforcer leur crédibilité et à tromper les amis.

De faux profils sont de plus en plus utilisés à des fins malfaisantes : les voleurs peuvent par exemple apprendre quand quelqu'un part en vacances et laisse ainsi son appartement sans surveillance.

- *Diffusion des logiciels malveillants*

Les utilisateurs font preuve en général d'une grande confiance à l'égard des réseaux sociaux. Les cybers pirates ont donc eu l'idée d'y transposer un bon vieux truc : en postant des messages contenant un lien renvoyant à des sites Web piratés, ils contribuent à la diffusion de logiciels malveillants.

Certains réseaux sociaux offrent des applications supplémentaires que les utilisateurs peuvent ajouter à leur profil.

C'est le cas par exemple des mini-jeux auxquels les utilisateurs peuvent jouer en réseau. Mais le problème est que ces applications proviennent de fournisseurs tiers dont les standards de sécurité ne correspondent pas nécessairement à ceux des réseaux sociaux.

De cette manière, les maliciels peuvent de façon volontaire ou non se diffuser parmi la communauté d'utilisateurs.

- *Mobbing (harcèlement)*

Avec les réseaux sociaux, le harcèlement ou mobbing prend une nouvelle dimension.

Des personnes peuvent par exemple être volontairement exclues de groupes d'amis ou voir leurs murs couverts d'insultes.

Ce phénomène peut devenir un véritable tourment, tout particulièrement pour les jeunes.

Le harcèlement est passible de sanctions.

On se lie plus rapidement d'amitié dans les réseaux sociaux que dans le monde « réel ». Ainsi, des informations parviennent à des personnes auxquelles elles n'auraient peut-être jamais été confiées.

Une personne malintentionnée peut mettre à profit ces informations pour compromettre quelqu'un ou manigancer contre lui.

Les « cyber harceleurs » peuvent également se créer de faux profils où ils se font passer pour une autre personne, réelle ou fictive.

De cette manière, ils peuvent, dans le plus parfait des anonymats, harceler d'autres personnes à travers le réseau social.

Même si les réseaux sociaux sont l'endroit idéal pour rencontrer d'autres internautes, ils représentent un réel danger : voleurs d'identités, fraudeurs… y sont bel et bien présents. Les réseaux sociaux nous amène à penser identité numérique (profil utilisateur) et la question que l'on peut se poser est : quel sera l'usage des données que nous inscrivons dans ces réseaux ?

Dans la « vraie vie », les sphères personnelles, familiales, professionnelles, amicales, institutionnelles… se croisent et se complètent afin de définir notre identité. Et donc, selon la sphère dans laquelle nous nous trouvons, nous ne partageons pas les mêmes informations et nous ne réagissons pas de la même manière vis-à-vis des membres qui la compose. Aujourd'hui, les sites de réseaux sociaux ne proposent pas de possibilités de filtrage qui permettrait de structurer et de spécialiser les réseaux sociaux selon les sphères de connaissance.

La notion de confiance est également un souci. Il n'est pas dit que les internautes inscrits sur un réseau social se sentent plus proches d'un autre membre du même réseau que d'un parfait inconnu, ce qui améliore a priori la qualité des échanges entre eux. C'est un discours de marchand…
En effet, les algorithmes de confiance et d'anonymisation sont très discutés
Comment peut-on avoir la certitude que l'«ami» de mon contact est véritablement son «ami» !
Peut-on faire confiance dans la réponse de telle personne ?

Chapitre 3

Sécurité dans les réseaux sociaux

Plusieurs centaines de millions de personnes utilisent actuellement les réseaux sociaux pour communiquer.

Même dans le milieu professionnel, ils commencent à gagner du terrain. D'après un responsable, deux personnes sur dix laisseront tomber les courriers électroniques au profit des réseaux sociaux d'ici 2014.

Mais l'engouement des usagers pour cet outil de communication commence à poser des risques sérieux concernant la sécurité.

I. Que faut-il savoir sur la sécurité des réseaux sociaux ?

1. Réseaux sociaux présentant des risques pour la sécurité [24]

Toutes les applications sociales ne présentent pas des risques similaires en termes de sécurité, loin de là.

Si l'essor de l'usage du réseau social *Facebook* dans la sphère de l'entreprise ne se dément pas, il n'en reste pas moins l'un des vecteurs de risque les plus élevés pour la sécurité, pour 39% des répondants.
Juste derrière, on retrouve les outils de *microblogging***,** au premier rang desquels *Twitter* (35%), suivi par les blogs (30%).
A noter que les podcasts vidéo ainsi que *YouTube* sont loin d'apparaître comme des vecteurs de risque mettant à mal la sécurité.
Pour autant, ce n'est pas parce qu'ils sont ressentis comme tel que leur potentiel de danger est moins élevé que les autres.

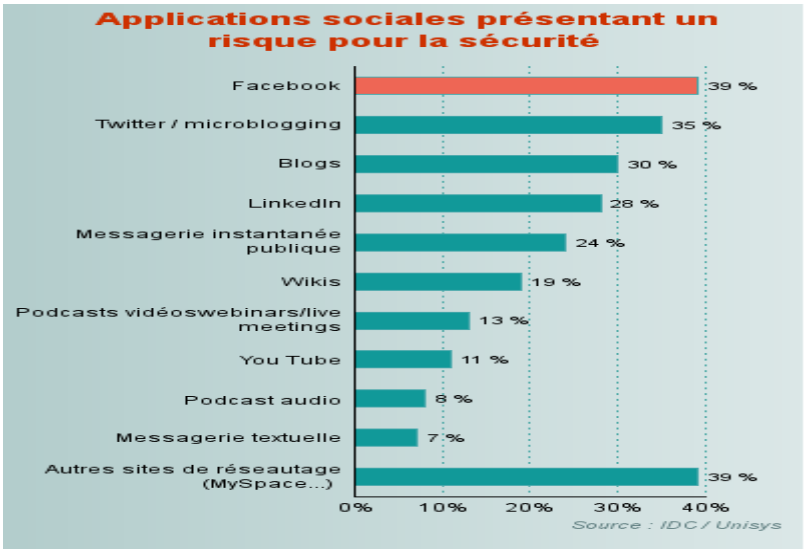


Figure 1 : Degré de manque de sécurité dans les réseaux sociaux

2. Quels sont les risques ?

Les sites tels que : Twitter, Windows Live Messenger, You Tube et encore Facebook sont des outils puissants permettant de se rencontrer, interagir et partager avec des personnes sur toute la planète. Pourtant, toutes ces possibilités amènent un risque considérable, pas uniquement pour vous mais également pour votre employeur, famille et amis.
Nous vous présenterons dans cette partie quels sont ces dangers ?

Une préoccupation commune liée à l'utilisation des réseaux sociaux concerne le respect de la vie privée, et le risque que vous ou des tiers partage trop d'information vous concernant. Ces dangers inclus :

- ➔ **Dommages sur votre carrière**: Des informations embarrassantes peuvent mettre en danger votre carrière.
  Dans leur processus de recrutement, beaucoup d'organisations font des recherches sur les sites de réseaux sociaux, afin de vérifier ce qui a été publié sur vous. Toute information embarrassante ou incriminante, peu importe la date de publication, peut vous empêcher de décrocher ce nouvel emploi. Cette pratique est également en vigueur dans de nombreuses universités pour les candidatures des nouveaux étudiants.

- ➔ **Attaques contre votre personne**: Les cybercriminels, peuvent chercher des informations et les utiliser contre vous. Par exemple, ils peuvent chercher des informations personnelles afin de deviner votre « question secrète » que les sites internet utilisent pour vous renvoyer votre mot de passe en cas de perte ou utiliser ces informations afin de faire une demande de carte de crédit sous votre nom.

- ➔ **Attaques contre votre employeur**: Des criminels pourraient utiliser les informations que vous publiez, afin de récupérer des informations permettant un avantage concurrentiel ou de préparer une cyber attaque contre votre employeur. De plus, vos actions en ligne peuvent donner une mauvaise image de votre employeur. Consultez la politique d'entreprise concernant l'utilisation des réseaux sociaux, afin de connaître la ligne de conduite à tenir pour protéger la réputation et les données de votre entreprise.

La meilleure façon de se protéger contre ces dangers est d'être prudent quant aux informations que vous publiez vous concernant. Evaluez si les données que vous partagez aujourd'hui pourraient être utilisées contre vous ultérieurement. Egalement, renforcer les paramètres de confidentialité sur votre profil de réseau social pour limiter l'accès aux informations personnelles que vous partagez.
Gardez à l'esprit que vos données peuvent être transmises par inadvertance par le site internet ou par vos amis, ainsi il est préférable de considérer toutes les informations publiées comme publiques. Soyez également attentifs aux publications d'autres personnes vous concernant. Si

certains de vos amis publient des informations, images ou toutes autres données que vous ne souhaitez pas rendre publique, demandez leurs de les supprimer.

3. Exemples de failles dans les réseaux sociaux

Les réseaux sociaux, n'ont pas fait apparaître de nouvelles menaces. Les pirates se contentent d'appliquer sur ces services des techniques existantes.

a. Twitter part en vrille [25]

Twitter part en live. Des dizaines de milliers d'adeptes du service de micro-blogging sont victimes depuis la fin de matinée d'une faille de sécurité du siteTwitter.com. Même la femme de l'ex-premier ministre anglais, Sarah Brown, s'est retrouvée à pointer vers un site japonais sans le vouloir. Il semblerait également qu'une mode, on l'espère passagère, des tweets arcen-ciel (what does it mean ?) permettant de poster des blocs de couleurs à la place des micromessages (à l'aide de codes à poster) ne soit pas pour rien dans l'histoire.

Plus concrètement, la faille pouvait également faire apparaître, selon les navigateurs, des suites de tweets ésotériques :

Figure 2 : Capture d'écran de Twitter

La faille porte le joli nom de « faille d'injection XSS ». Les messages porteurs du parasite s'affiche à l'insu des titulaires de compte sous la forme de signes incompréhensibles pour le commun des twittos mais qui sont en fait un morceau de code javascript, destiné à agir à l'insu des utilisateurs. Le simple affichage d'un message vérolé à l'écran -ou le fait de passer sa souris dessus- et voilà que vous vous retrouvez à « re-tweeter » le parasite. Selon les variantes, une fenêtre s'affiche à l'écran ou des bandes de couleur barrent le site de Twitter sur l'écran.

b. Facebook corrige une importante faille de sécurité [26]

Facebook a confirmé avoir corrigé une importante faille de sécurité, qui laissait fuiter des données confidentielles à des tiers.
Découverte par l'entreprise de sécurité informatique *Symantec*, le problème touchait le fonctionnement des applications pour le réseau social, ces petits programmes de

jeux ou de services qui s'intègrent aux pages facebook et utilisent le système d'authentification du réseau. Lorsqu'un utilisateur se connecte à une application, il permet à ce programme de créer un "token", l'équivalent numérique d'une clef de rechange, qui évite à l'utilisateur de devoir s'authentifier en permanence.

Or, pour les applications qui n'utilisent pas les protocoles les plus récents et les plus sécurisés, cette clef de rechange peut être déchiffrée par un tiers.

Environ 100 000 applications seraient concernées, selon les calculs de *Symantec*.

"Une personne qui a accès à ces informations a potentiellement accès à l'ensemble du compte de l'utilisateur, détaille Laurent Heslault, responsable technologie Europe de l'éditeur d'antivirus. Ces informations ne sont cependant pas si simples à exploiter de manière automatique sur une grande échelle, et il n'y a pas eu d'indication qu'elles aient pu être exploitées."

4. Comment mieux se protéger ?

En plus d'être l'origine de fuites d'informations nuisibles, les sites de réseaux sociaux peuvent être utilisés comme plateforme d'attaque contre votre système ou pour mener des escroqueries. Voici quelques étapes à suivre afin de vous protéger.

- ➔ **Ouverture de session**: Protégez votre compte de réseau social avec un mot de passe fort. Ne jamais partager ce mot de passe avec quiconque ni l'utiliser pour d'autres sites. De plus, certains sites de réseaux sociaux, comme Facebook ou Google+, supportent l'authentification forte avec l'utilisation de fonctions de mot de passe à usage unique (« One-time Password ») lors de connexions depuis des ordinateurs publiques ou l'utilisation de votre téléphone mobile comme élément du processus d'authentification. Activez ces fonctions lorsque cela est possible.

- ➔ **Chiffrement**: De nombreux sites comme Facebook, Google+ ou Twitter vous permettent de forcer le chiffrement de toutes les communications (appelé HTTPS). Si cela est possible, activez cette option.

- ➔ **Messages électroniques**: Soyez vigilants lors que vous cliquez sur des liens contenus dans des messages électroniques prétendants provenir d'un site de réseau social.

Accédez plutôt au site en question en utilisant les favoris de votre navigateur, puis contrôlez vos messages ou notifications en utilisant directement le site internet.

- **Liens**: Faites attention avant de cliquer sur les liens postés sur les murs des internautes ou sur leurs pages publiques. Les virus et vers se propagent facilement sur ce genre de sites. Si un lien vous semble étrange, suspect ou trop beau pour être vrai, ne cliquez pas dessus! et cela même si ce lien se trouve sur la page de l'ami en qui vous avez la plus grande confiance. Les comptes de vos amis ont pu être détournés ou infectés et pourraient propager des logiciels malveillants.

- **Arnaques**: Les criminels profitent du caractère libre et ouvert des sites de réseaux sociaux afin d'escroquer les particuliers. De telles arnaques utilisent parfois comme prétexte des offres d'emploi ou d'argent trop belles pour être vraies. Une autre arnaque populaire consiste à utiliser des comptes piratés dans le but de demander de l'aide aux amis de la victime, en prétendant que la personne s'est faite dévalisée dans un pays étranger et a besoin d'argent. Faites attention lorsqu'un amis ou un étranger vous contact sur un réseau social en vous demandant de l'argent ou vous offrant quelque chose d'étonnamment bon.

- **Applications**: Certains sites de réseaux sociaux vous permettent d'ajouter ou d'installer des applications d'une tierce partie comme des jeux. Gardez à l'esprit que très peu (voir aucun) contrôles de qualité sont effectués sur ces applications et qu'elles peuvent avoir un accès complet à votre compte ainsi qu'aux données que vous partagez.
  Des applications malveillantes peuvent utiliser cet accès dans le but d'interagir avec vos amis en votre nom et ainsi voler ou utiliser des données personnelles. Soyez attentifs et installez uniquement les applications provenant de sites connus, assurez-vous également qu'après installation elles soient régulièrement mises à jour. Lorsque vous n'utilisez plus l'application, supprimez-la.

Les sites de réseaux sociaux sont des outils puissants et amusants, ils vous permettent de communiquer avec le monde entier.
Si vous suivez les conseils ci-dessus, vous devriez être en mesure de profiter d'une expérience en ligne beaucoup plus sûre.

4.1. Comment protéger son compte facebook ?

Les problèmes de sécurité sur Facebook sont légion. Vie privée dévoilée, cambriolages en raison de statuts trop précis... Autant de risques qui poussent à la paranoïa et méritent que l'on se penche sur les paramètres de confidentialité du célèbre réseau social. Messages, Applications, Amis autorisés, localisation, photos, mur, coordonnées...

Contrairement à la majeure partie des réseaux sociaux, facebook propose plusieurs façons de sécuriser son profil et donc ses données. Informations personnelles, photos, publications, et

amis peuvent être rendus « privés » à l'aide de quelques manipulations assez simple mais pas nécessairement connues de tous.
Voici 10 règles pour sécuriser son Facebook :

4.1.1. Les « Poke », messages et requêtes d'amis

Certains trouveront cela anodin, mais les célèbres « Poke » peuvent à eux seuls être considérés comme une menace par leurs utilisateurs. En effet, lorsque vous contactez quelqu'un sur Facebook via un Poke, cela s'assimile à un message ou à une requête d'ami. Résultat, le destinataire peut voir votre profil temporairement et cela même si vos autres paramètres de confidentialité sont sensés l'en empêcher. En conséquence, si un pirate qui souhaite dérober l'identité d'un utilisateur lui envoie un poke, un message ou une requête d'ami, et si celui-ci répond par exemple « Est-ce que je vous connais ? ». Pour se protéger, mieux vaut ne pas toujours répondre...

4.1.2. Les applications

Facebook a introduit les applications tierces à son interface. Divertissant, mais aussi une formidable opportunité pour les amateurs de données non protégées. Si le réseau social a publié ses conditions d'utilisation pour informer les développeurs de ce qui est accepté, le risque reste néanmoins présent. Ainsi par défaut, certaines applications ont accès à vos informations plus que privées. Sur cette capture, une application de téléchargement de photos pour facebook demande l'accès obligatoire aux « Informations familiales et de situation amoureuse ». Sans parler des informations de vos amis. Notre conseil : vérifier régulièrement les applications acceptées par facebook, et personnaliser les paramètres de confidentialité pour chacune d'elles.

4.1.3. Les amis autorisés

Aussi banal et paranoïaque que cela puisse paraître, dès que vous acceptez quelqu'un comme ami sur facebook, cette personne peut accéder à toutes les informations vous concernant. Les photos font également partie de ce cas, et vos photos de vacances sont donc accessibles au premier quidam que vous accepterez en ami sur facebook.

Si vous souhaitez limiter certaines de vos publications sans supprimer des amis, il suffit de créer des listes d'amis thématiques.
Exemple : bureau, famille, école, etc. Attribuez ensuite à chaque liste les paramètres que vous souhaitez : bloquez par exemple l'accès à vos photos de vacances ou votre dernière beuverie à vos collègues de bureau. Pensez également à personnaliser l'accès à votre liste d'amis.
N'autorisez pas les gens qui ne sont pas encore vos amis à consulter votre liste d'amis en désactivant cette option.

4.1.4. La localisation

Il y a des milliers d'utilisations différentes de facebook.

C'est pour cette raison que les paramètres par défaut, dont les options, ne sont adaptés à aucun profil. Pour cette raison, mieux vaut désactiver toutes les options facultatives ou qui ne vous concernent pas, quitte à les réactiver et à les personnaliser ultérieurement.
Un exemple : la localisation. Une option qui pourra en amuser certains ou coûter cher à d'autres.
Bien entendu il est tentant de préciser que l'on est au concert de tel artiste avec ses amis, ou bien à la plage à l'autre bout du monde. Sauf que cela pourrait laisser tout loisir à d'éventuels cambrioleurs, par exemple, pour vider votre logement.
Cela reste une simulation, mais le phénomène n'est pas rare et mérite de ne pas être négligé.
Un conseil : assurez-vous que votre localisation sur facebook ne comporte aucun risque avant de communiquer votre position.

4.1.5. Les photos

Au même titre que les autres informations publiées, les photos postées sur facebook peuvent représenter une source potentielle de risque. L'exemple le plus célèbre reste cette personne ayant posté des photos d'elle en vacances, après avoir déclaré être en congé maladie. Un patron trop curieux, un collègue jaloux et une situation d'apparence anodine peut vite se retourner contre vous.

Bien entendu, il s'agit de modifier les paramètres de confidentialité des photos pour ne les rendre visibles que par vos amis, au minimum.

Idem pour chaque album créé. Autre point non négligeable, le « Tag » sur les photos. La dernière version des profils de facebook affiche une liste de photos de vous récemment marquées. Vérifiez donc les autorisations que vous avez délivré pour être identifié sur certaines photos de vous.

4.1.6. La recherche

Le premier degré de sécurité sur facebook réside en la recherche.

Plus votre profil est ouvert, plus il est facile à trouver et donc vulnérable.
Tout d'abord il existe trois options quand à la recherche sur le réseau social :

- ✓ « Tout le monde »,
- ✓ « Amis et leurs amis »
- ✓ « Amis seulement ».

Pensez qu'il suffit d'un seul de vos contacts qui accepte n'importe qui pour qu'il y ait un risque. Mieux vaut cocher la troisième possibilité.
Idem pour les invitations, les messages : ne laissez qu'un cercle restreint (Amis et leurs amis) accéder à ses informations, cela vous évitera toute mauvaise surprise.

Pour rappel, consulter la page facebook d'un candidat est désormais une pratique courante pour un responsable des ressources humaines avant un entretien.

4.1.7. Le mur

Par défaut, quasiment toute activité sera publiée sur votre mur : tel commentaire sur une publication d'un ami, tel « tag » sur une photo ...

Quatre possibilités existent :

- ✓ Les amis seulement,
- ✓ Amis de leurs amis,
- ✓ Certaines personnes,
- ✓ Uniquement l'utilisateur.

Cette dernière option n'a pas grand intérêt, en revanche sélectionner manuellement les personnes qui peuvent accéder à votre mur peut être pertinent. Vous pouvez ainsi écarter les collègues de votre mur, pour éviter qu'ils épient et remontent toute votre activité par exemple. Plus simplement, vous pouvez interdire l'accès à votre mur manuellement à certaines personnes.

4.1.8. Les coordonnées

Encore une partie qui peut paraître anodine, mais facebook n'est pas un carnet d'adresse. Dites vous que si vos amis ont besoin de vous joindre, ils ont bien d'autres moyen de vous joindre.

Nul besoin de laisser votre adresse postale, votre numéro de portable ou toute autre information privée.
Sur l'onglet « Coordonnées », il est donc conseillé de sélectionner « Personne ».
Laissez le strict minimum en termes de coordonnées sur votre profil.
Au pire, votre interlocuteur vous envoie un message pour vous demander vos coordonnées, vous vous répondrez en privé.

4.1.9. Publicités

Dernier point qui vous rend vulnérable sur facebook : les publicités.

Dans la dernière version des paramètres de confidentialité du réseau social, un onglet spécifique y a été consacré. Autant y consacrer cinq minutes si vous ne souhaitez pas voir votre photo ni votre nom accolé à une photo de sushi, avec la mention « Untel a aimé ça ».
Dans « Paramètres du compte », « Publicités facebook », cochez « Personne » sur les deux seuls onglets de la page. Pensez à bien enregistrer les modifications.

4.1.10. Vérifier régulièrement l'état de sa confidentialité

Plusieurs outils existent pour consulter le degré de confidentialité de votre profil.

Nul besoin d'installer un quelconque outil, certains sites font ça de façon tout à fait efficace, gratuitement et cela en quelques secondes.
Profilewatch.org par exemple, analysera votre profil rapidement.
Dans cet exemple, nous avons obtenu la note maximale de 10/10, en montrant bien qu'aucune information n'est publiquement visible.

Enfin, si vous consultez facebook depuis un ordinateur qui n'est pas votre outil personnel, pensez à demander à votre navigateur de ne pas enregistrer vos coordonnées et à vous déconnecter après chaque passage sur le site. Sans quoi quelconque collègue utilisant ce même poste pourra consulter votre liste d'amis par exemple.

4.2.Comment protéger son compte Twitter

4.2.1. Politique de Confidentialité de Twitter

Cette politique de confidentialité décrit les politiques et procédures de Twitter sur la collecte, l'utilisation et la divulgation de vos informations.

Twitter reçoit vos informations à travers différents sites web, SMS, API, applications, services et des tiers (les «Services»).

Lorsque vous utilisez un l'un des Services proposés par Twitter, vous consentez à la récupération, le transfert, la manipulation, le stockage, la divulgation entre autres utilisations de vos informations comme décrit dans cette politique de confidentialité.
Indépendamment du pays dans lequel vous résidez ou créez vos informations, celles-ci pourront être utilisées par Twitter aux États-Unis ou dans tout autre pays où Twitter est disponible.

4.2.2. Collecte et Utilisation de Données [27]

- **Informations recueillies à l'inscription :** Lors de la création ou de la configuration d'un compte Twitter, l'utilisateur fournit des renseignements personnels tels que le nom, le nom d'utilisateur, le mot de passe ou l'adresse e-mail. Certains de ces renseignements, tels que le nom et le nom d'utilisateur, sont affichées publiquement sur ces Services, y compris sur votre profil et dans les résultats de recherche. Certains Services, comme la recherche, les profils publics d'utilisateurs ou les listes ne requièrent pas de s'enregistrer.

- **Renseignements complémentaires :** L'utilisateur peut décider de fournir des renseignements complémentaires qui seront affichés publiquement, tels qu'une photo,

une courte biographie ou encore sa localisation. Il est possible de personnaliser son compte en ajoutant des informations telles que le numéro de téléphone pour la réception de SMS ou le carnet d'adresses afin de retrouver des contacts sur Twitter. Twitter peut utiliser ces renseignements pour envoyer des informations concernant ces services ou à des fins de marketing. Il est possible d'arrêter de recevoir de tels communiqués de la part de Twitter en suivant la procédure de désabonnement incluse dans ces communiqués. Si l'utilisateur contacte Twitter par e-mail, Twitter peut conserver ses informations de contact afin de lui répondre. Fournir les renseignements complémentaires décrits dans cette section est entièrement facultatif.

- **Tweets, Abonnements, Listes et autres informations publiques:** ces services sont tout d'abord destinés à vous aider à partager des informations avec le monde. La plupart des informations que vous communiquez sont des informations que vous demandez de rendre publiques. Cela inclut non seulement les messages et les données que vous tweetez, mais aussi les listes que vous créez, les personnes que vous suivez, les Tweets que vous marquez comme favoris ou encore les Retweets et d'autres informations.

- **Information sur le lieu:** Vous pouvez choisir de noter votre emplacement dans vos tweets et dans votre profil Twitter. Si vous activez l'envoi d'informations géographiques lors d'envoi de Tweets, il est également possible d'enregistrer les coordonnées exactes pour améliorer ce service.

- **Journal de Données :** les serveurs enregistrent automatiquement les informations générées par l'utilisation des Services ("Journal de Données").

  Le Journal de Données peut inclure des informations telles que l'adresse IP, le type de navigateur, le domaine de référence, les pages visitées et les recherches effectuées. D'autres actions comme l'interaction avec les publicités peuvent également figurer dans le Journal de Données. Si le Journal de Données n'a pas encore été supprimé, ceci se fera après 18 mois, y compris les identifiants communs, tels votre nom d'utilisateur, les adresses IP, ou les adresses e-mail.

- **Liens:** Twitter peut garder une trace de la manière dont vous interagissez avec des liens dans les Tweets, y compris les services et clients tiers en redirigeant les clics ou par d'autres moyens.

- **Services Tiers :** Twitter utilise de nombreux services hébergés par des tiers pour fournir ces Services (comme divers blogs ou wikis). Ces services peuvent recueillir des informations envoyées par votre navigateur dans le cadre d'une requête de page Web, telles que les cookies ou votre requête d'IP.

5. Le rôle du protocole HTTPS dans la sécurité

5.1Activer le protocole HTTPS pour une navigation plus sûre

Le protocole de transfert hypertexte HTTP permet d'échanger des données sur un réseau. Cette découverte a permis le développement de toute une toile de liens interconnectés, accessible depuis n'importe quelle machine autorisée. Le problème, c'est qu'avec la prolifération des services et des pages qui nécessitent un mot de passe, le protocole HTTP n'est plus adapté. Dans certains cas, les utilisateurs mal intentionnés peuvent profiter de la connexion sans chiffrement pour accéder à des informations confidentielles.

Pour y remédier, le protocole HTTPS sécurise les échanges en y ajoutant une couche de chiffrement SSL ou TLS. Pour des transferts d'informations chiffrés et plus sûrs, il est donc préférable de contrôler que l'adresse URL affichée commence bien par "https://".

Dans le cas contraire, comment procéder**?** Voici un petit tour d'horizon d'activer protocole HTTPS.

5.2Le lancement de votre navigateur

Lorsque vous ouvrez votre navigateur, il utilise par défaut le protocole HTTP. Attention! Les pages de démarrage et de connexion aux comptes en ligne constituent deux moments critiques, susceptibles d'être mis à profit par des pirates informatiques.

Sur votre navigateur, vous pouvez facilement activer le protocole HTTPS en ajoutant, dans la barre d'adresse de ce dernier, un "s" derrière "http". Le résultat n'est pas garanti mais cette technique a le mérite d'être particulièrement facile à mettre en œuvre.

Figure 3 : Comment activer le protocole HTTPS

II. Comment mieux protéger sa vie privée ?

1. Application des règles européennes relatives à la protection des données personnelles

Les réseaux sociaux en ligne sont considérés comme des "responsables de traitements" au sens de la directive relative à la protection des données personnelles, puisqu'ils fournissent les moyens de traitement des données personnelles des utilisateurs et déterminent l'usage qui peut en être fait, notamment à des fins commerciales.

Les règles européennes relatives à la protection des données personnelles leur sont donc applicables, y compris lorsqu'ils sont établis hors de l'Espace Economique Européen (EEE). En effet, dès lors qu'ils recourent à l'utilisation de cookies et au traitement d'adresses IP, ils doivent être considérés comme ayant recours à des moyens de traitement situés sur le territoire de l'EEE.

En effet, on soulève la question de savoir si les utilisateurs eux-mêmes peuvent être soumis, en tant que responsables de traitements, aux règles relatives à la protection des données personnelles. Dans la plupart des cas, les utilisateurs bénéficient d'une exemption au titre de la conduite d'activités exclusivement personnelles.

Néanmoins, il se peut qu'un utilisateur soit considéré comme un responsable de traitement : il en est ainsi lorsqu'il agit pour le compte d'une société commerciale ou d'une association, ou lorsqu'il utilise la plateforme mise à sa disposition à des fins commerciales, politiques ou caritatives.

Les utilisateurs "professionnels" doivent en conséquence respecter toutes les dispositions applicables à la protection des données personnelles dans les Etats membres où ils procèdent aux traitements, et notamment assurer la sécurité et la confidentialité des données traitées.

2. Mesures de protection

2.2. Comment protéger ses images ?

Tout internaute, qu'il connaisse ou pas les risques, publiant ses photos sur un réseau social est un jour confronté au problème du vol de ses images, pourtant réprimé sévèrement par la loi.

2.1.1. Supprimer les facilités proposées par les navigateurs web

Les navigateurs les plus couramment utilisés (Internet et Firefox, …) proposent un certain nombre de fonctionnalités destinées à la récupération des images par l'internaute : but louable s'il en est, il nous faut donc les contrer un minimum !

a. Empêcher le clic droit de la souris

Le fameux clic droit de la souris permet l'accès (en environnement Windows en tout cas) à un menu contextuel permettant, sur une image, de l'enregistrer sur l'ordinateur de l'internaute… C'est là l'un des biais les plus utilisés pour récupérer les images sur le web.

Voici donc un petit script Javascript qui inhibe simplement l'apparition du menu contextuel :

```
<script type="text/javascript"> <!-- function clickIE4(){ if
(event.button==2){ return false; } } funct
```

À noter que la plupart des navigateurs actuels permettent de désactiver le javascript… et donc de parader très simplement ce subterfuge !en y désactivant quelques facilités pratiques.
La solution passe alors par un attribut à utiliser directement sur la balise image HTML, pour ne désactiver le clic droit que sur les images :

```
(XHTML Strict…) <IMG src="ici/le-chemin-vers/votre-image.jpg"
oncontextmenu="return false" />
```

Empêcher la désactivation du javascript !

b. Empêcher l'affichage de la barre d'images dans Internet Explorer

Cette petite barre d'image arrivée avec la version 6 du navigateur, permet à l'internaute de pouvoir, au simple passage de la souris sur celle-ci (en attendant généralement une fraction de seconde), directement sauvegarder, envoyer ou imprimer une image présente sur une page web… Si comme beaucoup de fonctionnalités proposées, celle-ci est louable, il n'empêche pas qu'elle est devenue avec le temps l'un des outils les plus pratiques pour les voleurs d'image en herbe ! À priori elle a disparu avec IE7.

Il existe une astuce extrêmement simple pour empêcher son apparition dans le navigateur Microsoft : une simple balise META, à disposer dans la balise HEAD (avec les autres balises META généralement présentes) de votre page HTML

```
<META HTTP-EQUIV="imagetoolbar" CONTENT="no">
```

3. Comparaison entre Facebook et Twitter

	Facebook	Twitter
Catégorie de réseau social	Est un réseau social doublement fermé	Est une plateforme de micro-blogging doublement ouverte
Type de connexion	Connexion bilatérale	Suivre sans être suivi ou l'inverse
Condition sur les messages	Permet l'échange de messages entre deux amis sans conditionnement de longueur	Permet d'envoyer à partir d'un ordinateur ou téléphone portable des messages de 140 caractères au plus (espaces compris)
Destinataire des messages	Partage à un groupe spécifique	Partage à tous le monde
Mentions	Mentions de noms	Mentions @
Type des messages	Messages à une personne en particulier	DM (messages directs)
Types de services offerts	• Tchat vidéo d'une personne vers une autre • Tchat intégré	Tweeter dans les résultats de recherches
Options d'utilisation	Possibilité de se déconnecter de quelqu'un	Possibilité de bloquer un utilisateur
Principale utilité	Sert principalement à publier des informations importantes ou le contraire	Utiliser pour repérer ou signaler des informations que l'on juge dignes d'intérêts
Financement	716 millions $	155 millions $
Valorisation	15 milliards $	1 milliards $
Nombres d'utilisateurs	300 millions	55 millions

Tableau 1 : Comparaison entre Facebook et Twitter

III. Quelles solutions adoptées ?

L'éclatant succès actuel des réseaux sociaux a un revers: il s'appuie sur le captage, réalisé avec leur consentement mais à des fins marketings, des données personnelles de leurs utilisateurs.

Conséquence: les problèmes liés à la protection de la vie privée et des informations personnelles sont aujourd'hui en pleine lumière. On s'intéresse aux développements récents dans le domaine des réseaux sociaux décentralisés, qui permettent de dépasser le dilemme entre préservation de la vie privée et présence sur les réseaux sociaux.
Ces outils pourraient même être les premiers à tirer pleinement parti du potentiel social des outils de réseaux virtuels.

L'idée était pour le moins surprenante : développer un réseau social « open source, contrôlé à l'échelle individuelle, respectueux de la vie privée et multifonction », alors même que le succès massif que connaissent les réseaux sociaux actuels repose sur le bon vouloir des utilisateurs à dévoiler leurs données personnelles, facilitant ainsi une forme sophistiquée de segmentation par « profils ». Plus surprenant encore fut l'intérêt qu'elle éveilla auprès du grand public.

Cette architecture tente :

- D'envisager des architectures innovantes capables d'intégrer les outils de réseau au niveau de l'interface ET de l'application.
- Améliorer ainsi d'un même coup la connectivité et la protection de la vie privée.
- Renforcer le caractère personnel des requêtes et des processus d'autorisations liées à l'établissement de liens sur le réseau.

- L'attribution de différents degrés de confiance à différents contacts pris au sein du réseau.

1. Vers une architecture décentralisée [28]

Des chercheurs américains proposent une nouvelle architecture décentralisée combinant de multiples technologies de sécurité, pour adresser le problème du respect de la vie privée et des données sur les réseaux sociaux.

Réseaux sociaux et vie privée ne font jusqu'ici pas très bon ménage. De nombreuses failles, accidentelles ou malveillantes, menacent les données des internautes, sur des réseaux sociaux comme Facebook ou Twitter. Des chercheurs de l'université de l'Illinois et de l'université d'Indiana, ont planché sur la question, et proposent une nouvelle architecture qui porte bien son nom *DECENT* (*Decentralized Architecture for Enforcing Privacy in Online Social Networks*) qui permet de renforcer les contrôles d'accès à un réseau social, sachant prendre en

compte la confidentialité, l'intégrité et la disponibilité des données, mais aussi de protéger les relations d'un utilisateur donné, même en présence d'un noeud malveillant.

2. Qu'est-ce qu'un réseau social décentralisé ? [29]

Pour bien comprendre le concept, il faut mettre les mains dans l'architecture qui sous tends à ces réseaux.

C'est la manière dont circulent les informations qui nous intéresse.

Sur une plateforme de réseau social classique, par exemple Facebook, il n'existe qu'un seul nœud de réseau, le même pour tous. Chaque utilisateur se connecte à la plateforme Facebook, à partir de laquelle il peut interagir avec ses amis, eux aussi connectés à Facebook. En un mot, Facebook est une plateforme, une application unique qui permet à ceux qui y sont connectés d'échanger.

Contrairement à Facebook, les réseaux sociaux décentralisés ne reposent pas sur une plateforme unique, mais sur une multitude de plateformes connectées entre elles par un protocole d'échange. Autrement dit, vous pouvez vous connecter sur une plateforme quelconque et dialoguer avec un ami connecté sur une autre plateforme, comme si vous étiez au même endroit.

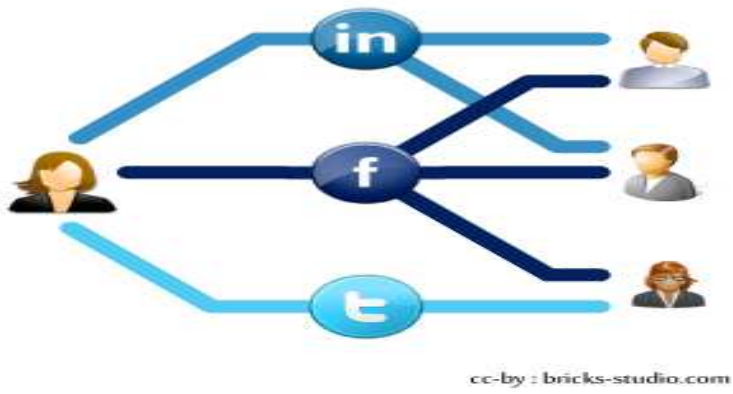


Figure 4 : Exemple d'architecture sur un réseau social centralisé

Sur un réseau social centralisé l'utilisateur passe par une plateforme pour interagir avec ses amis.

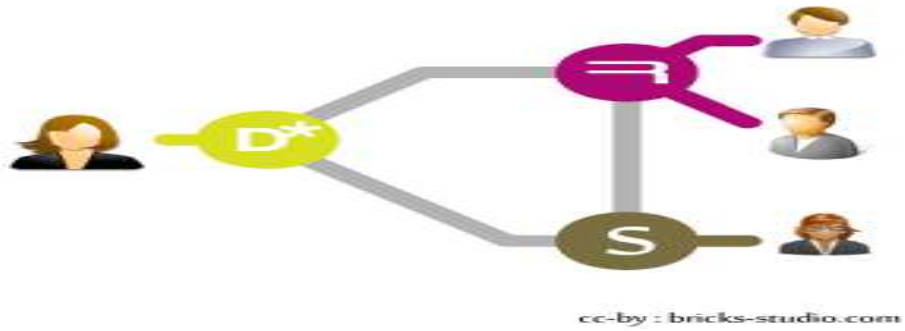


Figure 5 : Exemple d'architecture dans un réseau social décentralisé

Lorsque le réseau social est au contraire décentralisé, l'information transite par plusieurs plateformes.

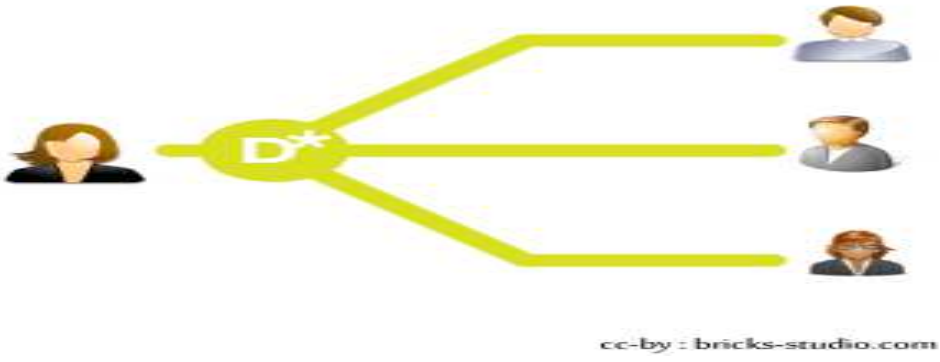


Figure 6 : Comment apparait un réseau social décentralisé aux yeux d'un utilisateur

Ce fonctionnement est dans la pratique totalement transparent pour l'utilisateur qui a l'impression que tout se passe depuis la plateforme qu'il utilise.

Les réseaux sociaux décentralisés reposent sur un protocole d'échange standard open source et ouvrent les services d'hébergement à la concurrence. Rien ne vous empêche d'ailleurs, de mettre en ligne votre propre serveur et de vous connecter au réseau global depuis une plateforme qui vous appartienne.

Cette ouverture à la concurrence a un certain nombre de conséquences, à la fois sur le dynamisme entrepreneurial, donc l'innovation et la richesse des services auxquels nous aurons accès, et à la fois sur la manière dont nous utiliserons les réseaux sociaux si ce système se généralise.

3. DISPORAMA

A l'été 2010, quatre étudiants de premier cycle de l'Université de New York (NYU) réussirent à lever près de 100 000 dollars, un montant plus de dix fois supérieur à celui qu'ils visaient pour développer leurs idée de réseau social décentralisé.

Dan Grippi, l'un des quatre fondateurs, s'en émerveille encore : « Pour quelque mystérieuse raison, tout le monde est tombé d'accord sur ce concept qui tournait autour du respect de la vie privée », explique-t-il dans les pages du New York Times.

Cette raison mystérieuse pourrait bien être la suivante : contre toute apparence, les utilisateurs, ou du moins, certains d'entre eux sont soucieux de leur vie privée.

S'ils apprécient le potentiel des réseaux sociaux en termes d'agrégation, de communication, d'échanges et d'interactions, et souhaitent continuer d'en profiter, les

utilisateurs de ces services ne voient pas leur droit à la vie privée comme une monnaie d'échange qu'il leur faudrait céder pour pouvoir accéder à ces réseaux.
Ils seraient donc tout à fait prêts à migrer vers une technologie qui leur permette de refuser, au moins partiellement, ce compromis entre respect de l'intimité et accès au réseau; pour lancer le mouvement, ils financent par leurs dons des gens qualifiés qui peuvent ainsi se consacrer au développement de technologies adaptées.

En retour, ces derniers, à l'instar des quatre jeunes développeurs de Diaspora, qui sont aujourd'hui les plus présents dans les médias mais sont loin d'être les seuls assurent que le compromis intimité-connectivité peut être contourné.

La solution s'appelle le réseau social décentralisé.

4. Inconvénients

Le plus grande inconnue pour ces projets de réseaux sociaux décentralisés est sans doute de savoir si les utilisateurs eux-mêmes seront prêts non seulement à migrer vers une autre plate-forme, mais aussi vers une application dont la prise en main et les bénéfices d'utilisation sont peut-être moins immédiats. La valeur ajoutée offerte par ces projets étant en résumé la possibilité pour les utilisateurs de générer leur propre petit serveur abritant les données de leur profil, ces produits risquent, selon certains, de ne pas toucher suffisamment d'adeptes parmi des utilisateurs habitués à une interface moins compliquée, accessible au plus grand nombre. Pourtant, comme le note un commentateur, « qu'un groupe de développeurs ait lancé une

levée de fonds pour créer une alternative à Facebook – et que des personnes aient répondu à l'appel – représente peut-être la critique la plus accablante envers ce réseau social ». Si l'ingrédient manquant est la notoriété et un large soutien, le moment est peut-être idéal pour se lancer et accélérer les choses.

Néanmoins, le cout matériel et la protection des membres seront sans doute plus élevés.

En effet, vu que chaque utilisateur sera considéré comme étant client et serveur à la fois, il faudra adopter des techniques plus élaborée pour instaurer une politique de sécurité.

IV. Proposition d'une solution

Après une étude approfondie de la vie privée dans les réseaux sociaux en général, et de la protection de la vie privée dans les deux réseaux sociaux Facebook et Twitter en particulier, nous avons aboutie à un certain nombre de conclusions.

L'ensemble des données et informations concernant des utilisateurs ainsi que leurs différents échanges transitent par le serveur du réseau social utilisé (dans notre cas Facebook ou Twitter).

Chaque information lors de sont passage par le serveur en question, se voit attribuée une copie qui sera sauvegardée, par la suite elle sera transmise au destinataire voulu.

Dés l'heure, l'utilisateur se voit dépourvu du pouvoir de contrôler les informations le concernant ou lui appartenant, que ce soit données vidéos, textes ou encore images (photos).

Une solution a été proposé, elle consiste à décentralisé le réseau social, ceci rend chaque utilisateur administrateur de ces données, car il se voit être client et serveur à la fois.

Mais cette solution présente un certain nombre d'inconvénient, comme le cout matériel, problème de maintenance,…

La solution la plus optimale dans ce cas serait de masquer les informations transitant par le serveur du réseau social, et cela dans le but d'une meilleure protection de la vie privée.

La technique adéquate pour cela est l'utilisation de la ***cryptographie***, ainsi toute donnée sera illisible par les autres.

Qui ne connait pas la galère de devoir s'inscrire sur une dizaine de réseaux sociaux et de tenir à jour ses profils.

L'utilisateur moyen est inscrit à Facebook, à MSN, à Twitter, et à quelques forums et autres réseaux spécialisés.

Si le mode de fonctionnement des réseaux sociaux décentralisés se répand, on peut imaginer qu'à plus ou moins long terme on verra se dessiner un protocole unique d'échange entre les réseaux.

Mais les inconvénients de chaque réseau social poussent à chercher une solution qui offre une protection de la vie privée en assurant la sécurité des données échangées.

Cette solution serait la « ***cryptographie*** ».

Chapitre 4

Analyse et conception

Chapitre 4 Analyse et Conception

Dans le but d'une meilleure organisation et une bonne maîtrise du travail, tout processus de développement d'applications ou systèmes informatiques doit suivre une méthode ou démarche bien définie.

Dans ce chapitre, nous allons entamer le processus par une analyse qui mettra en évidence les différents acteurs intervenant dans le système cible ainsi que leurs besoins. La phase conception, s'appuyant sur les résultats de la phase analyse donnera la modélisation des objectifs à atteindre. Pour ce faire, notre démarche va s'appuyer sur le langage UML, conçu pour la visualisation, la spécification et la construction des systèmes logiciels.

I. Présentation d'UML

UML (*Unified Modeling Language*) est un langage unifié pour la modélisation dans le cadre de la conception orienté objet. Il s'agit d'un langage graphique de modélisation objet permettant de spécifier, de construire, de visualiser et de décrire les détails d'un système logiciel. Il est issu de la fusion de plusieurs méthodes dont « Bootch » et «OMT » et adapté à la modélisation de tous types de système. Il devient aujourd'hui un standard dans le domaine d'analyse et de conception orientée objet.

Il propose plusieurs modèles qui sont des descriptions abstraites du système étudié et qui sont :

- Le modèle de classe qui capture la structure statique
- Le modèle des cas d'utilisation qui décrit les besoins de l'utilisateur
- Le modèle d'interactions qui décrit les scénarios et les flots de messages
- Le modèle des états qui exprime le comportement dynamique des objets
- Le modèle de réalisation qui montre les unités de travail
- Le modèle de déploiement qui précise la répartition des processus

Ces modèles sont élaborés pour les utilisateurs au moyen de diagramme. Un diagramme spécifie un aspect précis du modèle.

II. Analyse

1. Problématique

Dés l'heure, ou un abonné d'un réseau social, quelconque soit-il, partage des informations de types : textes, vidéos, images, ce dernier se voit dépourvu du contrôle de ses données.

Lors du passage de ces données par le serveur du réseau social utilisé, ces dernières ce voient enregistrées, pour être enfin transmises à l'interlocuteur.

Pour remédier à ce problème, nous proposons d'introduire le concept de cryptographie.

2. Objectif

Il s'agit d'introduire un serveur de confiance, qui aura pour rôle l'attribution de clé de cryptage /décryptage pour les utilisateurs d'un réseau social.

Nous avons conçu un réseau social permettent l'échange de données textuelles. Ces dernières se verront cryptées avant leur passage par le serveur du réseau.

3. Quelques définitions de base

- **Un acteur** : Il représente un ensemble cohérent de rôles que peut jouer l'utilisateur (entité externe) avec le système, et interagit avec celui-ci en fournissant de l'information en entrée et/ou la reçoit en sortie.

- **Un cas d'utilisation** : Est un texte qui décrit l'interaction et les dialogues entre l'acteur et le système.
  Les cas d'utilisation sont une technique puissante pour consigner et traduire le comportement détaillé du système.

- **Un scénario** : Représente une succession particulière d'enchainements qui s'exécutent du début à la fin du cas d'utilisation. Un enchainement étant l'unité de description de séquences d'actions.
  Un ensemble de scénarios pour un cas d'utilisation identifie tous ce qu'il peut arriver lorsque ce cas d'utilisation est mis en œuvre.

La figure ci-dessous montre la représentation graphique de la démarche de modélisation choisie pour concevoir notre application :

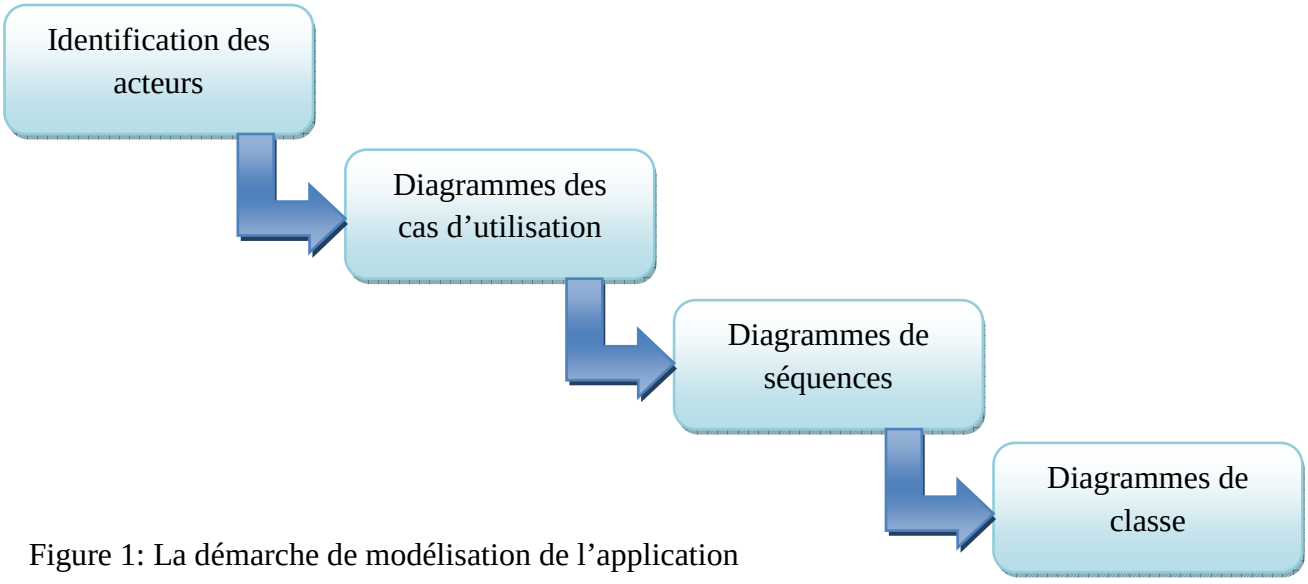


Figure 1: La démarche de modélisation de l'application

4. Identifications des acteurs

Les principaux acteurs sont :

- **Utilisateur** : Toute personne disposant d'un compte au sein du réseau social.

5. Spécification des tâches

Chacun des acteurs que nous avons définis précédemment, effectue un certain nombre de tâches qu'on résume dans le tableau suivant :

Acteurs	Tâches
Utilisateur	**T0** : Accéder à l'accueil **T1** : S'inscrire au réseau social **T2** : Se connecter à son compte **T3** : Consulter la liste de ses contacts ainsi que les informations relatives aux profils **T4 :** Supprimer un contact **T5** : Consulter son compte **T6** : Envoyer un message sans le crypter **T7** : Envoyer un message en le cryptant **T8** : Décrypter un message reçu **T9** : Se déconnecter de son compte

Tableau 1 : Spécification des tâches

6. Spécification des scénarios

Les scénarios décrivant chacune des tâches définies précédemment sont récapitulés dans le tableau suivant :

	Tâches	Scénarios
Utilisateur	**T0** : Accéder à l'accueil	**S0** : Lancer la page de démarrage
	T1 : S'inscrire au réseau social	**S1** : Sélectionner l'option d'inscription **S2** : Introduire un nom, prénom, pseudonyme ainsi qu'un mot de passe **S3** : Valider la requête
	T2 : Se connecter à son compte	**S4** : Sélectionner l'option de connexion **S5** : Saisir son pseudonyme et son mot de passe **S6** : Valider la requête
	T3 : Consulter la liste de ses contacts ainsi que les informations relatives aux profils	**S7** : Sélectionner l'option de consultation de la liste des contacts
	T4 : Supprimer un contact	**S8** : Sélectionner l'option de suppression de contacts
Utilisateur	**T5** : Consulter son compte	**S9** : Afficher la fenêtre de dialogues **S10** : Voir la liste des contacts connectés
	T6 : Envoyer un message sans le crypter	**S11** : Saisir son message dans la zone dédiée **S12** : Sélectionner le contact voulu **S13** : Envoyer le message
		S14 : Saisir son message dans la zone

	T7 : Envoyer un message en le cryptant	dédiée **S15** : Crypter le message en appuyant sur le bouton « crypter » **S16** : Envoyer le message
	T8 : Décrypter un message reçu	**S17** : Réception du message **S18** : Décrypter le message en appuyant sur le bouton « décrypter »
	T9 : Se déconnecter de son compte	**S19** : Sélection l'option de déconnection **S20 :** Valider la requête

Tableau 2 : Spécification des scénarios

7. Spécification des cas d'utilisation

Cas d'utilisation : Inscription au réseau social

Use case : Inscription au réseau social
Scénarios : S0, S1, S2, S3
Acteur : Utilisateur

Description :

1. L'utilisateur lance la page de démarrage
2. Il accède à la page d'inscription
3. Il saisie son nom, prénom, pseudonyme ainsi qu'un mot de passe
4. Il valide sa requête

Cas d'utilisation : Connexion au compte

Use case : Connexion au compte
Scénarios : S0, S4, S5, S6
Acteur : Utilisateur

Description :

1. L'utilisateur lance la page de démarrage
2. Il accède à l'option de connexion
3. Il saisie son pseudonyme ainsi que son mot de passe
4. Il valide sa requête

Cas d'utilisation : Consulter la liste de ses contacts ainsi que les informations relatives aux profils

Use case : Consulter la liste de ses contacts ainsi que les informations relatives aux profils
Scénarios : S0, S7
Acteur : Utilisateur

Description :

1. L'utilisateur lance la page de démarrage
2. Il accède à l'option liste des contacts
3. Il peut voir l'ensemble des internautes inscrits au réseau social ainsi que leur profil, y compris le sien

Cas d'utilisation : Supprimer un contact

Use case : Supprimer un contact
Scénarios : S0, S8
Acteur : Utilisateur

Description :

1. L'utilisateur lance la page de démarrage
2. Il accède à l'option supprimer contact
3. Il peut supprimer un ou plusieurs contacts en saisissant son pseudonyme

Cas d'utilisation : Consulter son compte

Use case : Consulter son compte
Scénarios : S0, S4, S5, S6, S9, S10
Acteur : Utilisateur

Description :

1. L'utilisateur lance la page de démarrage
2. Il sélectionne l'option de connexion
3. Il saisie son pseudonyme ainsi que son mot de passe
4. Il valide sa requête
5. La fenêtre de dialogues s'affiche ainsi que la liste des contacts connectés

Cas d'utilisation : Envoyer un message sans le crypter

Use case : Envoyer un message sans le crypter

Scénarios : S0, S4, S5, S6, S9, S10, S11, S12, S13

Acteur : Utilisateur

Description :

1. L'utilisateur lance la page de démarrage
2. Il sélectionne l'option de connexion
3. Il saisie son pseudonyme ainsi que son mot de passe
4. Il valide sa requête
5. La fenêtre de dialogues s'affiche ainsi que la liste des contacts connectés
   Sélectionner l'option d'envoi de messages
6. Choisir le nom d'un ami
7. Ecrire le message
8. Envoyer le message

Cas d'utilisation : Envoyer un message en le cryptant

Use case : Envoyer un message en le cryptant
Scénarios : S0, S4, S5, S6, S9, S10, S14, S15, S16
Acteur : Utilisateur

Description:

1. L'utilisateur lance la page de démarrage
2. Il sélectionne l'option de connexion
3. Il saisie son pseudonyme ainsi que son mot de passe
4. Il valide sa requête
5. La fenêtre de dialogues s'affiche ainsi que la liste des contacts connectés
6. Choisir le nom d'un ami
7. Saisir son message dans la zone dédiée
8. Appuyer sur le bouton « crypter »
9. Le message s'affiche crypté dans la zone de texte à envoyer
10. Appuyer sur le bouton « envoyer »

Cas d'utilisation : Décrypter un message reçu

Use case : Décrypter un message reçu
Scénarios : S0, S4, S5, S6, S9, S10, S17, S18
Acteur : Utilisateur

Description :

1. L'utilisateur lance la page de démarrage
2. Il sélectionne l'option de connexion
3. Il saisie son pseudonyme ainsi que son mot de passe
4. Il valide sa requête
5. La fenêtre de dialogues s'affiche ainsi que la liste des contacts connectés
6. Lorsqu'il reçoit un message crypté d'un contact connecté, il appui sur le bouton « décrypter » pour voir le message en clair

Cas d'utilisation : Se déconnecté de son compte

Use case : Se déconnecté de son compte
Scénarios : S19, S20
Acteur : Utilisateur

Description :

1. Sélectionner l'option de déconnexion
2. Valider la requête

III. Conception

Le processus de conception repose sur l'organisation conceptuelle, logique et physique des données collectées durant la phase analyse. En effet, elle s'appuie essentiellement sur quelques diagrammes du langage de modélisation UML.

1. Diagrammes des cas d'utilisation

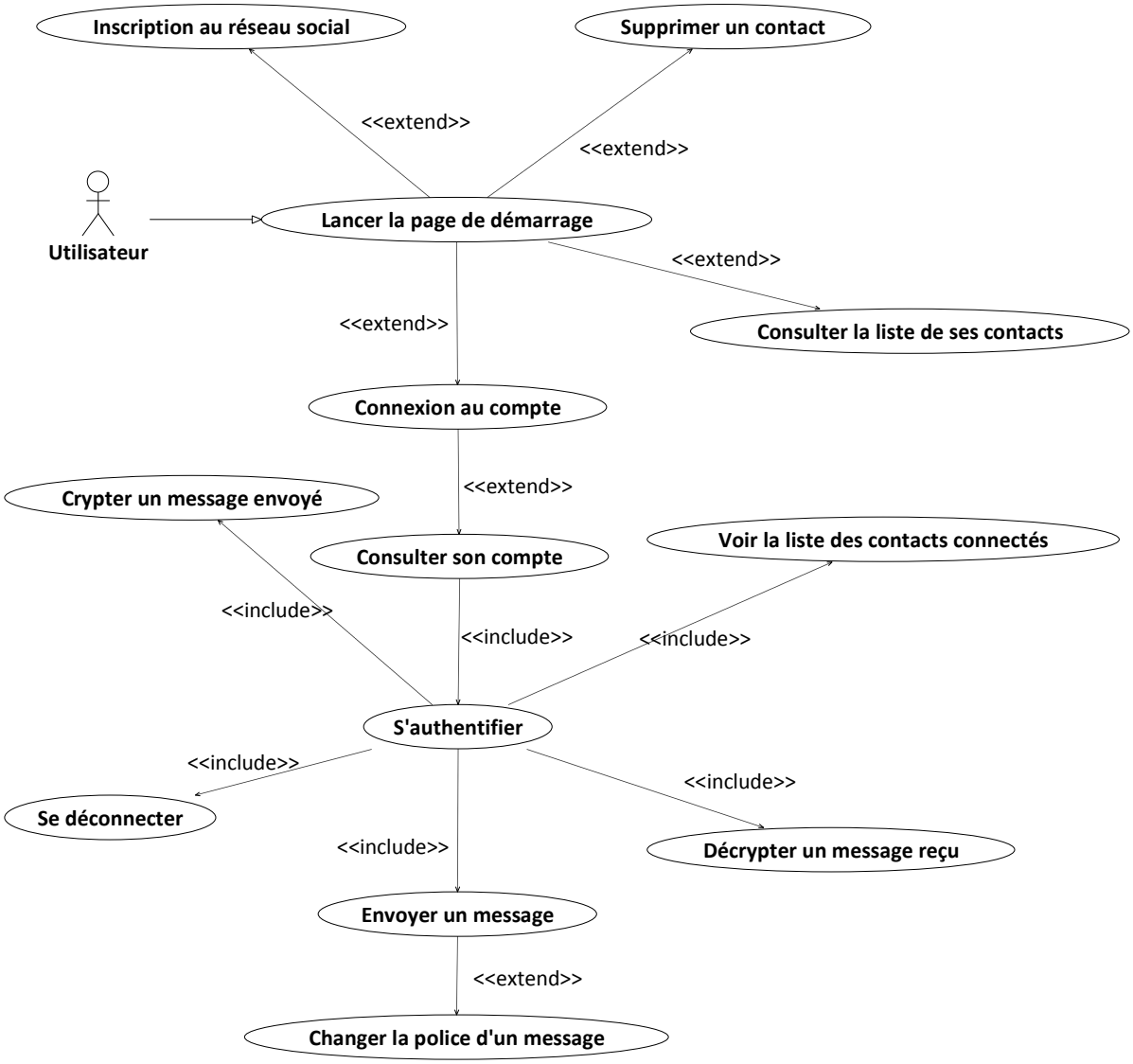


Figure 2 : Diagramme des cas d'utilisation pour l'utilisateur

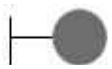
2. Diagrammes de séquences

Le diagramme de séquence représente la succession chronologique des opérations réalisées par un acteur : saisir une donnée, consulter une donnée, lancer un traitement ; il met en évidence les objets manipulés ainsi que les opérations qui font passer d'un objet à l'autre.

Dans notre cas on s'intéresse seulement à effectuer la représentation du diagramme de séquence pour des cas d'utilisation déjà présentés auparavant.

- **Objet interface :**

Représente l'interface entre l'acteur et le système tel que les pages web ou écrans de saisie, c'est une description des opérations visibles.

L'icône : 

- **Objet entité :**

Représente les concepts métier.il est très souvent persistant, est décrie dans un cas d'utilisation et se trouve dans un autre cas d'utilisation tel que operateur, enregistrement,…

L'icône : 

- **Objet contrôle :**

C'est un objet actif, tel qu'il possède un flot de contrôle .un objet actif peut activer un objet passif pour le temps d'une opération, en lui envoyant un message.il dirige les activités des entités et interfaces.ces objets sont obtenus en extrayant les verbes des cas d'utilisations.

L'icône : 

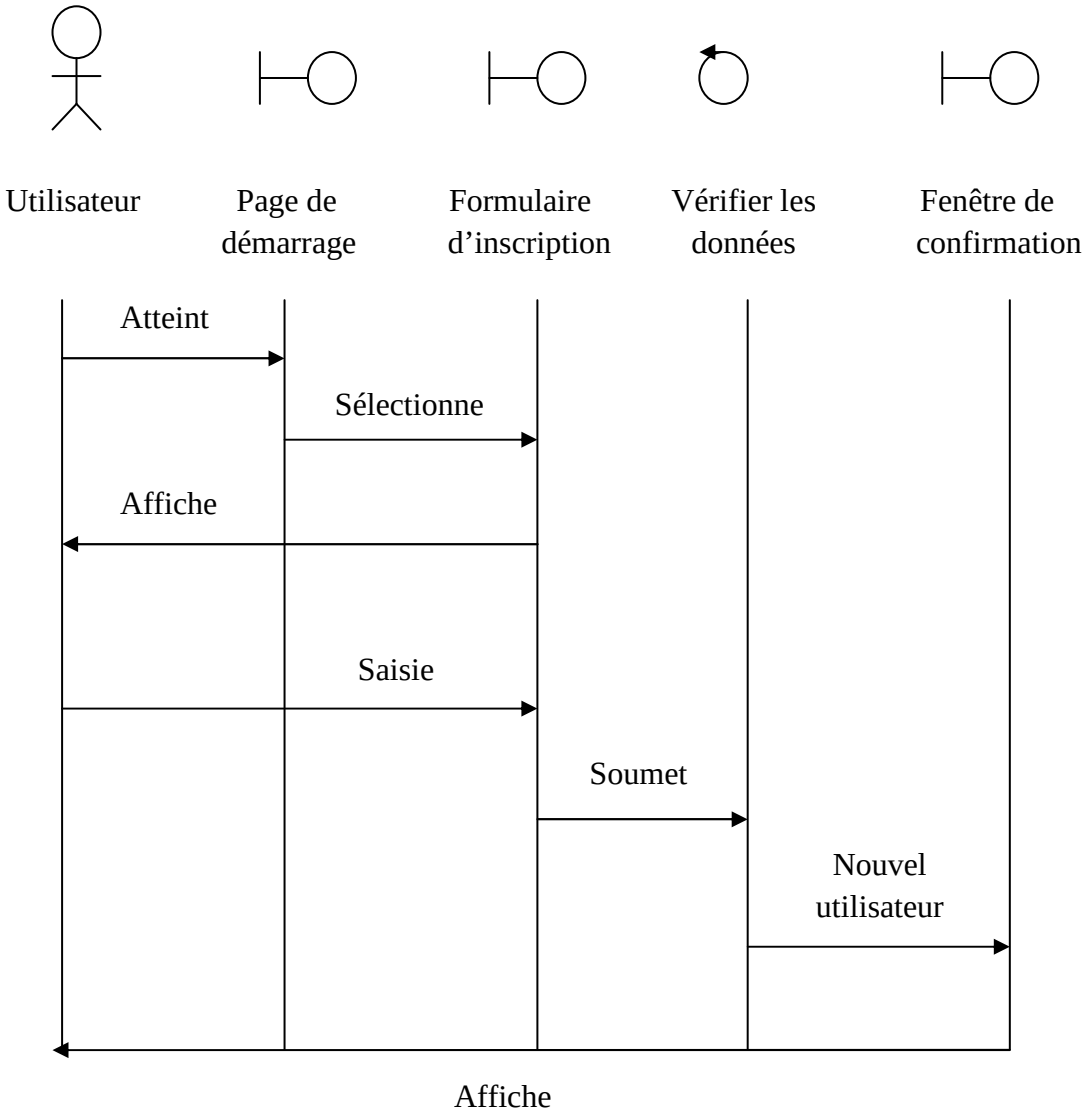


Figure 3 : Diagramme de séquence du cas d'utilisation : « **Inscription au réseau social** »

1. L'utilisateur lance la page de démarrage
2. Il accède à la page d'inscription
3. Il saisie son nom, prénom, pseudonyme ainsi qu'un mot de passe
4. Il valide sa requête

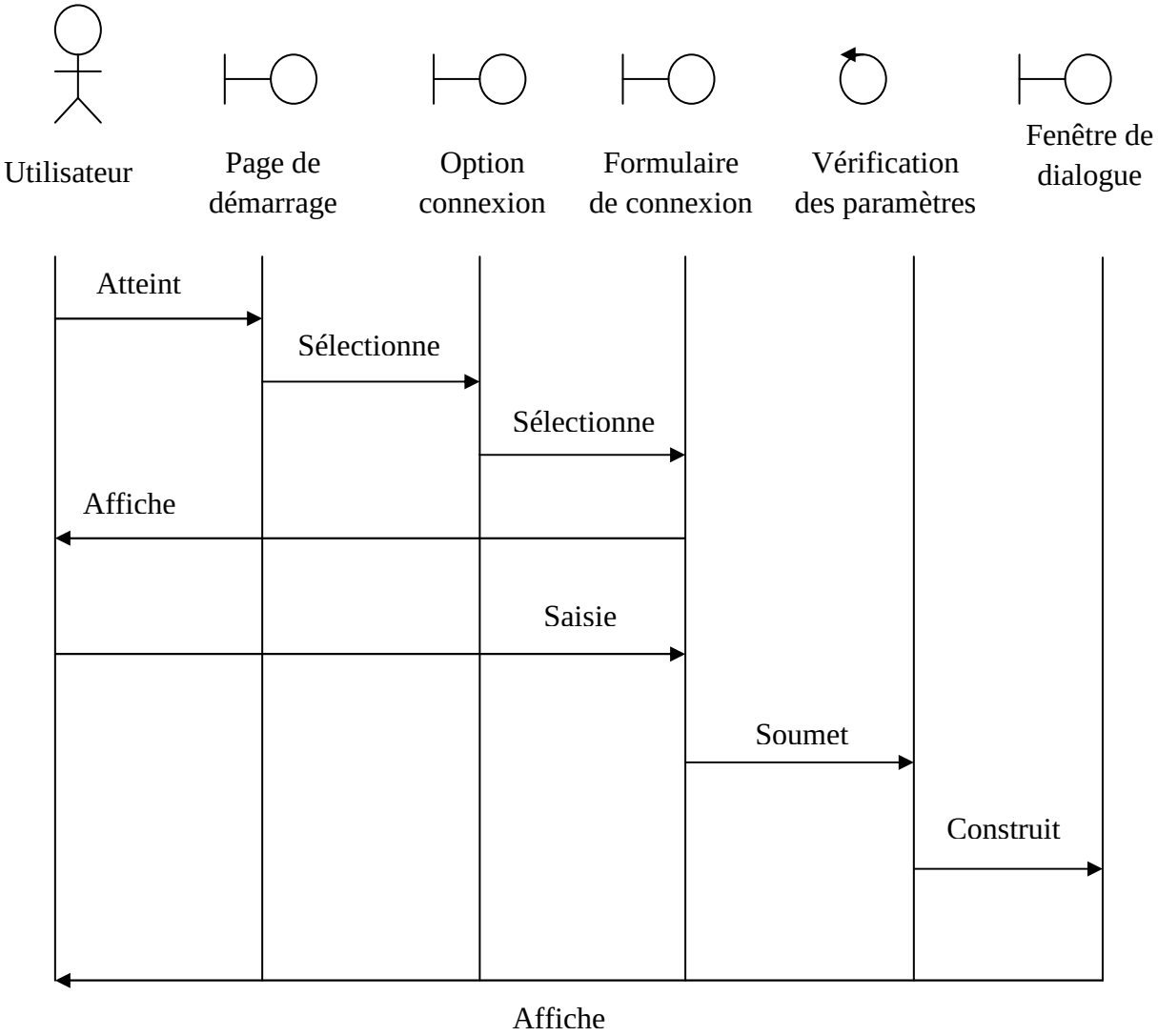


Figure 4 : Diagramme de séquence du cas d'utilisation : « **Connexion au compte »**

1. L'utilisateur lance la page de démarrage
2. Il accède à l'option de connexion
3. Il saisie son pseudonyme ainsi que son mot de passe
4. Il valide sa requête

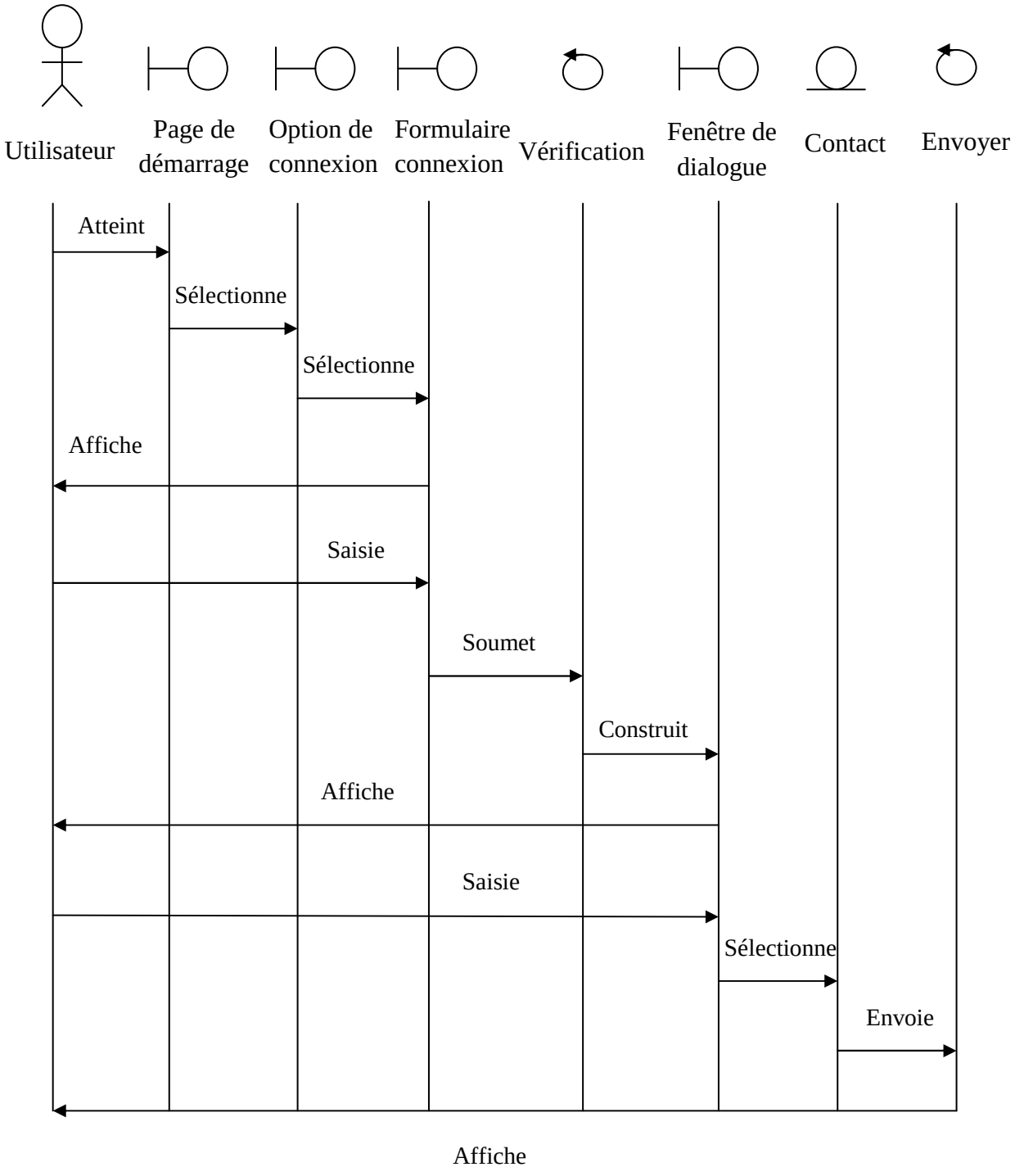


Figure 5 : Diagramme de séquence du cas d'utilisation : « **Envoyer un message sans le crypter »**

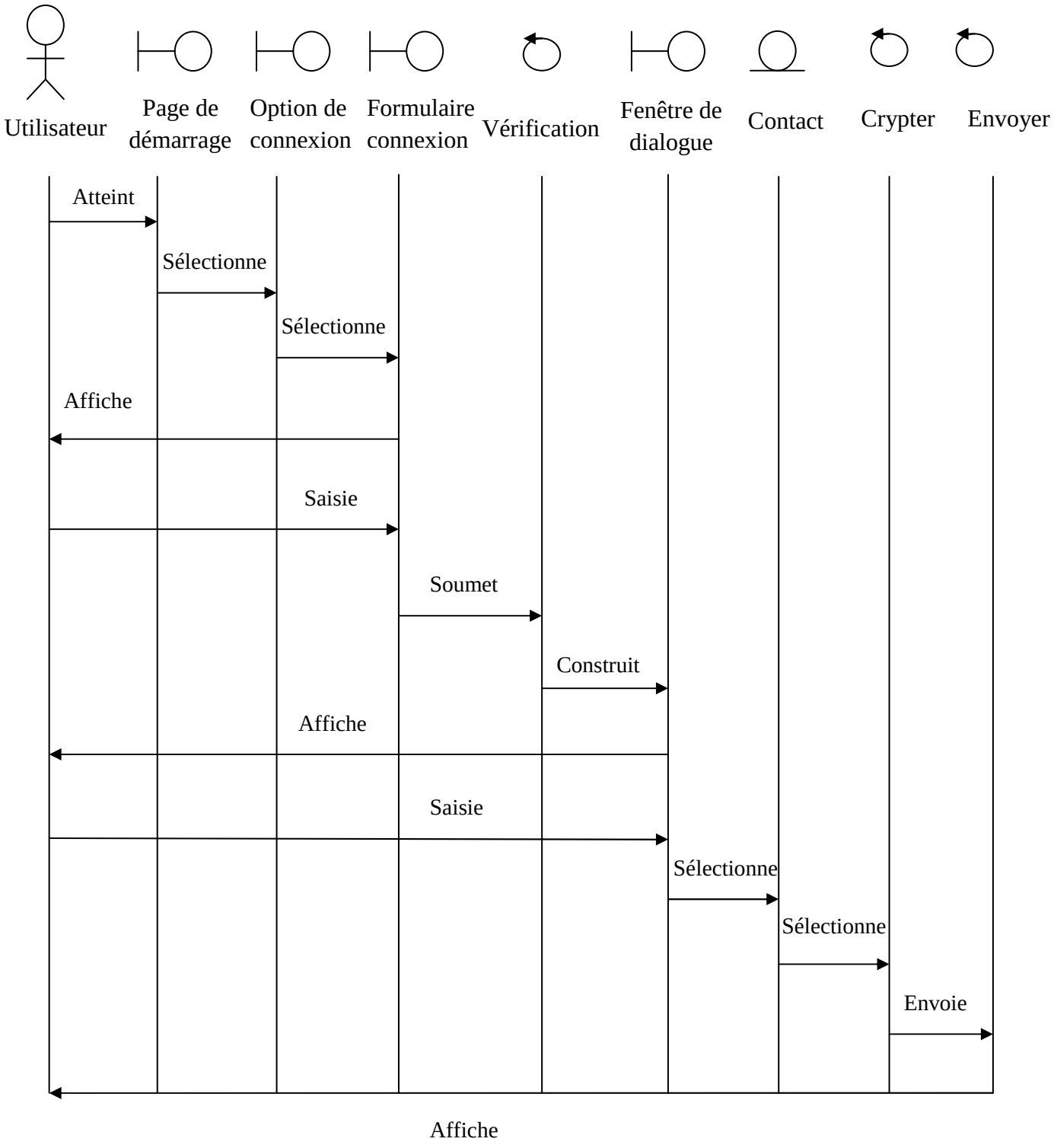


Figure 6 : Diagramme de séquence du cas d'utilisation : « **Envoyer un message en le cryptant »**

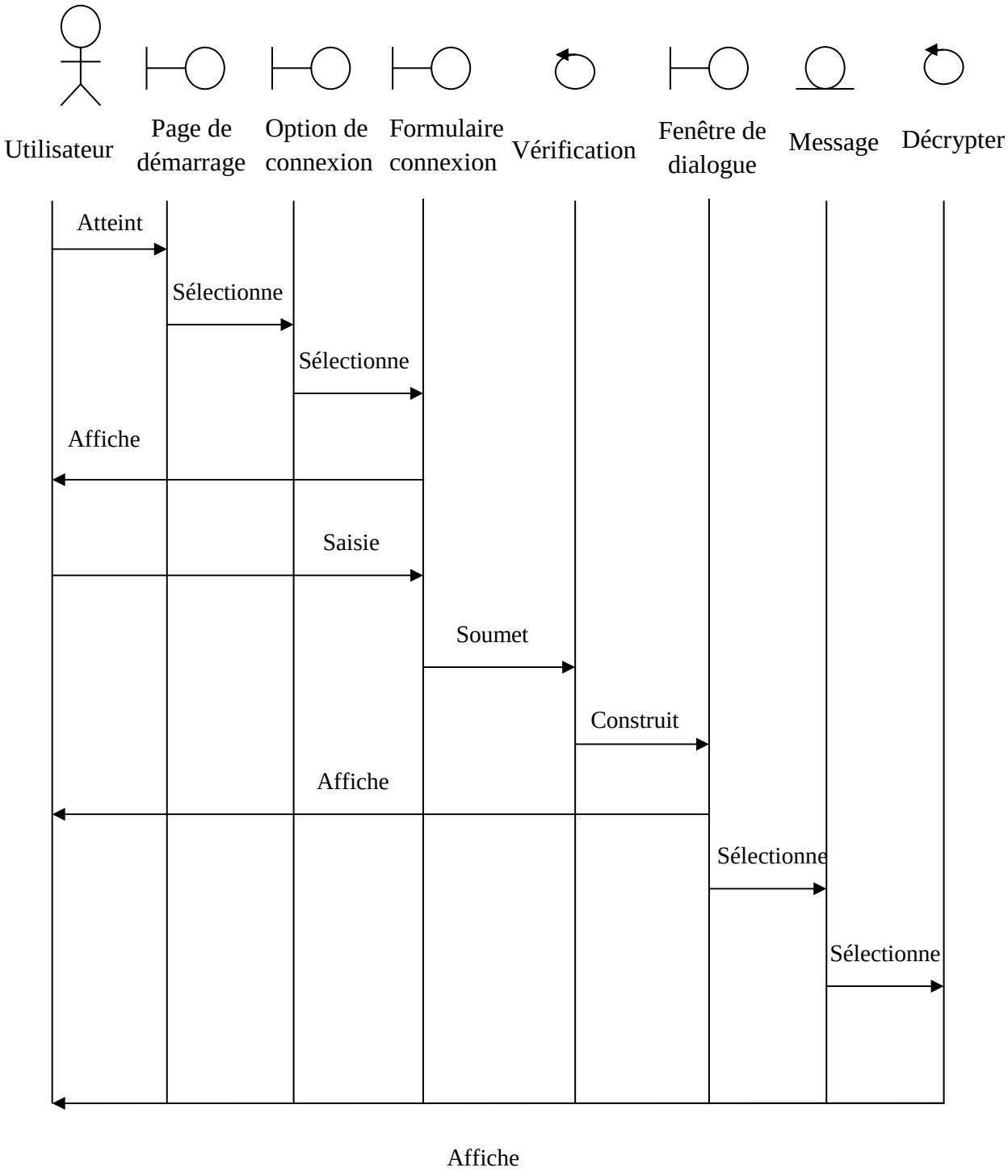


Figure 7: Diagramme de séquence du cas d'utilisation : « **Décrypter un message reçu »**

3. Les diagrammes de classe

Une fois que les diagrammes de séquences sont élaborés, on passera aux diagrammes de classe qui représentent la vue logique des objets pages.

Les diagrammes de classe représentent l'architecture conceptuelle du système.

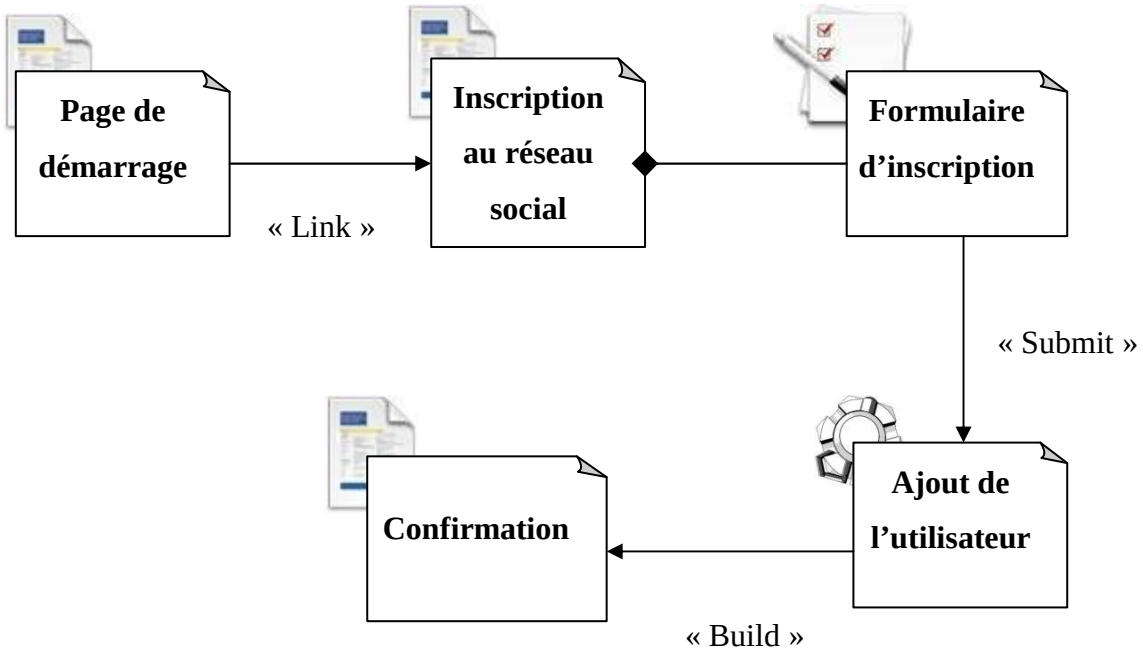


Figure 8 : Diagramme de classe général du cas d'utilisation : « **Inscription au réseau social** »

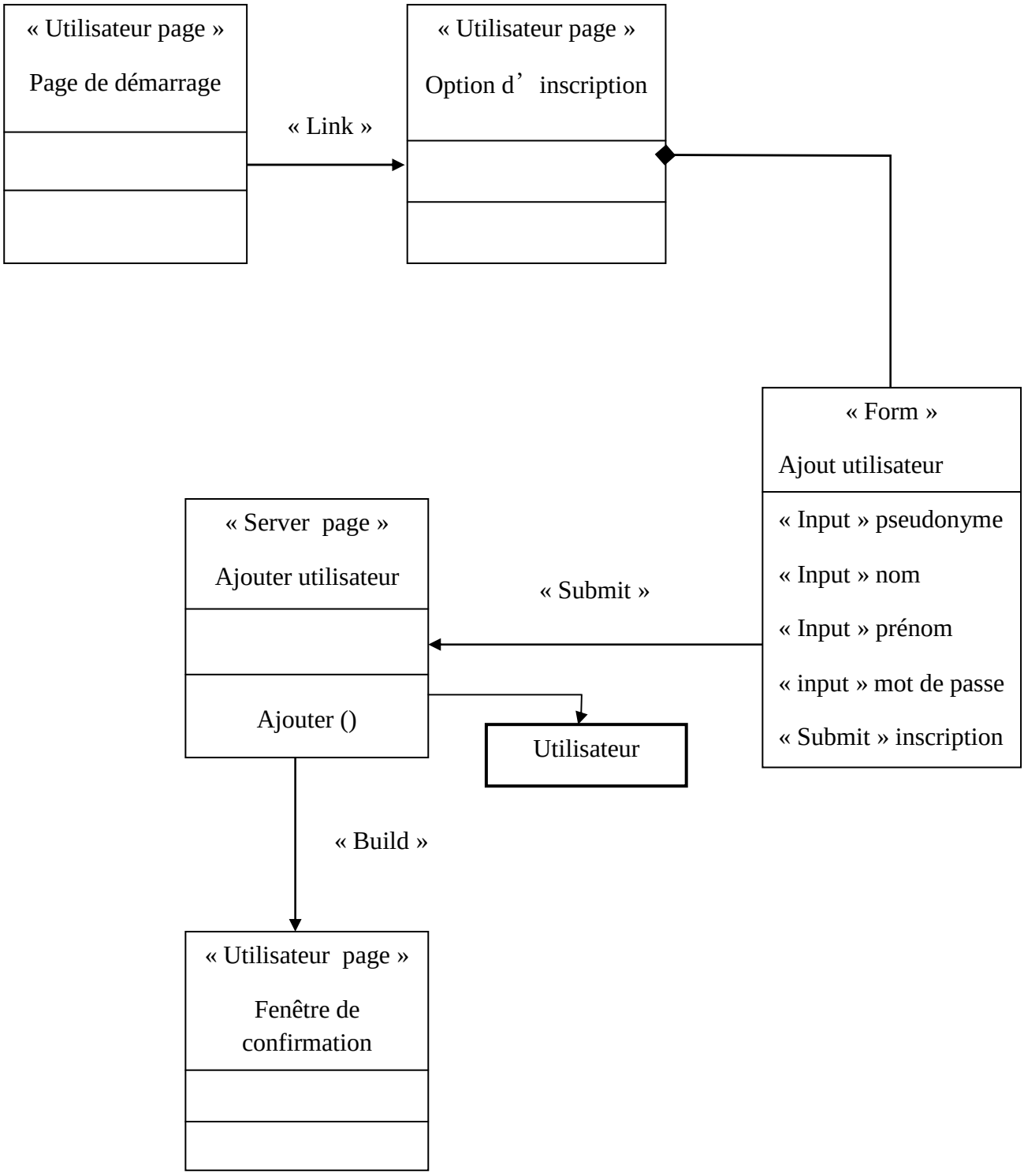


Figure 9 : Diagramme de classe détaillé du cas d'utilisation : « **Inscription au réseau social** »

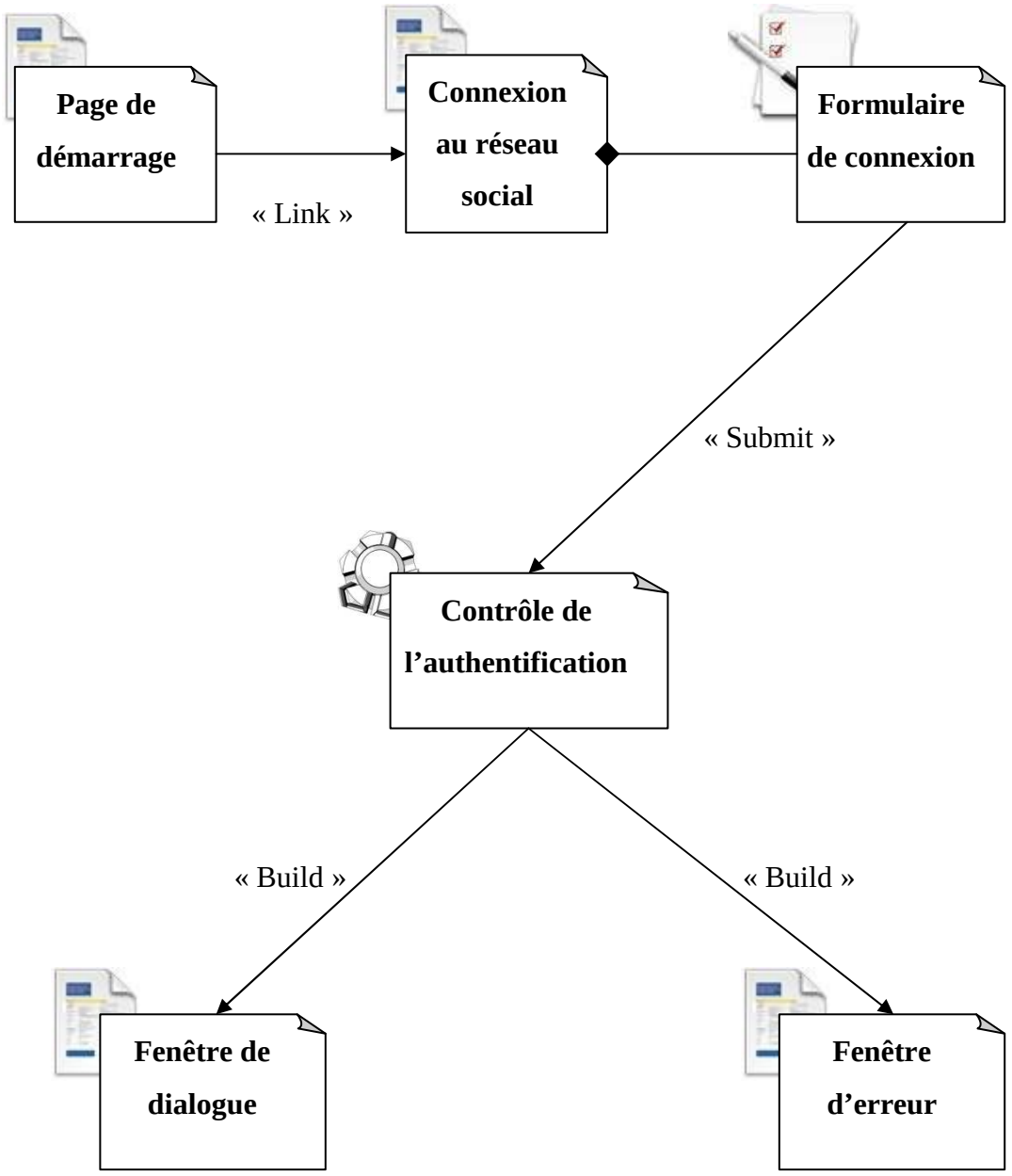


Figure 10 : Diagramme de classe général du cas d'utilisation : « **Connexion au compte »**

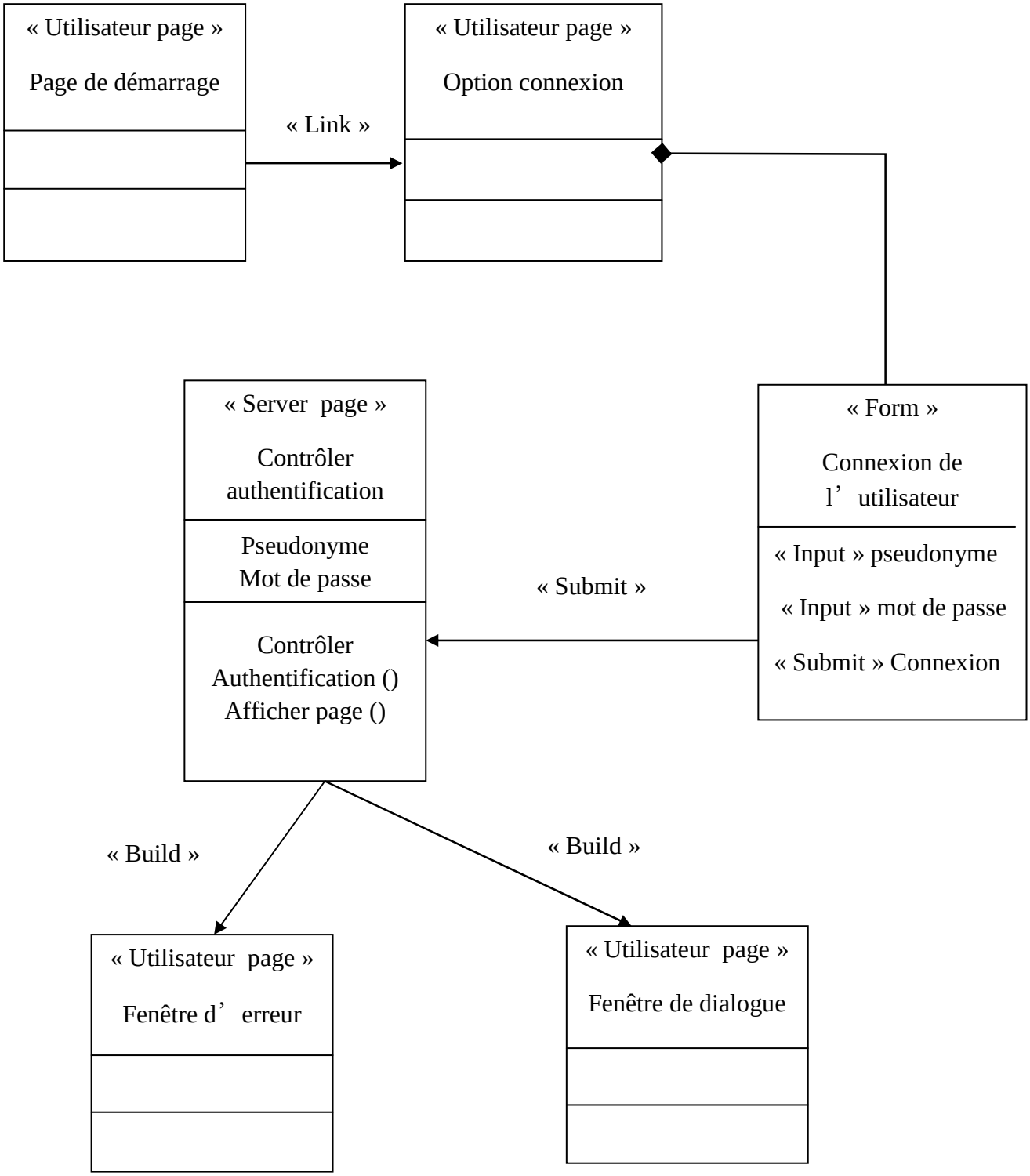


Figure 11 : Diagramme de classe détaillé du cas d'utilisation : « **Connexion au compte »**

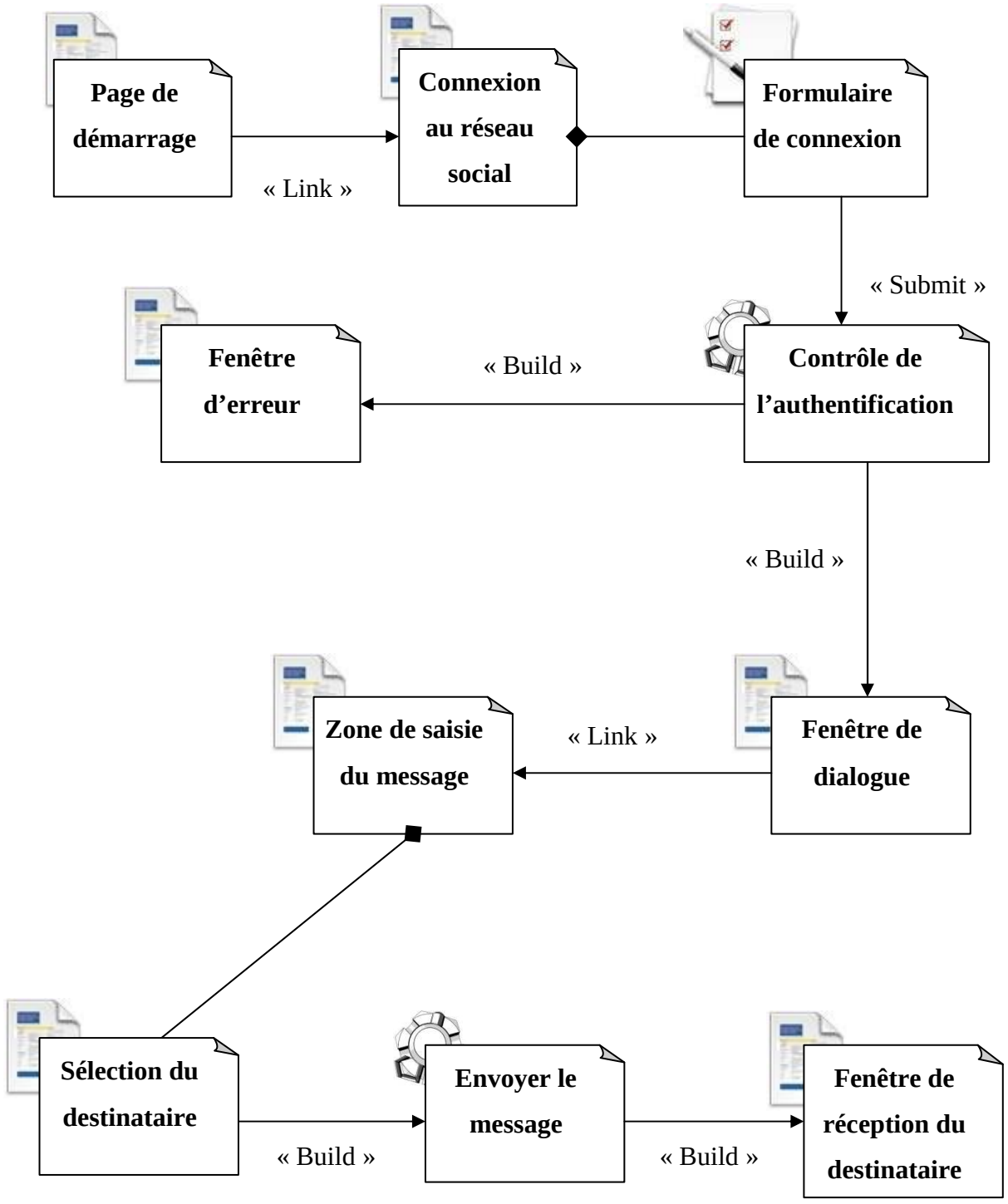


Figure 12 : Diagramme de classe général du cas d'utilisation : « **Envoyer un message sans le crypter »**

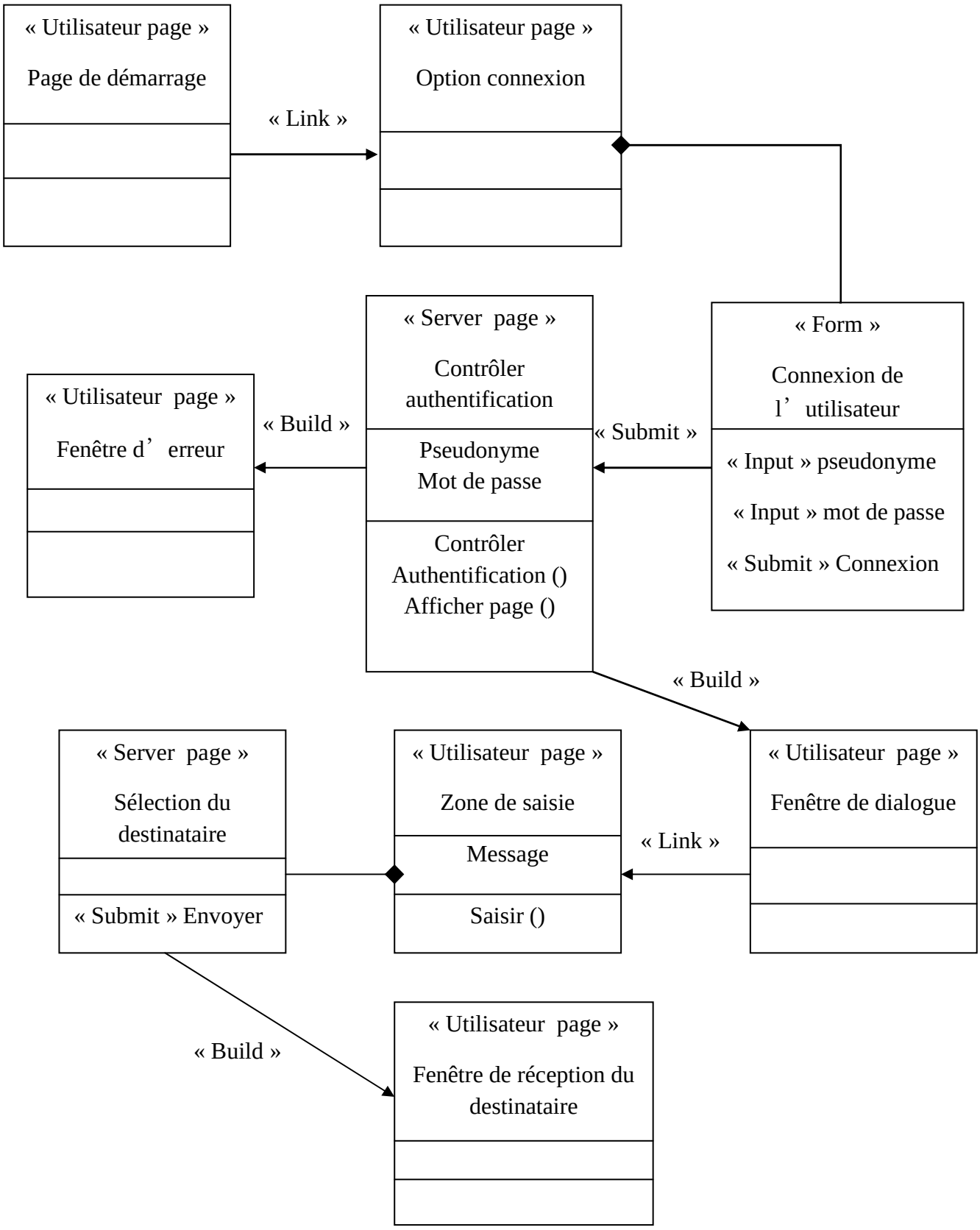


Figure 13 : Diagramme de classe détaillé du cas d'utilisation : « **Envoyer un message sans le crypter »**

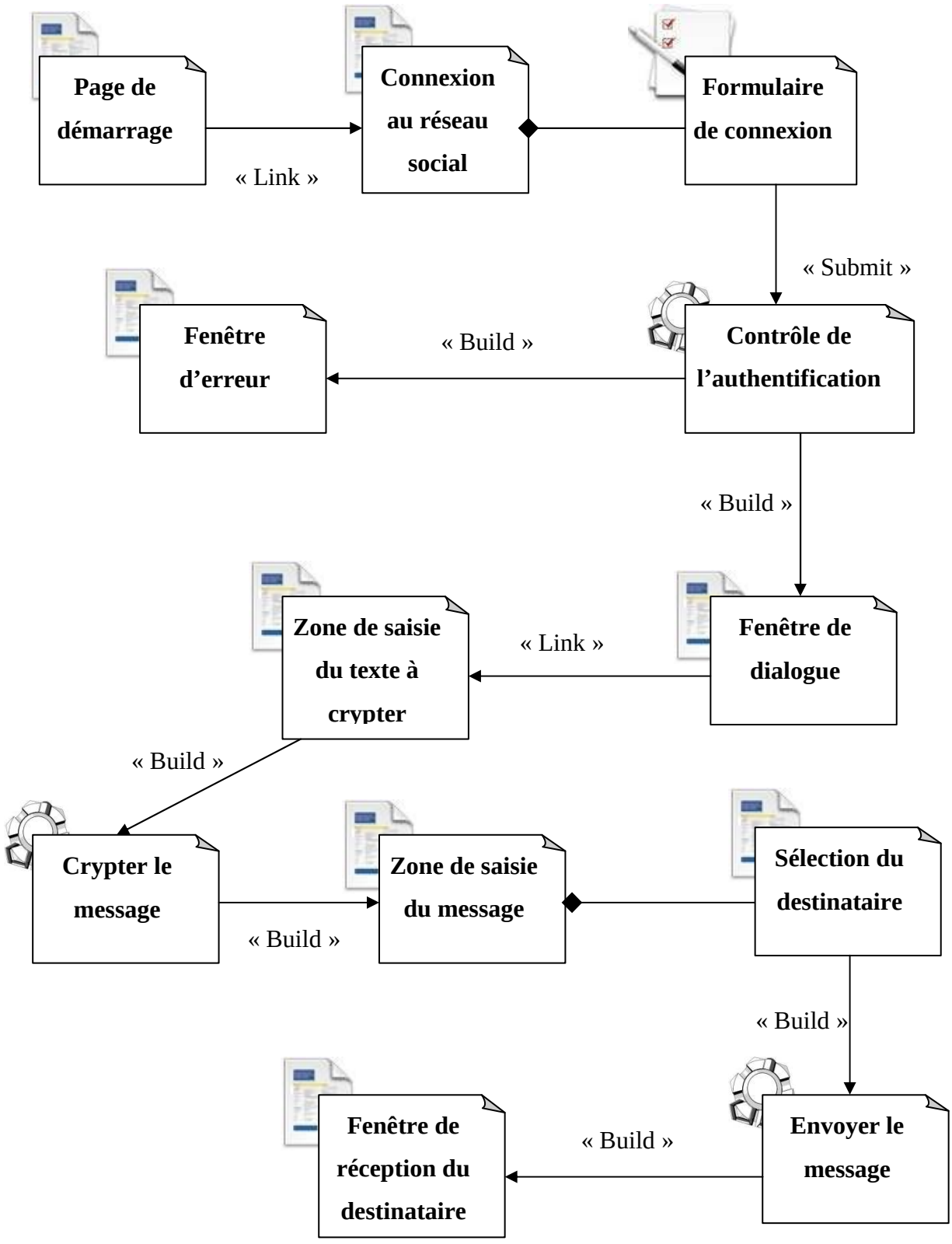


Figure 14 : Diagramme de classe général du cas d'utilisation : « **Envoyer un message en le cryptant »**

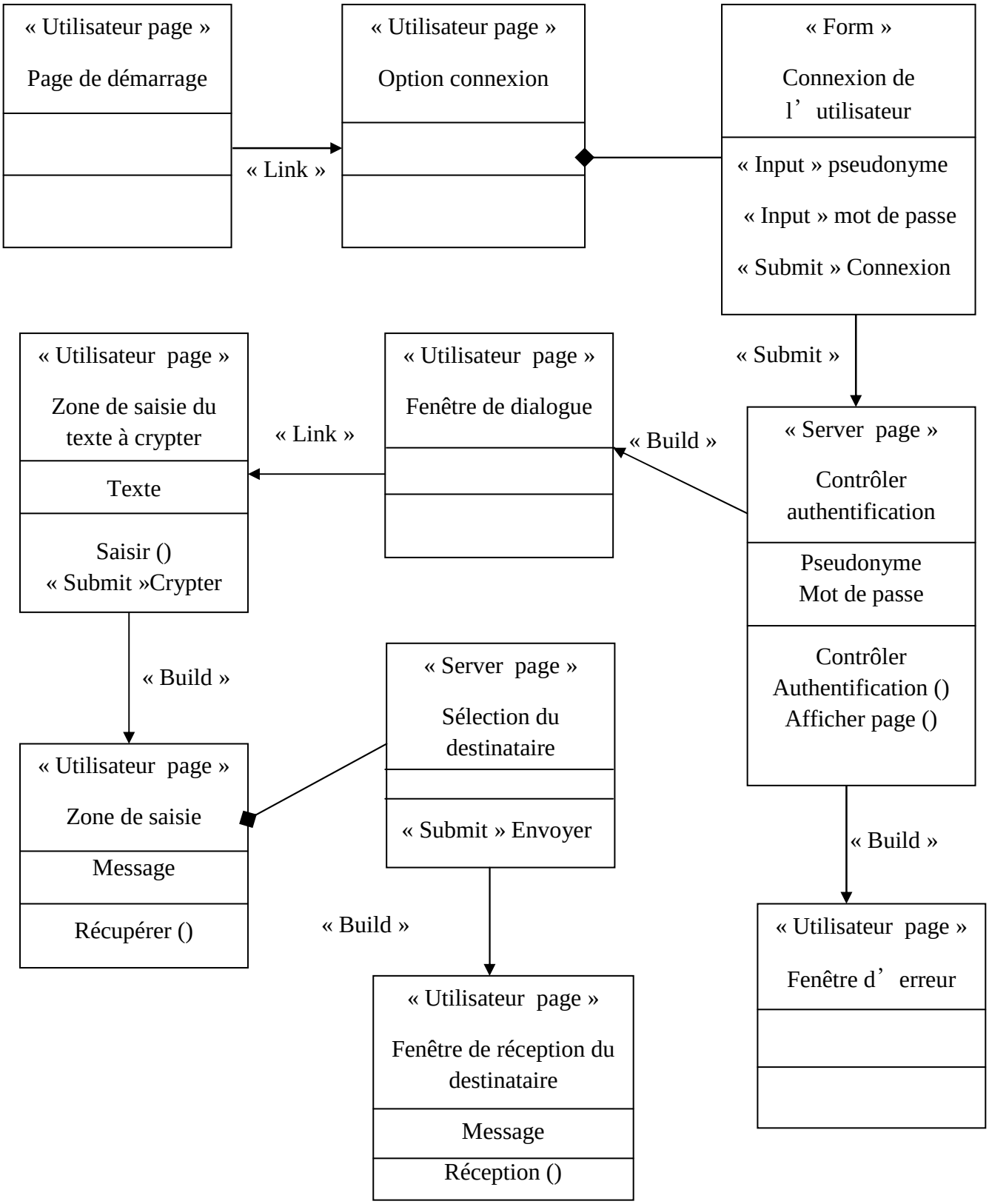


Figure 15 : Diagramme de classe détaillé du cas d'utilisation : « **Envoyer un message en le cryptant »**

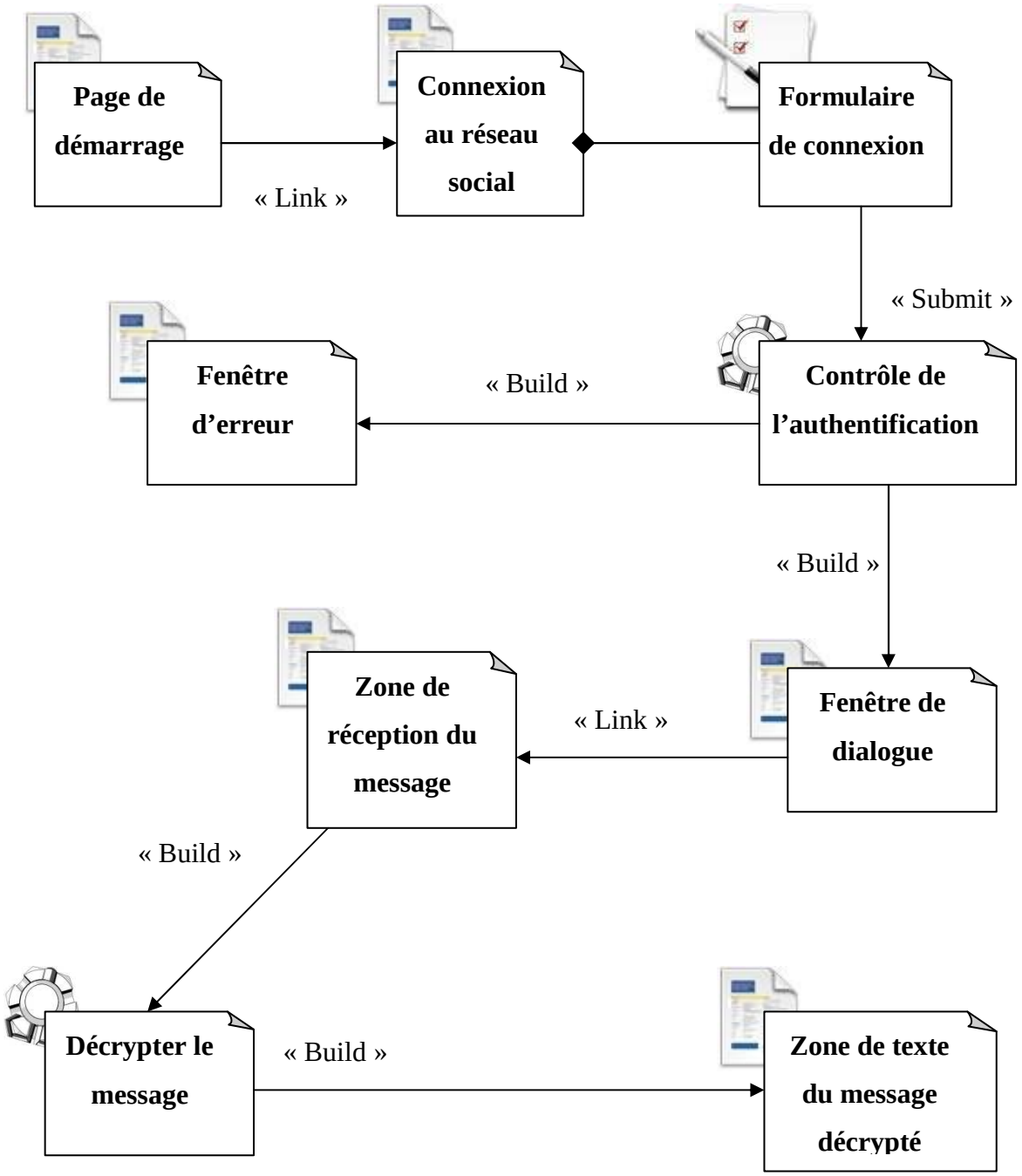


Figure 16 : Diagramme de classe général du cas d'utilisation : « **Décrypter un message reçu »**

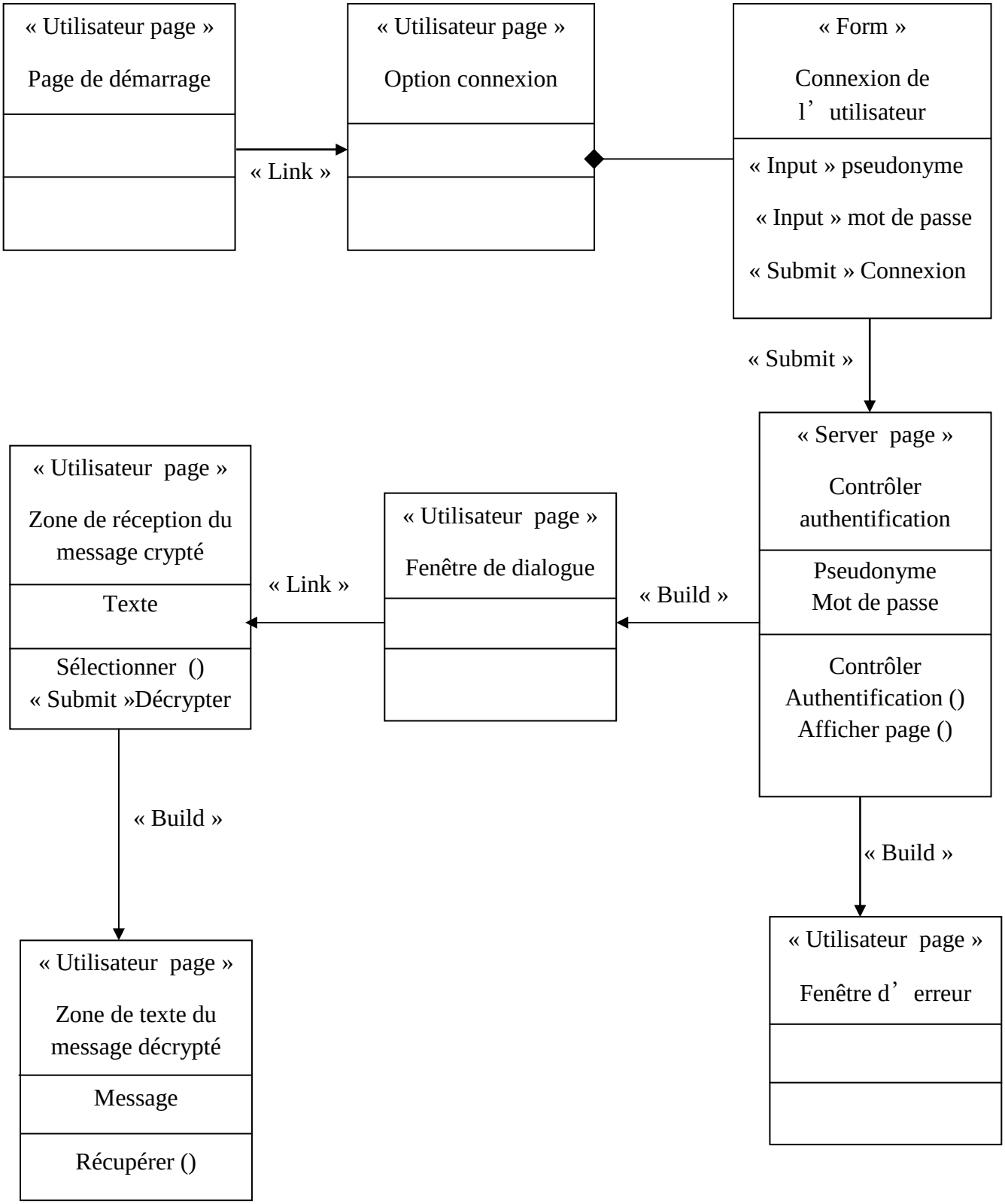


Figure 17 : Diagramme de classe détaillé du cas d'utilisation : « **Décrypter un message reçu »**

Dans ce chapitre, nous avons proposé une démarche de modélisation pour développer notre application.

Cette démarche est basée sur l'UML, nous avons commencé par la spécification des cas d'utilisations dans un premier temps, suivi d'une élaboration des diagrammes de séquences ensuite les diagrammes de classes.

L'application ainsi que les différentes étapes de sa réalisation vous seront présentés dans le chapitre suivant.

Chapitre 5

Outils de développement et Réalisation

La performance et qualité d'une application repose sur le bon choix des outils adéquats répondants aux besoins de cette dernière.

Le schéma ci-dessous résume les différents outils requis pour la réalisation de notre application (voir figure 1 : Schéma récapitulatif des outils retenus).

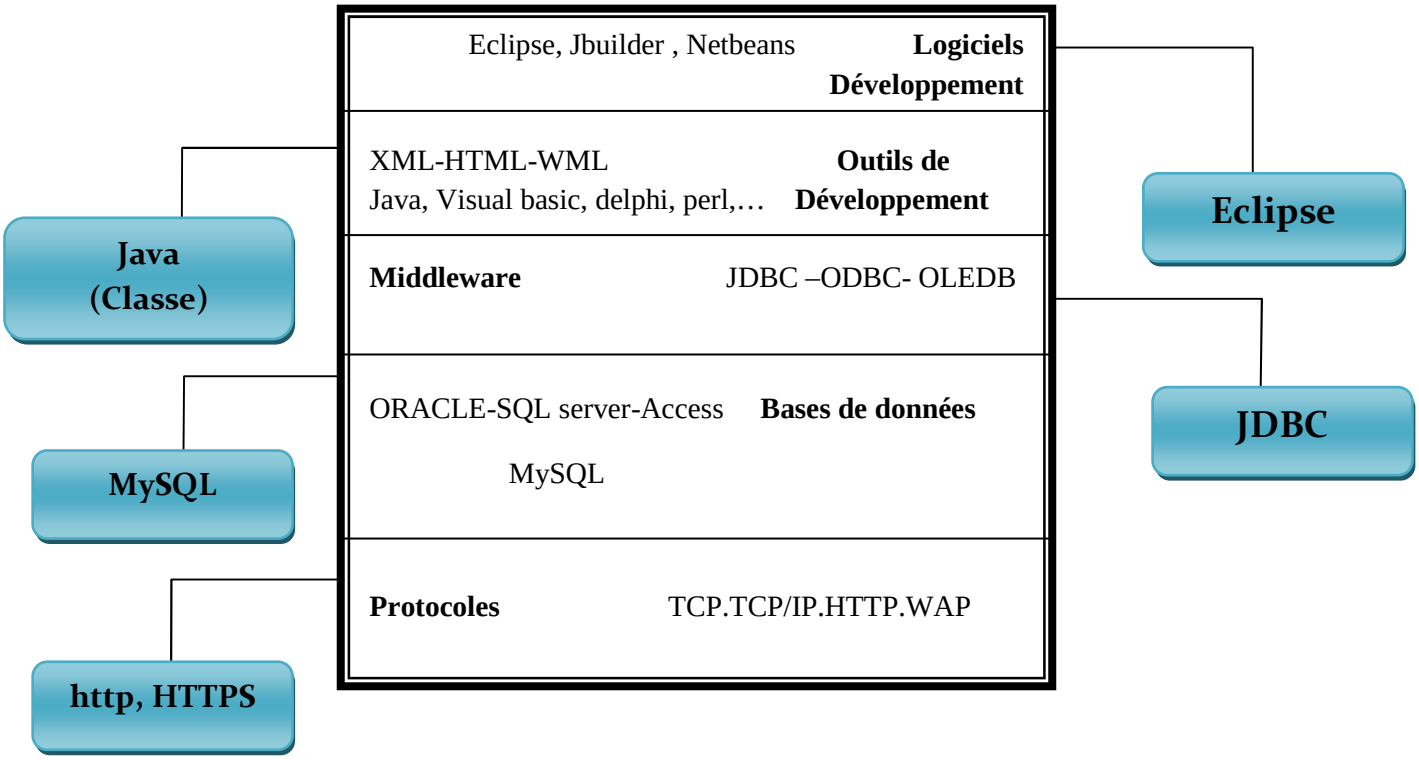


Figure 1 : Schéma récapitulatif des outils retenus

Dans ce qui suit sera présenté les principales motivations de nos choix.

I. Choix des outils technologiques

La réalisation de notre application a nécessité l'utilisation de plusieurs outils de développement, que nous citerons dans ce qui suit :

1. Les langages de programmation

1.1. Le langage java [30]

Le langage Java a la particularité principale que les logiciels écrits avec ce dernier sont très facilement portables sur plusieurs systèmes d'exploitation tels que UNIX, Windows, Mac OS ou GNU/Linux avec peu ou pas de modifications. C'est la plate-forme qui garantit la portabilité des applications développées en Java (voir figure 2 : Indépendance de java des architectures matérielles).

- ✓ Le langage reprend en grande partie la syntaxe du langage **C++**, très utilisé par les informaticiens. Néanmoins, Java a été épurée des concepts les plus subtils du **C++** et à la fois les plus déroutants, tels que les pointeurs et références, et l'héritage multiple remplacé par l'implémentation des interfaces. Les concepteurs ont privilégié l'approche orientée objet de sorte qu'en Java, tout est objet à l'exception des types primitifs (nombres entiers, nombres à virgule flottante, etc.)

- ✓ Java permet de développer des applications client/serveur. Côté client, les applets sont à l'origine de la notoriété du langage. C'est surtout côté serveur que Java s'est imposé dans le milieu de l'entreprise grâce aux servlets, ce pendant le serveur des applets, et plus récemment les JSP (*Java Server Pages*) qui peuvent se substituer à PHP, ASP et ASP.NET.

- ✓ Java a donné naissance à un système d'exploitation (Java OS), à un environnement de développement (Eclipse/JDK), des machines virtuelles (MSJVM, JRE) applicatives multi plates-formes (JVM), une bibliothèque Java (J2ME) avec interface graphique (AWT/Swing), des applications Java (logiciels, servlet, applet).

- ✓ La portabilité du code Java est assurée par la machine virtuelle. JRE – la machine virtuelle qui effectue la traduction et l'exécution du bytecode en code natif – supporte plusieurs processus de compilation (à la volée/bytecode, natif). La portabilité est dépendante de la qualité de portage des JVM sur chaque OS.

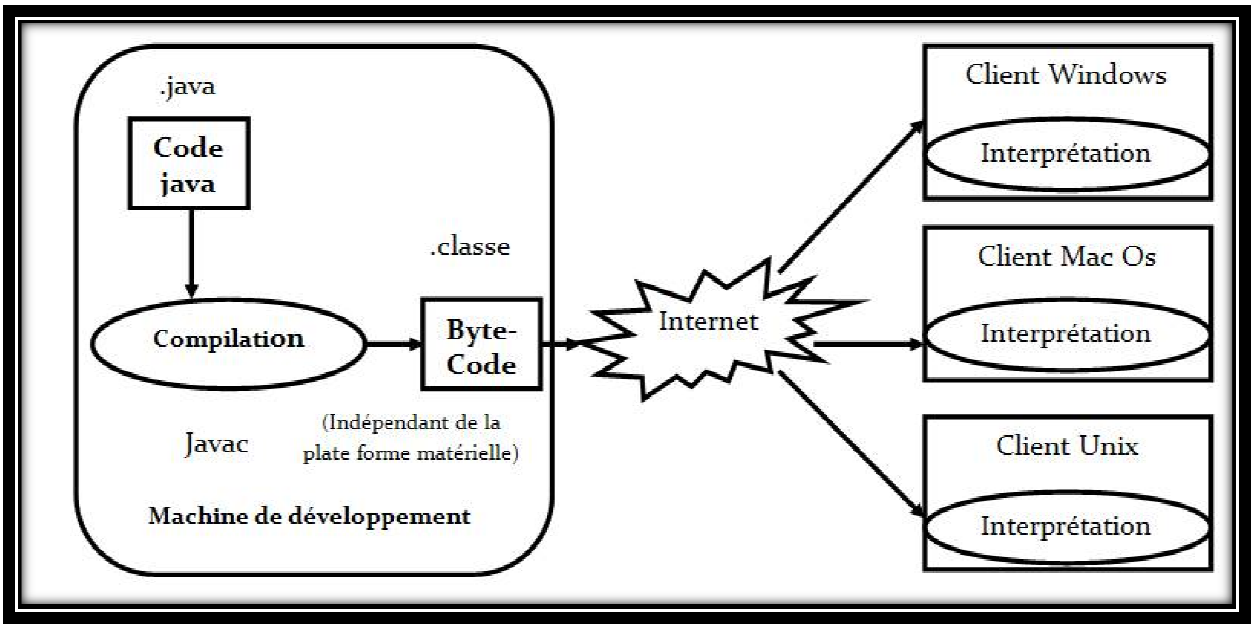


Figure 2 : Indépendance de java des architectures matérielles

1.1.1. Les classes (technique de développement)

Une classe est la description de données appelées **attributs**, et d'opérations appelées **méthodes**.

Une classe est un modèle de définition pour des objets ayant le même ensemble d'attributs, et le même ensemble d'opérations.
A partir d'une classe on peut créer un ou plusieurs objets par **instanciation** ; chaque objet est une **instance** d'une seule classe.

Les caractéristiques de la programmation objet sont :

- Encapsulation des données (attributs) et des comportements (méthodes) : les attributs et les méthodes sont définies dans le même environnement (capsule).
- Masquage de l'information : l'utilisateur de la classe peut ne pas avoir accès directement aux attributs.
- Héritage : on peut définir une classe à partir d'une autre classe.
- Polymorphisme : une même méthode peut avoir un comportement différent en fonction de l'instance à la quelle est appliquée.

a. *Définition d'une classe :*

```
class X extends Y{
    // liste des attributs
    // liste des méthodes
}
```

Si *Y* est la classe de base de la hiérarchie des objets Java *Object*, alors la partie *extends* est facultative.

Exemple :

```
class A extends  Object{
    int a ;
    void f(){
        ...
            }
                    }
```

est équivalent à

```
class A {
    int a ;
    void f(){
        ...
    }
}
```

Une classe a une visibilité :

- **Public** le mot *class* est alors précédé de *public*, tout utilisateur qui importe le paquetage peut utiliser la classe. Dans ce cas elle doit être définie dans un fichier qui a pour nom le nom de la classe.
- **Privé** le mot *class* est alors précédé de *private*, seules des classes définies dans le même fichier peuvent utiliser cette classe.
- **Paquetage** le mot *class* n'est pas précédé de mot particulier, toutes les classes du paquetage peuvent utiliser la classe.

b. *Création d'instances*

Pour créer une instance de la classe *A*, on écrira :

```
A a ;        // définition de la variable référence
a = new A() ; // création de l'instance
```

La création d'une instance par l'opérateur **new** se déroule en trois temps :

- Réservation de l'espace mémoire suffisamment grand pour représenter l'objet.
- Appel du constructeur de l'objet. Initialisation des attributs, et d'une référence à l'objet représentant la classe de l'instance en train d'être créée.
- Renvoi d'une référence sur l'objet nouvellement créé

```
class Point {
  int x ;
  int y ;
    . . .
}

Point a,  b ;
a = new  Point(…) ;
b = a;
```

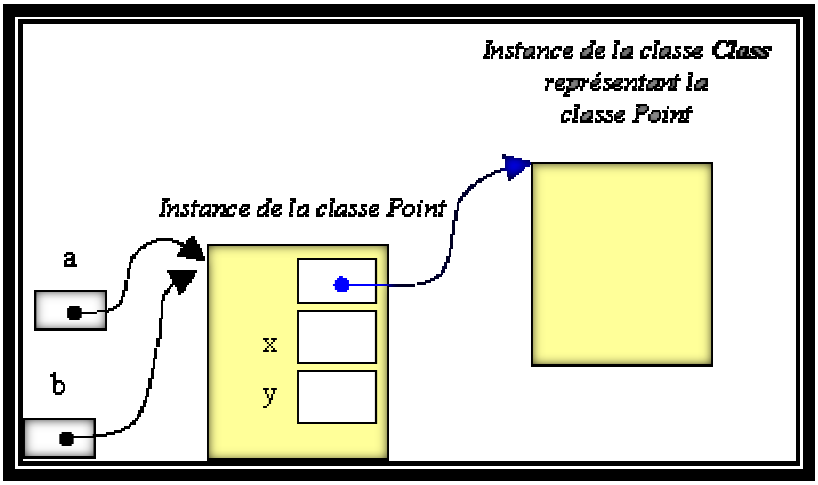


Figure 3 : Instance d'une classe java

La destruction des instances se fait automatiquement par un « *thread* » le *garbage collector* qui cherche tous les objets qui ne sont plus référencés et les supprime. Le *garbage collector* peut être appelé directement par *System.gc()*.

1.1.2. L'exécution d'une classe java

Pour exécuter des applications en JAVA sur un système, il faut avoir une machine virtuelle. Cette machine virtuelle va interpréter le code compilé, code généré à partir des fichiers *.java*

La compilation des fichiers .java en fichiers .class se fait au moyen de la commande javac NomFichier.java. Pour exécuter ensuite ce fichier qui vient d'être généré.

» Portabilité :

L'un des gros avantages du langage JAVA est sa portabilité. La portabilité signifie que le programme écrit une seule fois fonctionnera sur une grande quantité de plateformes différentes, sans nécessiter une quelconque modification du code. Seule la machine virtuelle qui interprète les fichiers précompilés subit des modifications.

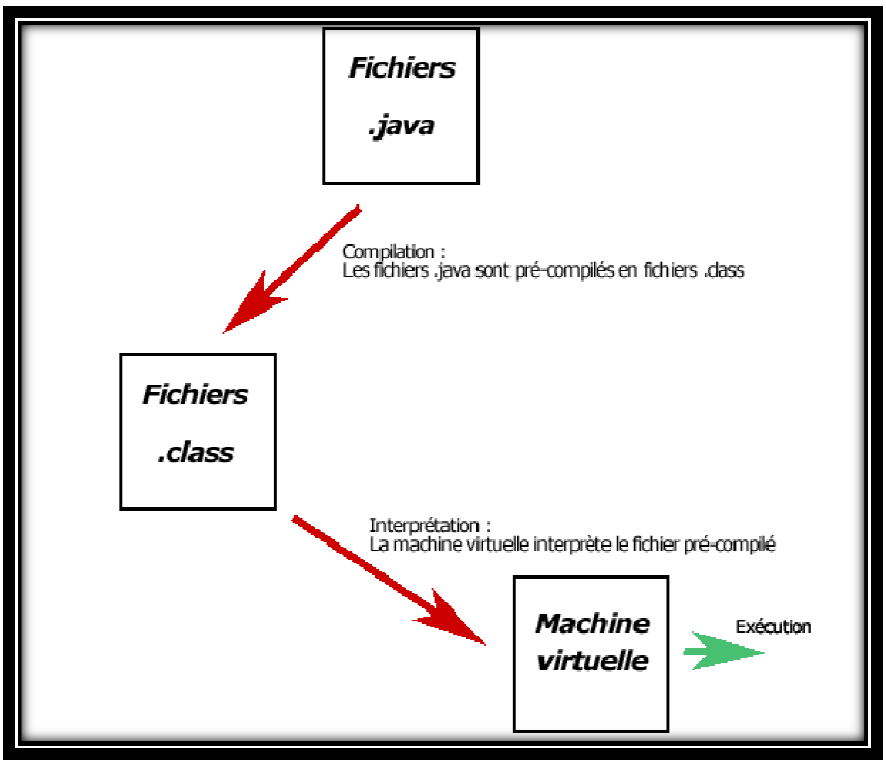


Figure 4:Exécution d'une classe java

1.1.3. Structure et cycle de fonctionnement d'une classe [31]

Une classe ou une interface suit un cycle de vie particulier dans la machine virtuelle de son chargement à son retrait.

1. Chargement.
2. Liaison.
3. Initialisation.
4. Instanciation.
5. Récupération de la mémoire.
6. Finalisation.
7. Déchargement.

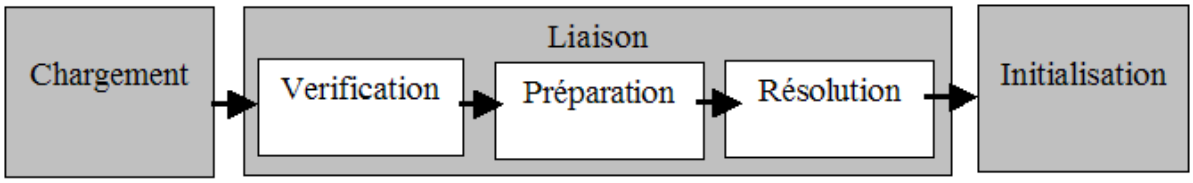


Figure 5:Cycle de vie d'une classe java

Chaque étape est dédiée à une tâche spécifique :

- chargement (load) : permet de lire le bytecode dans la machine virtuelle
- liaison (link) : permet de rendre utilisable le bytecode. Cette étape est composée de trois processus (vérification, préparation, résolution)
  - ✓ La vérification (verify) permet de s'assurer que le bytecode est compatible avec la machine virtuelle
  - ✓ La préparation (prepare) effectue l'allocation mémoire nécessaire à la classe
  - ✓ La résolution (resolve) transforme les références symboliques du constant pool en références mémoire.
- Initialisation (initialize) : initialisation des valeurs des variables.

1.1.3.1. Le chargement des classes

La machine virtuelle charge, lie et initialise les classes et interfaces requises à l'exécution.

Le démarrage d'une application commence par le chargement de sa classe principale (celle fournie en paramètre de la JVM)

Toutes les classes utilisées pour l'instanciation de cette classe et celles utilisées dans sa méthode main () sont chargées à leur première utilisation.

1.1.3.2. La liaison de la classe

La liaison de la classe comporte trois étapes :

- La vérification
- La préparation
- La résolution

La vérification est la première étape du processus de liaison : elle permet de s'assurer que la classe chargée est conforme aux spécifications et qu'elle ne risque pas de dégrader la machine virtuelle. La vérification consiste donc en une analyse de la structure et des informations de la classe.

Les spécifications de la JVM détaillent une liste d'exceptions et d'erreurs qui doivent être levées lors de cette étape.

La vérification effectue de nombreux contrôles sur le bytecode tel que :

- Vérifie les instructions (utilisation d'instructions valides, véracité des sauts, ...)
- Vérifie les déclarations d'entités du constant pool (numéro de classes, de méthodes, de champs, ...)
- Recherche les classes mères et vérifie que toutes les classes héritent de la classe Object (sauf la classe Object elle-même).
- Vérifie que les classes finales n'ont pas de classes fille
- Vérifie que les méthodes finales ne sont pas réécrites
- Vérifie que les méthodes des interfaces implémentées soient définies
- Vérifie que deux méthodes n'ont pas la même signature
- ...

Certains de ces contrôles nécessitent des informations sur les classes parentes ou sur d'autres classes utilisées qui seront alors chargées mais pas initialisées.

Tous ces contrôles peuvent paraître redondants avec ceux effectués par le compilateur lors de la génération du bytecode mais en fait, il est tout à fait possible que le bytecode ait été altéré, généré à la volée ou que le compilateur possède un ou plusieurs bugs.

Durant l'étape de préparation, la machine virtuelle alloue la mémoire requise par chaque champs et initialise leurs valeurs avec la valeur par défaut de leur type respectif.

1.1.3.3. L'initialisation de la classe

Ce processus a pour rôle d'initialiser les variables de classe avec leur valeur initiale tel que définit dans le code source. La valeur initiale peut être définie de deux façons :

- Lors de la déclaration du champ static
- Dans un bloc d'initialisation static

```
public class MaClasse {
  static List maListe1 = new ArrayList() ;
  static List maListe2 = null;

  static {
    maListe2 = new ArrayList();
  }
}
```

Figure 6 : Initialisation de classe

Les spécifications de la JVM imposent que l'initialisation d'une classe intervienne à sa première utilisation active :

- Création d'une nouvelle instance en utilisant l'opérateur new
- Création d'un tableau de la classe
- Utilisation d'un membre de la classe qui ne soit pas hérité ni ne soit une constante
- Utilisation d'une de ses sous classes (l'initialisation d'une classe impose l'initialisation de toutes ses super classes).

1.2. Environnement de développement(Eclipse)

Eclipse est un environnement de développement intégré, libre, extensible, universel et polyvalent, permettant de créer des projets de développement mettant en œuvre n'importe quel langage de programmation. Eclipse IDE est principalement écrit en Java (à l'aide de la bibliothèque graphique SWT, d'IBM), et ce langage, grâce à des bibliothèques spécifiques, est également utilisé pour écrire des extensions.

La spécificité d'Eclipse IDE vient du fait de son architecture totalement développée autour de la notion de plugin (en conformité avec la norme OSGi) : toutes les fonctionnalités de cet atelier logiciel sont développées en tant que plug-in. [32][33]

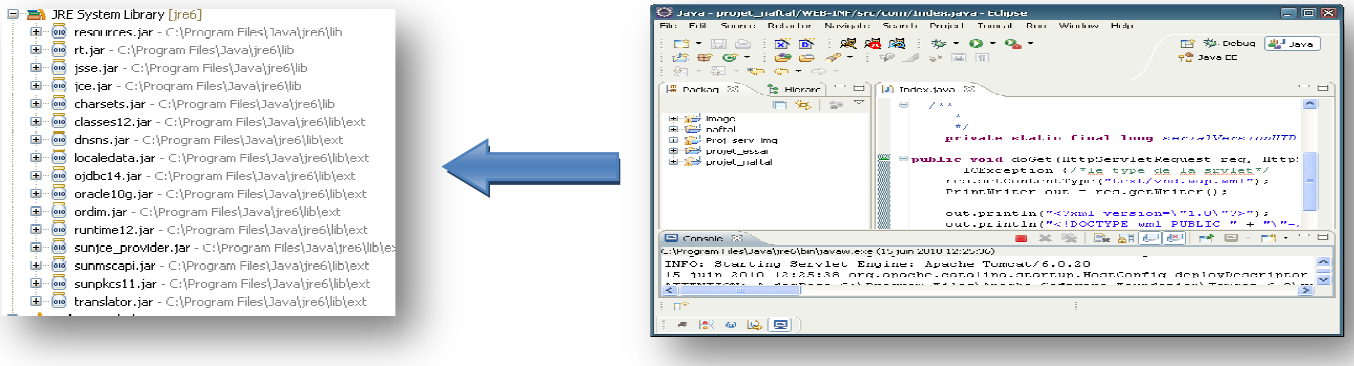


Figure 7 : Plate -forme Eclipse

- ✓ **Les avantages d'Eclipse :**

Eclipse possède de nombreux points forts qui sont à l' origine de son énorme

Succès dont les principaux sont :

- ➢ Une plate-forme ouverte pour le développement d'applications et extensible grâce a un mécanisme de plug-ins
- ➢ Plusieurs versions d'un même plug-in peuvent cohabiter sur une même plateforme.
- ➢ Un support multi langage grâce a des plug-ins dédies : Cobol, C, PHP, C# , ...
- ➢ Support de plusieurs plateformes d'exécution : Windows, Linux, Mac OS X, ...
- ➢ Malgré son écriture en Java, Eclipse est très rapide à l'exécution grâce a l'utilisation de la bibliothèque SWT

Pour notre application, nous avons choisit Eclipse Galileo, version plate-forme 3.5, apparu en juin 2009.

Package de classe	Rôle
Java.io	Fournit des classes pour les entrées/sorties systèmes, les flots de données, la sérialisation et les systèmes de fichiers.
Javax.sql	Permet au serveur de traiter des requêtes de toutes nature dans un environnement reparti et plus particulièrement des requêtes http.
Java.sql	Fournit un certain nombre d'interfaces et classes permettant la connexion à une base de données ainsi que la soumission des requêtes SQL.

Tableau 1 : Les différents packages de classe dans Eclipse

1.3. Le serveur de données MySQL

La base de données MySQL est devenue la base de données open source la plus populaire au monde grâce à sa haute performance, sa fiabilité et sa simplicité d'utilisation. Beaucoup des sociétés les plus importantes et à forte croissance telles que Google, Lafarge, EADS, Alcatel-Lucent, Nokia et You Tube, réduisent leurs coûts de manière significative en utilisant MySQL pour leurs sites Web, leurs applications critiques d'entreprise, ou en embarquant MySQL au sein de leurs solutions. Non seulement MySQL est la base de données open source la plus populaire au monde mais elle est aussi devenue le choix privilégié pour la nouvelle génération d'applications développées sur la pile LAMP (Linux, Apache, MySQL, PHP / Perl / Python.). MySQL fonctionne sur plus de 20 plates-formes incluant Linux, Windows, OS/X, HP-UX, AIX, Netware, vous offrant une grande flexibilité. [34]

Figure 8 : Login de serveur de données MySQL

1.4. L'outil MySQL-Front

C'est un logiciel graphique de gestion de bases de données MySQL. On peut directement manipuler les bases, tables, champs et données par le biais de l'interface graphique mais également transmettre des scripts SQL au SGBD MySQL. MySQL Front n'est toutefois disponible que sous Windows et il n'y a qu'une version de démonstration de 11 jours disponible en téléchargement.

1.5. Le middleware Java Data Base Connectivity(JDBC)

1.5.1. Qu'est ce que le JDBC [30][35]

La technologie *JDBC* (*Java DataBase Connectivity*) est une API fournie avec Java (depuis sa version 1.1) permettant de se connecter à des bases de données, c'est-à-dire que *JDBC* constitue un ensemble de classes permettant de développer des applications capables de se connecter à des serveurs de bases de données (*SGBD*).

L'API JDBC a été développée de telle façon à permettre à un programme de se connecter à n'importe quelle base de données en utilisant la même syntaxe, c'est-à-dire que l'*API JDBC* est indépendante du *SGBD.*
De plus, *JDBC* bénéficie des avantages de Java, dont la portabilité du code, ce qui lui vaut en plus d'être indépendant de la base de données d'être indépendant de la plate-forme sur laquelle elle s'exécute.

1.5.2. Les avantages du JDBC

La combinaison Java/JDBC possède de nombreux avantages nous citerons entre autres les points suivants :

a. La possibilité d'écrire du code applicatif pour le traitement des bases de données indépendamment de tout outil ou de tout langage propriétaire.

b. La possibilité d'exécuter le code applicatif en question sur n'importe quel type de plate-forme disposant d'une machine virtuelle : Windows, Linux, Mac, Palm, Téléphones mobiles, ...etc.

c. Les dernières versions de JDBC apportent encore de nouvelles possibilités (le traitement des requêtes en opérant des déplacements autres que séquentiels et des mises à jour directes sur les bases de données, les traitements par lots, d'autres types de données, l'utilisation des transactions)

II. Réalisation de la solution

Après avoir fixé nos choix sur les outils technologiques mentionnés dans la partie précédente, place á la réalisation, qui fera l'objet de ce chapitre.

Nous commencerons par une présentation du système, et son architecture, nous poursuivrons par spécifier les pas suivis lors du développement de l'application, ainsi nous énumérerons les différents services qu'offre le système.

1. Présentation du système

Notre système est un réseau social appelé à être utilisés dans le niveau local comme dans le niveau mondial via internet.

L'objectif de cette solution est de pouvoir protéger la vie privée des internautes des hackers, des espions …, grâce à l'introduction de la cryptographie.
Le principe est celui de Zimmermann [5]:

[5] http://www.philzimmermann.com/EN/background/index.html

C'est de pouvoir communiquer de manière intègre en utilisant un algorithme à clé secrète (c'est l'algorithme AES). Et de se mettre d'accord sur la clé secrète par un protocole d'échange de clés. Ce genre de protocole utilise des propriétés de cryptographie à clé publique.
Ensuite de communiquées en utilisant l'algorithme AES qui est à clé privée. Une fois que leur conversation est terminée, ils jettent la clé de session.

*« **Si l'intimité est mise hors la loi, seuls les hors-la-loi auront une intimité**. »*

2. Architecture du système [36]

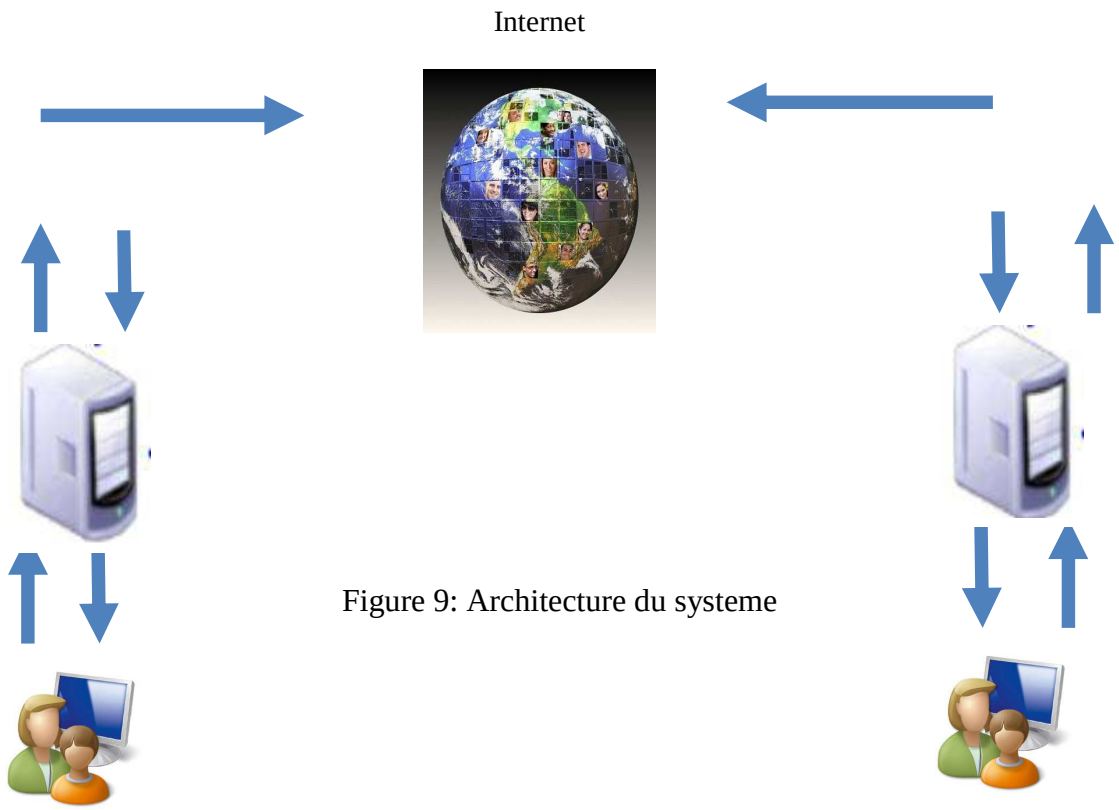


Figure 9: Architecture du systeme

Notre système est doté d'une architecture á 3 niveaux (appelée architecture 3-tiers), ou il existe un niveau intermédiaire, c'est-á-dire que l'on a généralement une architecture partagée entre :

- Couche présentation
- Couche métier
- Couche accès aux données

Cette architecture peut être définie comme étant un modèle logique d'architecture applicative qui vise à s'éparer très nettement trois couches logicielles au sein d'une même application ou système, á modéliser et présenter cette application comme un empilement de trois strates dont le rôle est clairement défini :
- La *présentation des données* : correspondant à l'affichage, la restitution sur le poste de travail, le dialogue avec l'utilisateur

- Le *traitement métier des données* : correspondant á la mise en œuvre de l'ensemble des règles de gestion et de la logique applicative

-Et en fin l'*accès aux données persistantes* (persistancy en anglais) : correspondant aux données qui sont destinées á être conservées sur la durée, voire de manière définitive.

3. Développement de l'application

Nous avons bâti notre application avec une panoplie de classes, servant á effectuer les traitements nécessaires, cette ultime phase comporte un certain nombre d'étapes qui se succèdent.

Nous avons entamé la réalisation de notre système par la création de notre base au sein du SGBD SQL.

3.1. Création d'une classe

Après l'installation et la configuration de tous les outils nécessaires (la JVM, l'environnement Eclipse).

Pour créer une classe dans l'environnement Eclipse, il faudra tous d'abord :

- Démarrer l'environnement Eclipse

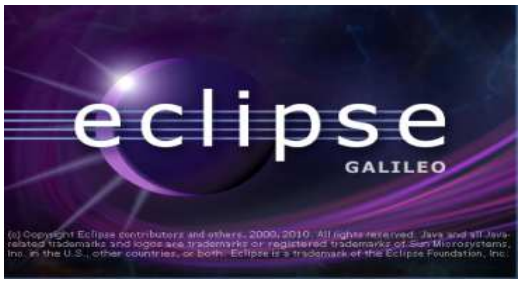


Figure 10 : Démarrage de l'environnement Eclipse

- Créer un nouveau projet java

En premier lieu, il faudra choisir le type de projet que l'on souhaite créer en suivant les instructions portées sur la figure suivante(voir figure 10 : Création d'un projet java):

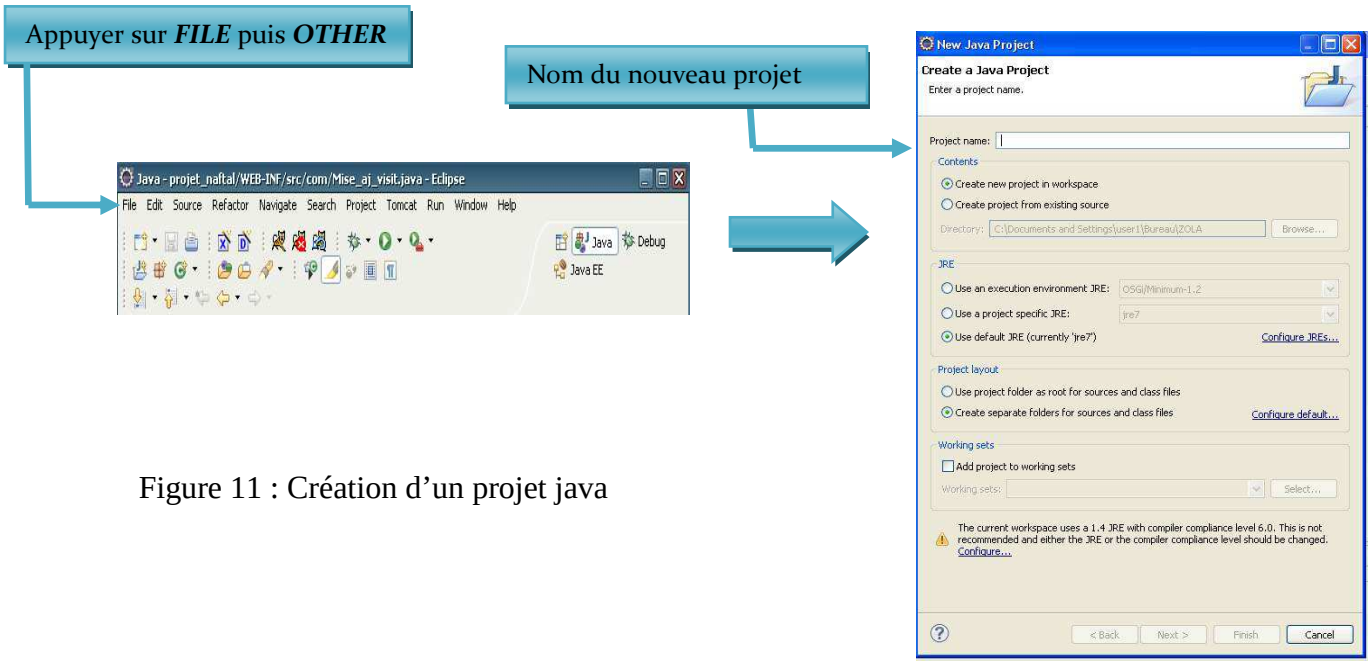


Figure 11 : Création d'un projet java

Après la création du nouveau projet, ce dernier contiendra toutes les librairies nécessaires. Ces dernières seront affichées sur le coté gauche de la fenêtre (voir figure 11 : Affichage du projet et de tous ses attributs) :

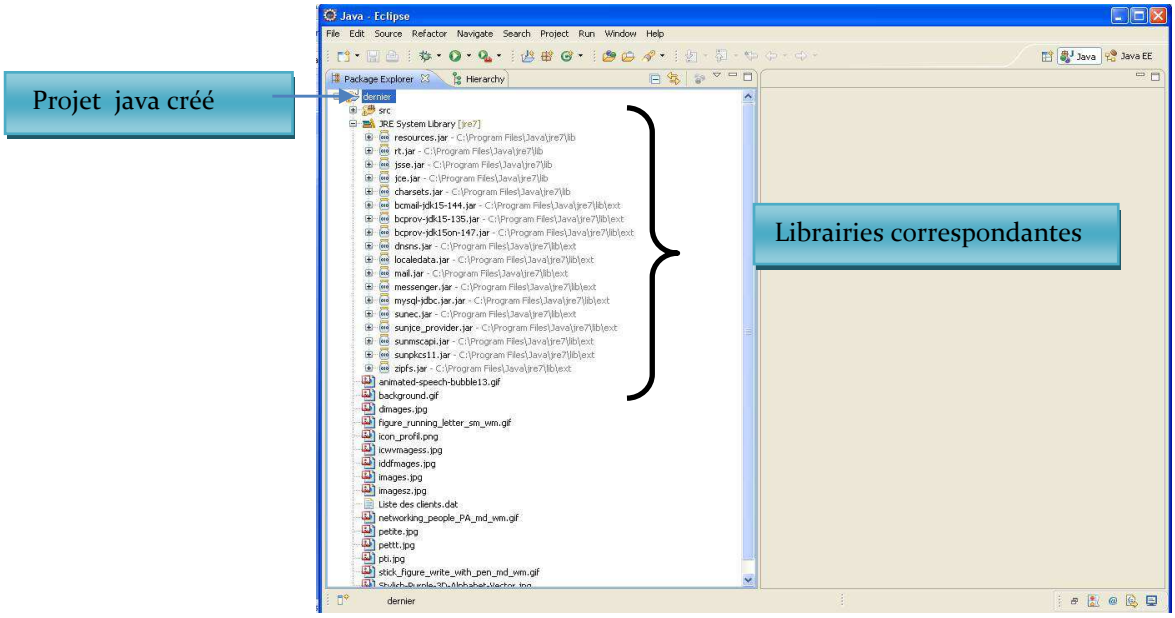


Figure 12 : Affichage du projet et de tous ses attributs

Maintenant, il vous faut créer une nouvelle classe dans le projet java, pour cela, sélectionner le projet crée au paravent puis suivre les instructions portées sur la figure ci-dessous (voir figure 13 : Création d'une nouvelle classe à l'intérieur du projet java) :

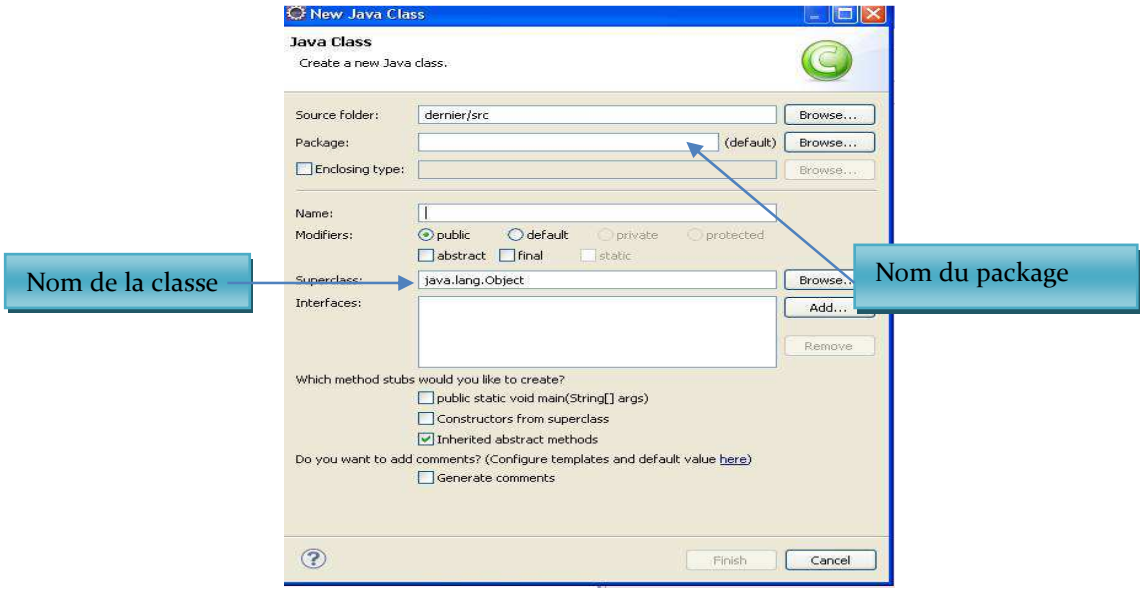
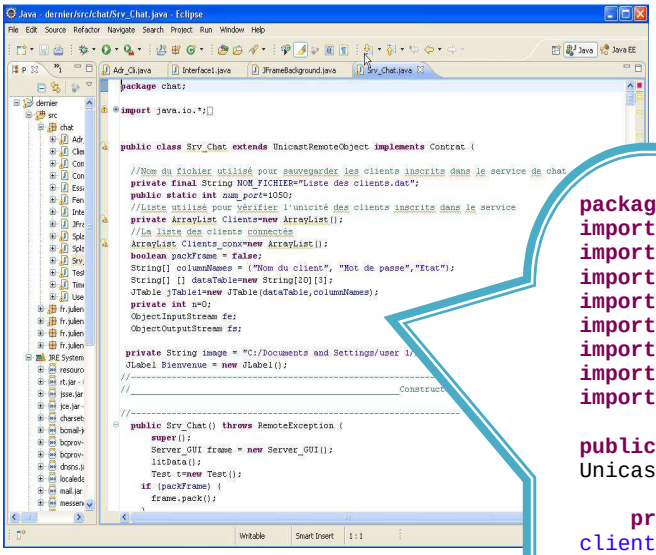


Figure 13 : Création d'une nouvelle classe



```
package chat;
import java.io.*;
import java.net.*;
import java.rmi.*;
import java.awt.event.*;
import javax.swing.*;
import javax.swing.border.*;
import java.io.DataInputStream;
import java.io.DataOutputStream;

public class Srv_Chat extends
UnicastRemoteObject implements Contrat {

    private final String NOM_FICHIER="Liste des
clients.dat";
  public static int num_port=1050;
  private ArrayList Clients=new ArrayList();

  ArrayList Clients_conx=new ArrayList();
  boolean packFrame = false;
  String[] columnNames = {"Nom du client", "Mot
de passe","Etat"};
  String[] [] dataTable=new String[20][3];
  JTable jTable1=new
JTable(dataTable,columnNames);
  private int n=0;
   ObjectInputStream fe;
……
```

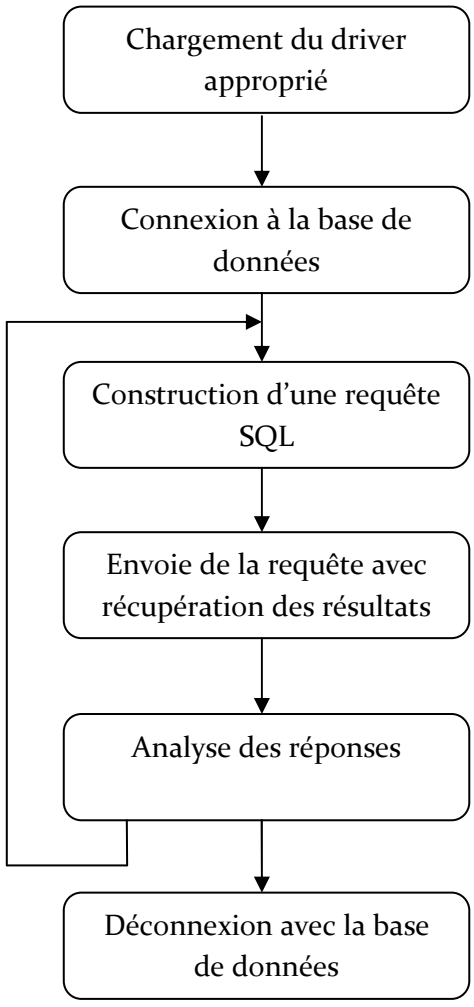
Figure 14 : Exemple d'une classe java

4. Déploiement de l'application

L'application proposée est un ensemble de classes, la méthode de déploiement et création est la même que celle citée précédemment, seul le nombre de classes du projet créé changes.

4.1. Algorithme d'accès à la base de données

La réalisation d'un programme JDBC permettant l'accès à la base de données est montrée dans l'algorithme qui suit (voir l'Algorithme 1 : Structure d'un programme JDBC) :



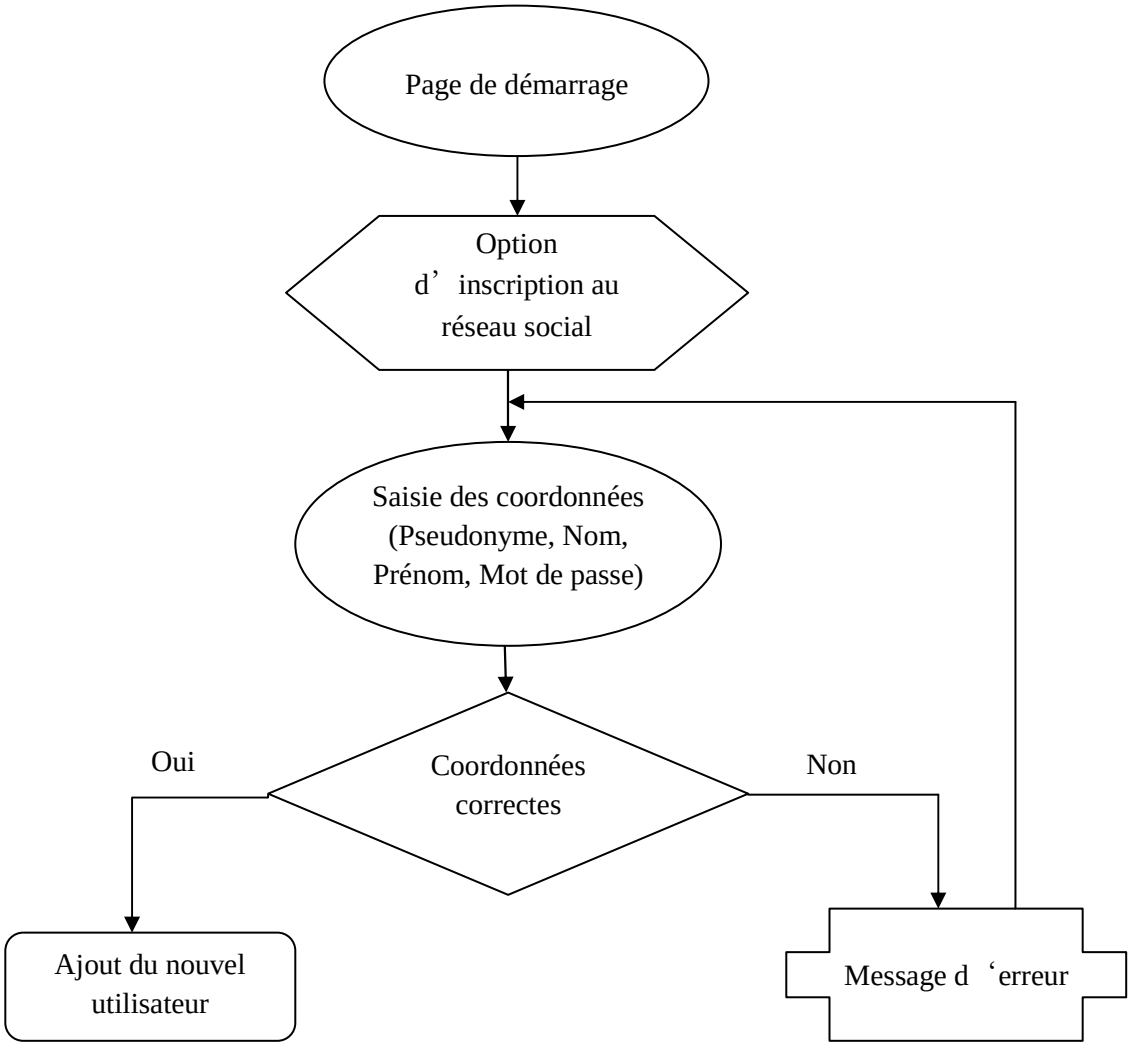
Algorithme 1 : Structure d'un programme JDBC

IV. Mise en œuvre de la solution

➢ Inscription d'un utilisateur

L'inscription d'un utilisateur suit les étapes suivantes (voir Algorithme 2 : Organigramme de l'exécution de l'inscription)

❖ **Algorithme de fonctionnement :**

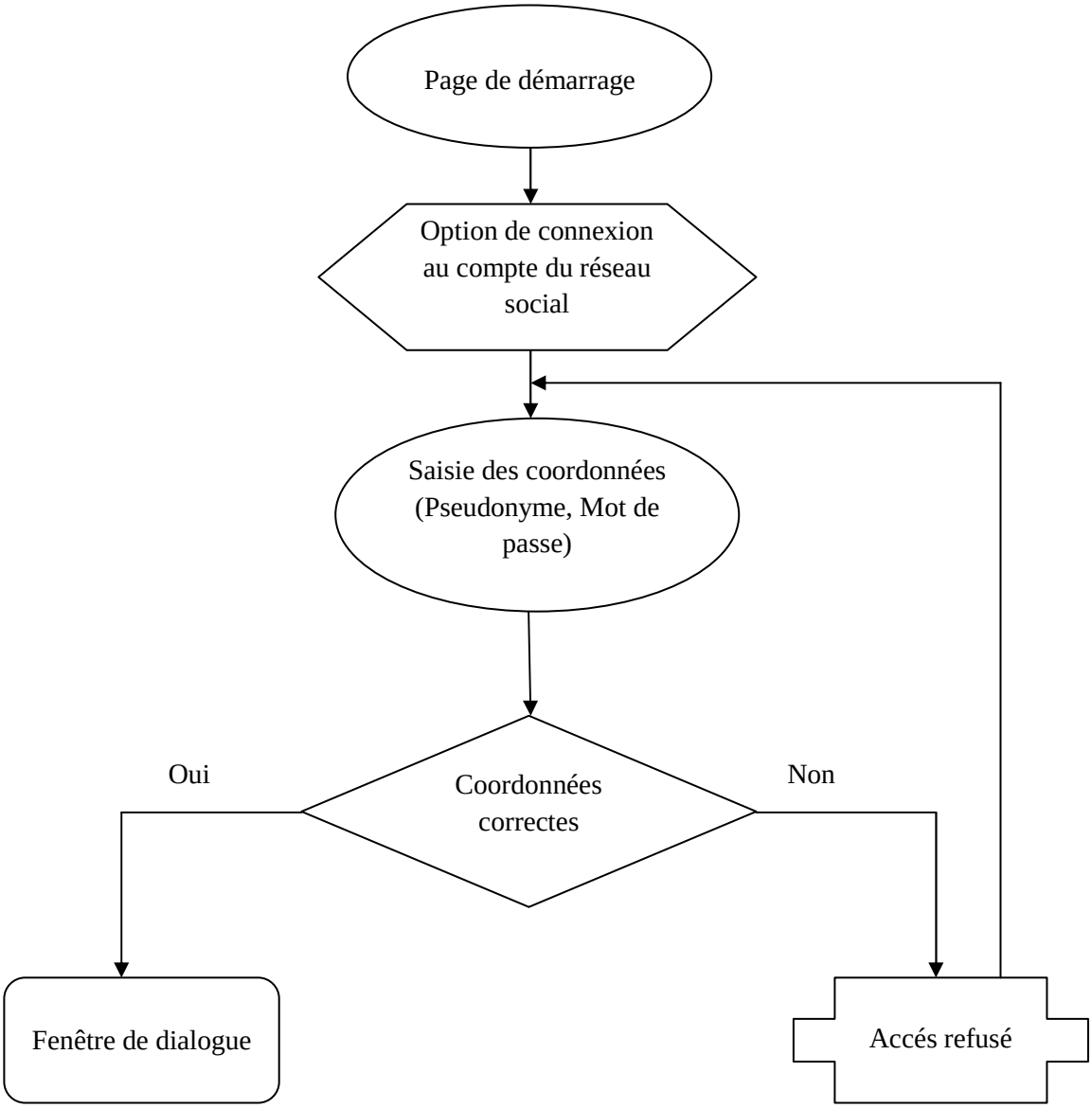


Algorithme 2: Organigramme de l'exécution de l'inscription

➢ Connexion d'un utilisateur à son compte

La connexion d'un utilisateur à son compte suit les étapes suivantes (voir Algorithme 3 : Organigramme de l'exécution de la connexion)

❖ **Algorithme de fonctionnement :**



Algorithme 3 : Organigramme de l'exécution de la connexion

- **Présentation de l'application**

✓ **Page de démarrage**

C'est la page qui apparait à l'écran de l'utilisateur lors du lancement de l'application (voir figure 15 : Page de démarrage)

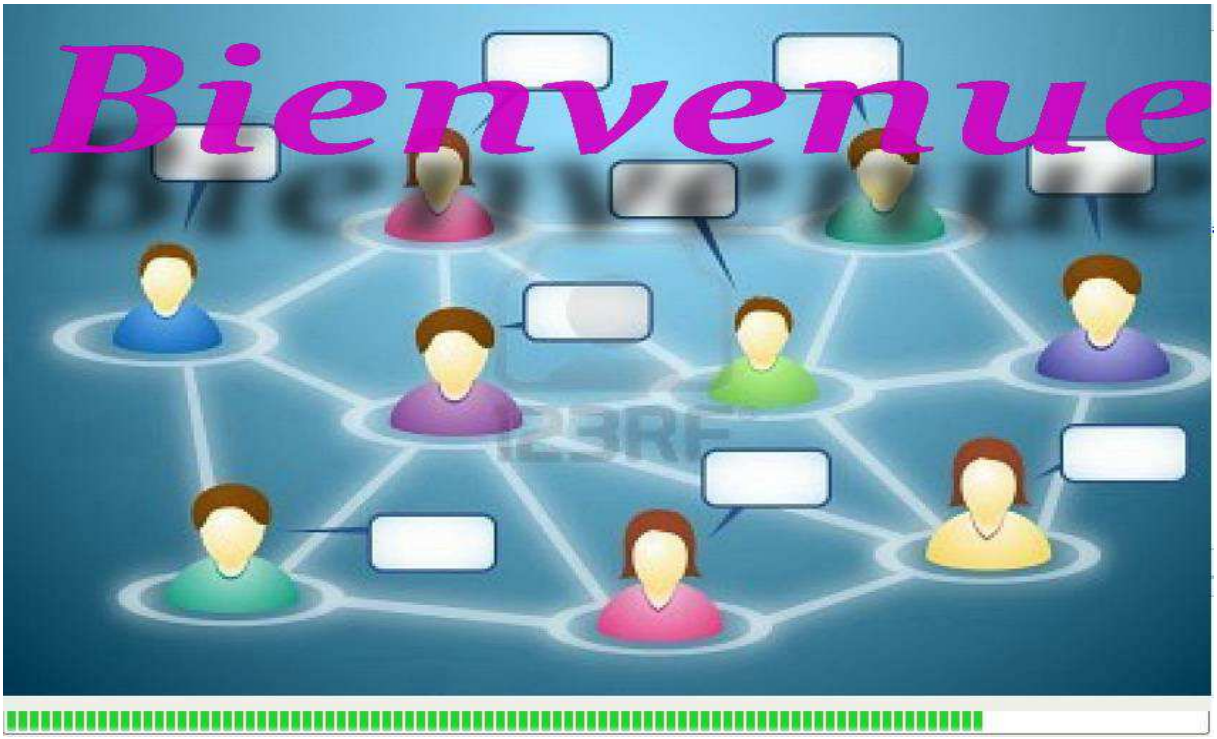


Figure 15 : Page de démarrage

✓ Page d'accueil

Elle contient tous les liens vers les autres pages. Elle permet à l'utilisateur de s'inscrire au réseau social, de se connecter à son compte,….

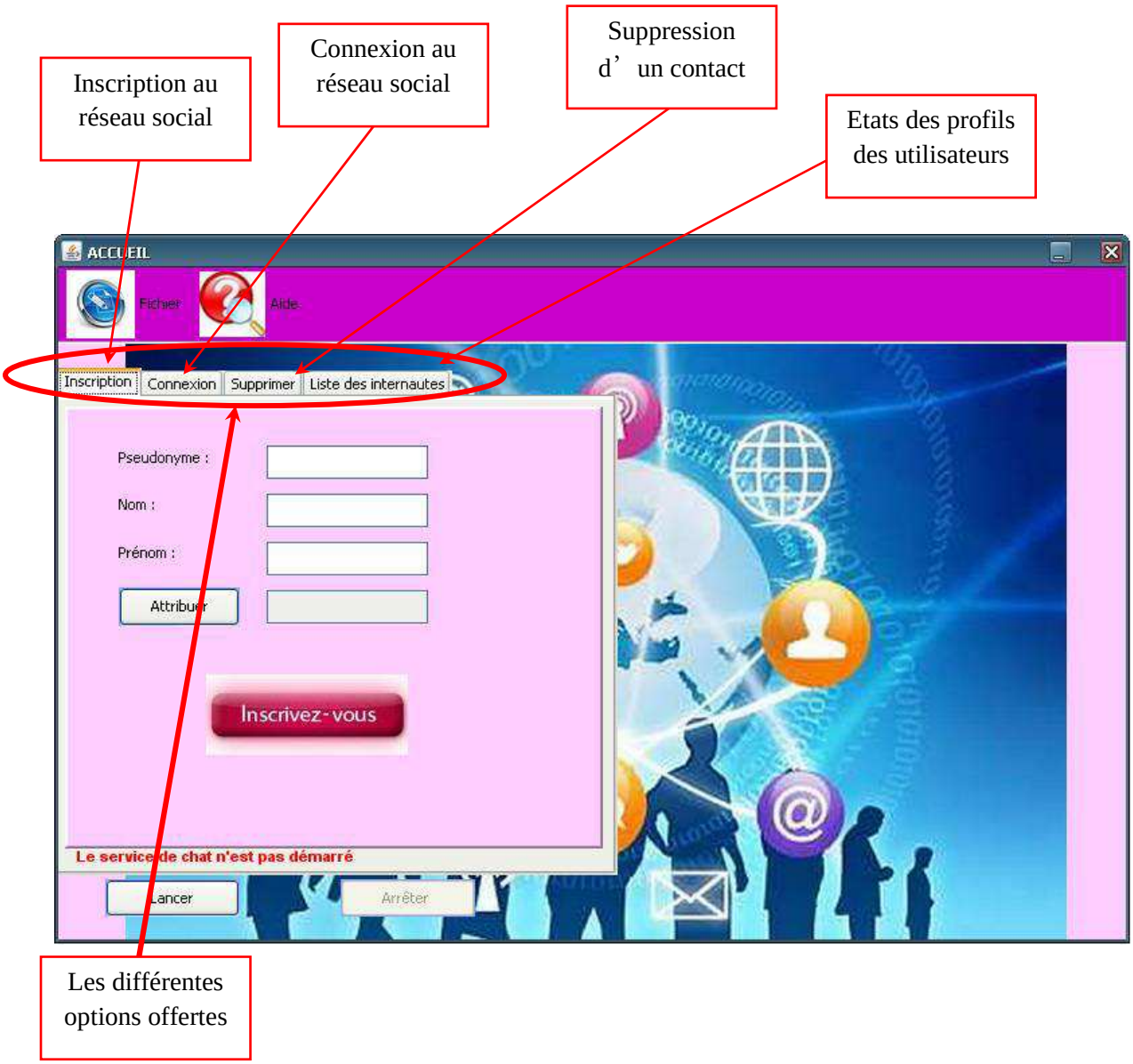


Figure 16 : Page d'accueil

✓ Inscription au réseau social

Cette option permet à l'utilisateur de s'inscrire pour participer aux différents dialogues entre les autres abonnés au réseau.

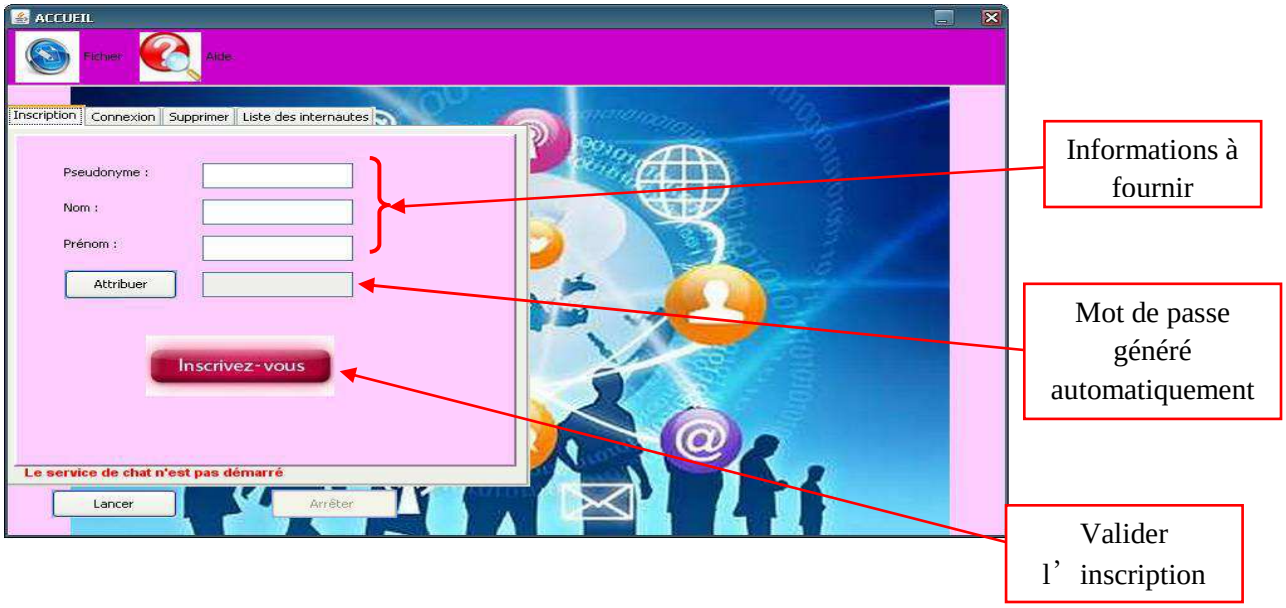


Figure 17 : Inscription au réseau social

✓ Connexion au réseau social

Cette option permet à l'utilisateur de se connecter à son compte de réseau social.

Figure 18 : Connexion au réseau social

✓ Suppression d'un contact

Cette option permet à l'utilisateur de supprimer un contact de sa liste d'amis.

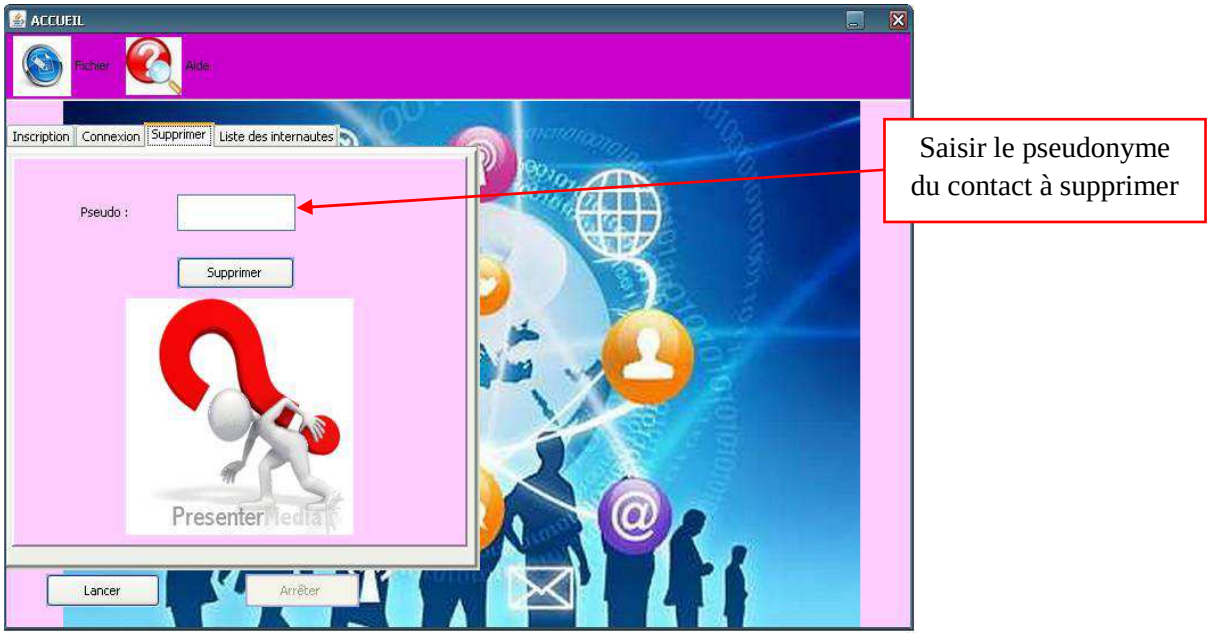


Figure 19 : Suppression d'un contact

✓ **Fenêtre de dialogue**

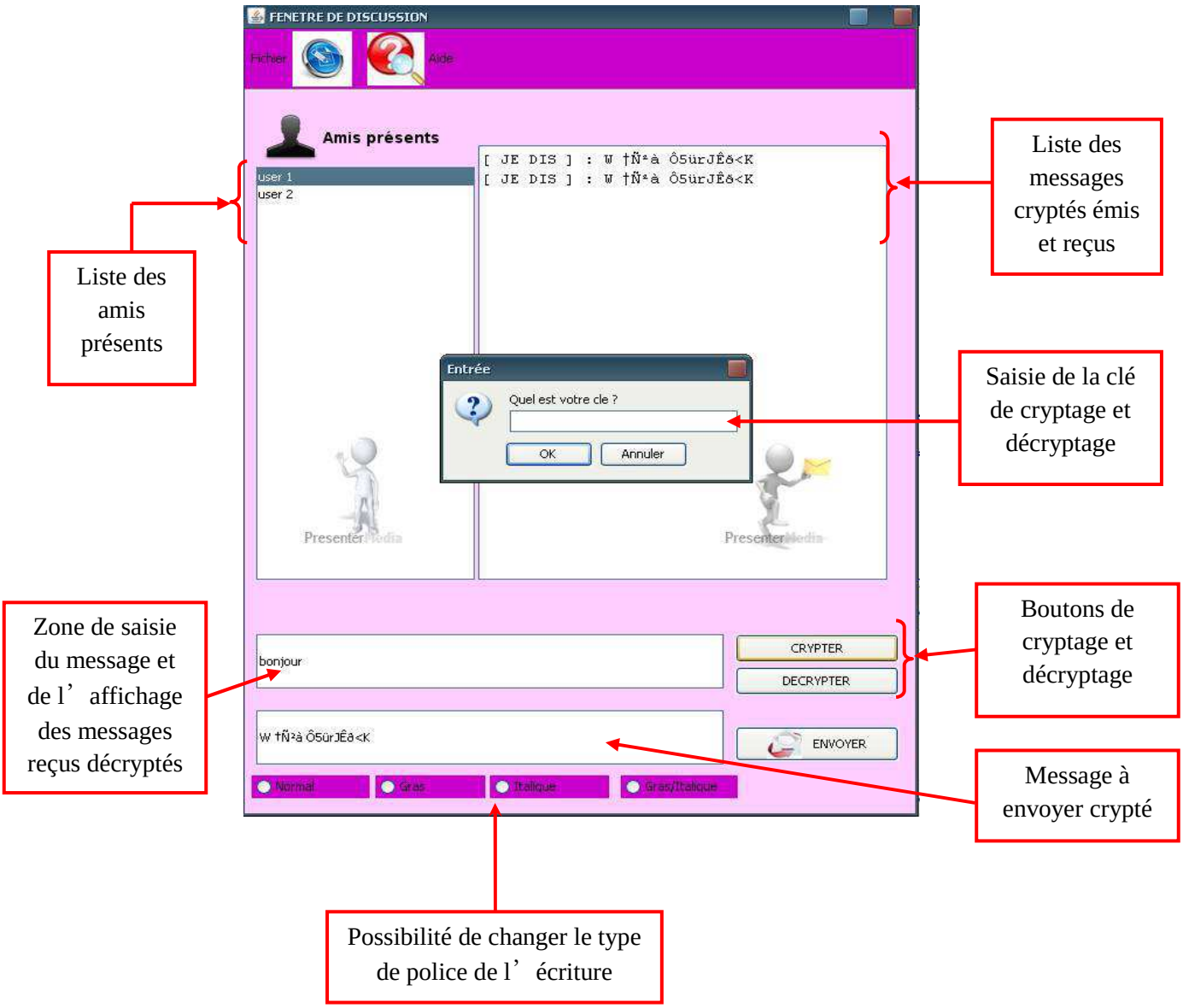


Figure 20 : Fenêtre de dialogue d'un utilisateur

Chapitre 5 Outils de développement et Réalisation

Dans ce chapitre nous avons donné l'architecture générale de notre application et défini l'environnement de son développement. Comme nous avons expliqué son fonctionnement en présentant quelques interfaces.

Conclusion Générale

Aujourd'hui, l'information circule beaucoup plus vite et de manière plus fiable qu'autrefois, grâce à de nouvelles technologies dans le domaine de l'information, l 'évolution des sources d'informations, et surtout la place des médias dans la société.

En effet, les réseaux sociaux informatiques tels que *Facebook* et *Twitter* y contribuent. Ils s'imposent dans notre vie.

Par exemple, accueillant plus de 350 millions d'utilisateurs, *Facebook* constitue un formidable site sur lequel les membres vont s'amuser et passer du bon temps, pratiquer des jeux, défier leurs amis, discuter, partager des photos, retrouver d'anciens amis, se créer un nouveau réseau etc. Visiblement, les hommes et les femmes y sont inscrits à part égale.

Les gens s'y inscrivent par conformité, par plaisir, pour découvrir le monde extérieur, rencontrer des gens, par curiosité, pour partager des passions, rester en contact, pour le travail, et bien souvent par effet de mode. Et pourtant, comme nous l'avons expliqué, les dangers sur ces sites ne sont pas des moindres. Cela ne freine pas les utilisateurs qui les utilisent et apprécient même de plus en plus.

Certaines personnes voient aussi dans ces réseaux sociaux informatiques un progrès pour la démocratie. Leur utilisation propose aux citoyens un nouvel espace pour le débat public. Ils permettent d'accéder sans se déplacer à toutes sortes de documents, ou encore de trouver des réponses à ses questions sans passer par un intermédiaire. Ils servent également de lieu d'échange entre les dirigeants et les citoyens qui peuvent donner leur opinion, proposer des idées et même parfois voter par le biais des réseaux.
Mais il faut tout de même garder en tête que ce monde créé par chacun de nous, présente de nombreux dangers non négligeables. Il existe tout d'abord, comme nous l'avons vu, des dangers d'usurpation d'identité, des dangers de contrôle permanent sur les gens, qui sont

fichés, des dangers de déshumanisation des contacts, et d'individualisme, de manière générale.

L'avenir de ces sites suscite des questions. Pour l'instant, malgré la forte médiatisation autour de *Facebook*, et de tous les autres puissants systèmes de communication, on ne dispose pas de preuve vis-à-vis de la capacité du site à proposer des outils rentables pour une entreprise. Tous les medias ont venté ces nouveaux sites, mais ils ont aussi, cependant, exposé les dangers psychologiques liés à la possibilité de vivre une "deuxième vie" virtuelle, et un monde fabuleux plein de nouvelles idées, ainsi une vie exposée au monde entier…

Afin de diminuer les risques de ces sites la sécurité informatique est une stratégie bien planifiée en concertation avec les différents intervenants, les risques soupesés afin de déterminer jusqu'à quel point la sécurité doit être implantée.
Parfois, trop de sécurité peut nuire aux opérations lorsque cette dernière n'a pas fait l'objet d'une bonne analyse. Les besoins de chaque réseau est différent et le processus d'affaires à une influence directe sur les actions devant être prises en matière de sécurité.
Les services principaux de la sécurité informatique sont : confidentialité, authentification et intégrité et ces mécanismes sont nombreux, le mécanisme qu'on a choisi c'est la cryptographie car il est plus adapter au besoin du client.

Ce mécanisme est choisie car il est aujourd'hui en mesure de fournir des solutions dans des contextes d'utilisation assez variés : confidentialité des messages, authentification d'entités, signature électronique...
Pour concevoir un système électronique, il est donc nécessaire d'étudier le contexte d'emploi pour choisir les bons types de mécanismes à employer. Il est également indispensable de choisir des primitives de confiance, mais aussi de les composer de manière sécurisée.
Le problème des utilisateurs de la cryptographie est plus simple, il consiste généralement à choisir un ou plusieurs algorithmes parmi une liste. Ces choix doivent être effectués en respectant les principes présentés dans ce module.

La cryptographie a été d'abord utilisée pour garantir la confidentialité des données, elle s'est depuis "démocratisée" en assurant la sécurité des services de télécommunications, étendant de ce fait son champ d'action à **l'authentification** d'une personne ou d'un message, la **non-répudiation**, **l'intégrité** mais aussi **l'anonymat** des transactions.
Cet anonymat est parfois primordial dans les nouveaux services des télécommunications et entre aujourd'hui dans un domaine plus vaste dénommé en anglais « «privasy » et le plus souvent traduit par « protection de la vie privée » Ce domaine consiste à offrir aux utilisateurs de services un maximum de garanties sur la non-divulgation de leurs *données personnelles*.
Les travaux de recherche que j'ai décrite dans ce mémoire s'inscrivent dans une démarche d'élargissement du domaine de la cryptographie à la protection de la vie privée. Il existe de nombreux outils cryptographiques, parmi lesquels les **algorithmes de cryptage**, qui seront abordées dans ce denier, permettant aux utilisateurs d'être protégés. Et de partager leurs données en toute sécurité.

En fin notre travail a consisté en la conception et la réalisation d'un réseau social dynamique et sécurisé en utilisant le renommé mécanisme de cryptage, l'objectif de ce travail était de comparer des réseaux sociaux en suivant leurs méthodes de sécurité et d'améliorer afin de protéger la vie privée des internautes.
Ainsi nous pensons avoir répondu aux besoins exprimés par les utilisateurs et nous souhaitons que ce travail puisse servir comme un outil d'aide et de documentation pour les étudiants à venir.

Références bibliographiques

[1] : Mémoire : Sécurité et vie privée dans les réseaux sociaux, université Luxembourg, 2009

[2] : (FR) C'est quoi un réseau social ? (http://skyisnolimit.wordpress.com/2008/07/30/cest-quoi-un-reseau-social-12/), Blog Sky is no limit's Paradigm, 30 juillet 2008

[3] : Histoire du réseau de télécommunication d'AT&T en Anglais http://www.corp.att.com/history/nethistory/switching.html

[4] :boris.tritscher@unit.ch

[5] : Introduction à la Cryptographie, Haikel MEJRI, CISSP hhm@certification.tn,2005

[6] : Conférences portant sur le web, Université LAVAL.

[7] : La saga du Web, NVI.

[8] : http://www.woueb.net/2010/11/19/nombre-de-dunbar/

[9] : Utiliser Twitter en classe de découverte, Classe de découverte à Paris, 22 au 25 juin 2010

[10] : http://cyberclub.blogs.com/tic/2012/01/tous-sur-twitter-.html

[11] : http://www.ac-besancon.fr/IMG/pdf/TutoTwitter.pdf

[12] : http://www.commentcamarche.net/faq/19337-creer-une-page-facebook-pour-son-entreprise

[13] : La sécurité G Florin, S Natkin CNAM- Cedric

[14] : Sécurité des réseaux informatiques Bernard Cousin Université de Rennes 1

[15] : SécuritéInforatique.com

[16] : Sécurité informatique « attaques informatiques » Jean-Olivier Gerphagnon, Marcelo Portes de Albuquerque &Marcio Portes de Albuquerque

[17] : Introduction à la sécurité informatique Laurent Poinsot

[18] : Sécurité Informatique, Fabrice Prigent, 15 Décembre 2010

[19] : [CRY, 98] : Une introduction à la Cryptographie Printedin the United States of America, [Traduction Francaise : news :fr.misc.cryptologie], 1998

[20] : http://fr.wikiversity.org/wiki/Cryptographie/Terminologie_et_notations

[21] : nspiteri@interpresse.fr, 05 Juillet 2011

[22] : être o'Net Académie d'Orléans-Tours

[23] : Fiche mémento « Du bon usage des réseaux sociaux » InfoSurance

[24] : journal le monde.fr, 28-09-2011

[25] : http://www.ecrans.fr/ , par Alexandre Hervaud, Florent Latrive, 21 septembre 2010

[26] : journal le monde.fr

[27] : privacy@twitter.com

[28] : http://www.atelier.net/en/node/398979

[29] : Tags: expérience utilisateur, réseau sociauxThibaut Deveraux, 21 décembre 2010

[30] : I.Valenbois ,L.Millecam « java autoformation »ellipse 2001 .

[31] : (http://www.jmdoudoux.fr/java/dej/chap-jvm.htm)

[32] : Jean michel DODOUX « developpons en java avec eclipce »

[33] : Eric sarrion « développement web avec J2EE »

[34] : http://www.Mysql.fr

[35] : Servlets et java server page le guide du développeur »,
.P.Y.ssaumont,A.Mirecourt

[36] : http : //fadace.developpez.com/sgbdcmp/#LII-I-1