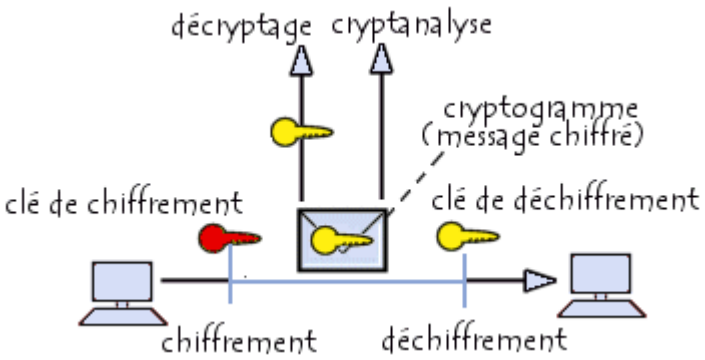
UNIVERSITÉ DE ROUEN
Faculté des sciences et techniques
Site de Mont Saint-Aignant

A la demande de M^me^ Leloup,
Le 21/03/2005



La cryptographie, une sécurité pour le commerce électronique

KARP Nicolas
HARIVEL Christophe

Méthodologie documentaire
Licence Informatique 3ème année

Sommaire

Inventaire terminologique bilingue

Français	Anglais
Sécurité	Security
Réseau	Network
Pare-feu	Firewall
Cryptage	Encoding
Internet	Internet
Base de données	Data base
Algorithme	Algorithm
Système	System
Codage de l'information	Coding of information
HTTP	HTTP (HyperText Transfer Protocol)
SSL	SSL (Secure Sockets Layers)
E-commerce	E-trades
Anonymat	Anonymous
Logiciel	Software
Protocole	Protocol
Transfert de données	Data transfert
Economie	Economy

Source:

Le Trésor de la Langue Française Informatisé, site consulté le 8 février 2005.

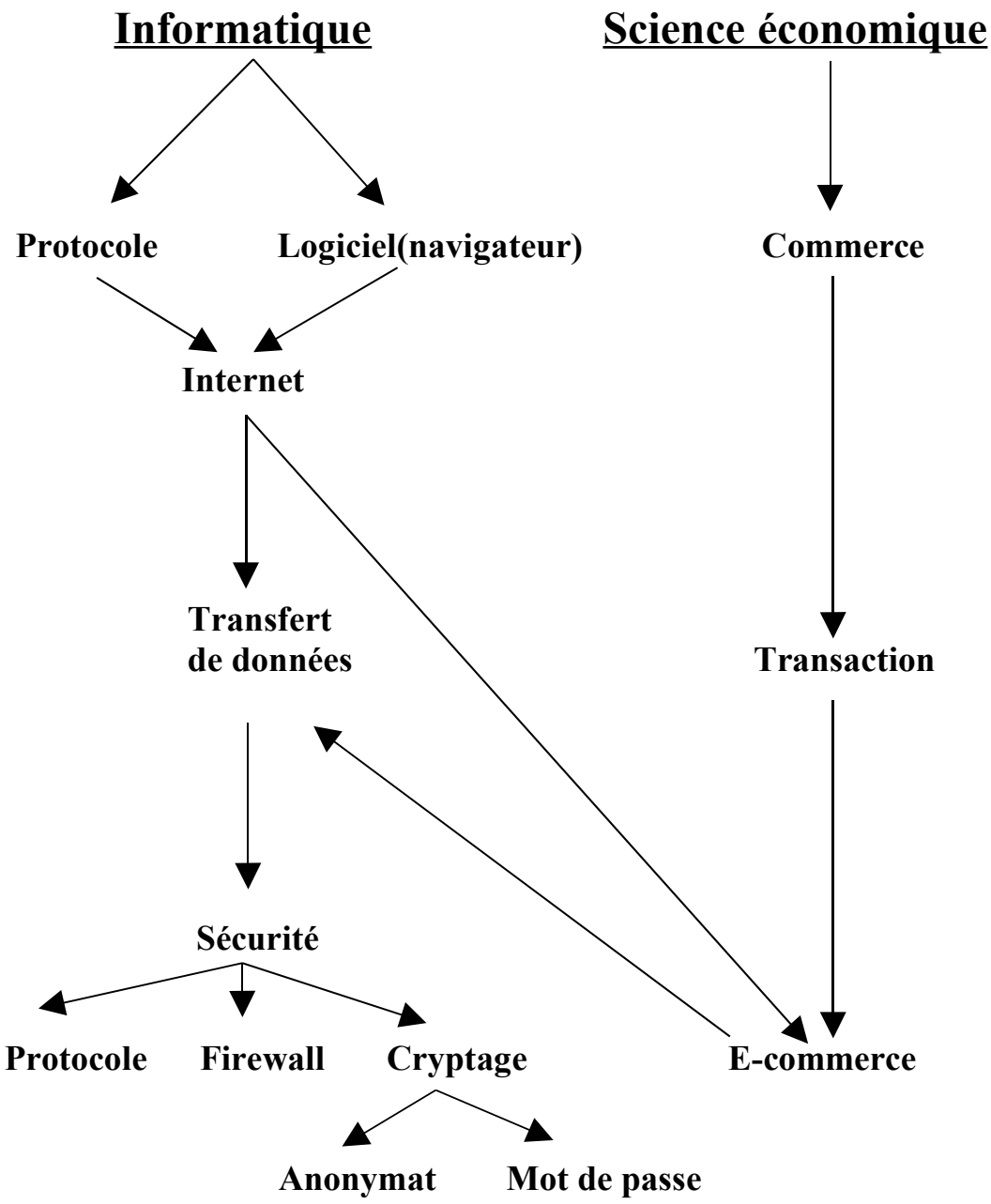
http://atilf.atilf.fr

Dictionnaires en ligne, visités le 08/02/05.

http://www.yourdictionary.com

http://www.granddictionnaire.com

Arborescence



Introduction

L'homme a toujours ressenti le besoin de dissimuler des informations, bien avant même l'apparition des premiers ordinateurs et des machines à coder. Depuis sa création, le réseau Internet a tellement évolué qu'il est devenu un outil essentiel de communication. Cependant cette communication met de plus en plus en jeu des problèmes d'économie des entreprises présentes sur le Web. Les transactions faites à travers le réseau peuvent être interceptées, d'autant plus que les lois ont du mal à se mettre en place sur Internet, il faut donc garantir la sécurité de ces informations, c'est la cryptographie qui s'en charge.

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique.

Ces dernières années le nombre de commerçants en ligne a subi une augmentation exponentielle. Cette augmentation fût favorisée par l'entrée en vigueur sur le marché des offres de connexion Internet, la ligne ADSL (**A**symmetric **D**igital **S**ubscriber **L**ine).Grâce à cet accès, l'utilisateur accède aux informations contenues sur le Web plus rapidement, c'est pourquoi le nombre de connectés au réseau mondial ne cesse d'accroître.

On appelle "Commerce électronique" (ou e-Commerce) l'utilisation d'un média électronique pour la réalisation de transactions commerciales. La plupart du temps il s'agit de la vente de produits à travers le réseau Internet. Le niveau de sécurisation de ces transactions doit être maximal pour éviter le vol des donnés de l'utilisateur (numéro de carte bancaire, information personnelle..). La cryptographie est un atout essentiel pour la protection de ces données, dites sensibles, elle permet leur confidentialité mais aussi à garantir leur intégrité et leur authenticité.

Dans une première partie, nous vous présenterons un historique du « world wide web » et du commerce électronique. Puis,dans une deuxième partie nous vous expliquerons quels sont les différents types de cryptage puis dans une troisième partie nous verrons comment sécuriser les transactions électroniques.

I.Historique du Web et des transactions électroniques

1. Création d'ARPANET

En 1962, l'US Air Force demande à un groupe de chercheurs de créer un réseau de communication militaire capable de résister à une attaque nucléaire. Le concept de ce réseau reposait sur un système décentralisé, permettant au réseau de fonctionner malgré la destruction d'une ou plusieurs machines.

En 1969, le réseau expérimental **ARPANET** fut créé par l'ARPA (**Advanced Research Projects Agency** dépendant du **DOD**, ***Department of Defense***) afin de relier quatre instituts universitaires:

- Le Stanford Institute
- L'université de Californie à Los Angeles
- L'université de Californie à Santa Barbara
- L'université d'Utah

Le réseau ARPANET est aujourd'hui considéré comme le réseau précurseur d'Internet.

Source : HAUBEN, Mickael. *History of ARPANET*. Page visitée le 08/03/2005

http://www.dei.isep.ipp.pt/docs/arpa.html

2. Instauration de nouveaux protocoles et des liens hypertext

En 1976, le protocole TCP ,connu aujourd'hui sous le nom de TCP/IP, fût déployé sur le réseau ARPANET composé à ce moment de 111 machines.

Dès 1980, Tim Berners-Lee, un chercheur au CERN de Genève, mit au point un système de navigation hypertexte et développa, avec l'aide de Robert CAILLAU, un logiciel baptisé *Enquire* permettant de naviguer selon ce principe. Fin 1990, Tim Berners-Lee met au point le protocole HTTP (HyperText Tranfer Protocol), ainsi que le langage HTML (HyperText Mark-up Language) permettant de naviguer à l'aide de liens hypertextes, à travers les réseau. Le World Wide Web est né.

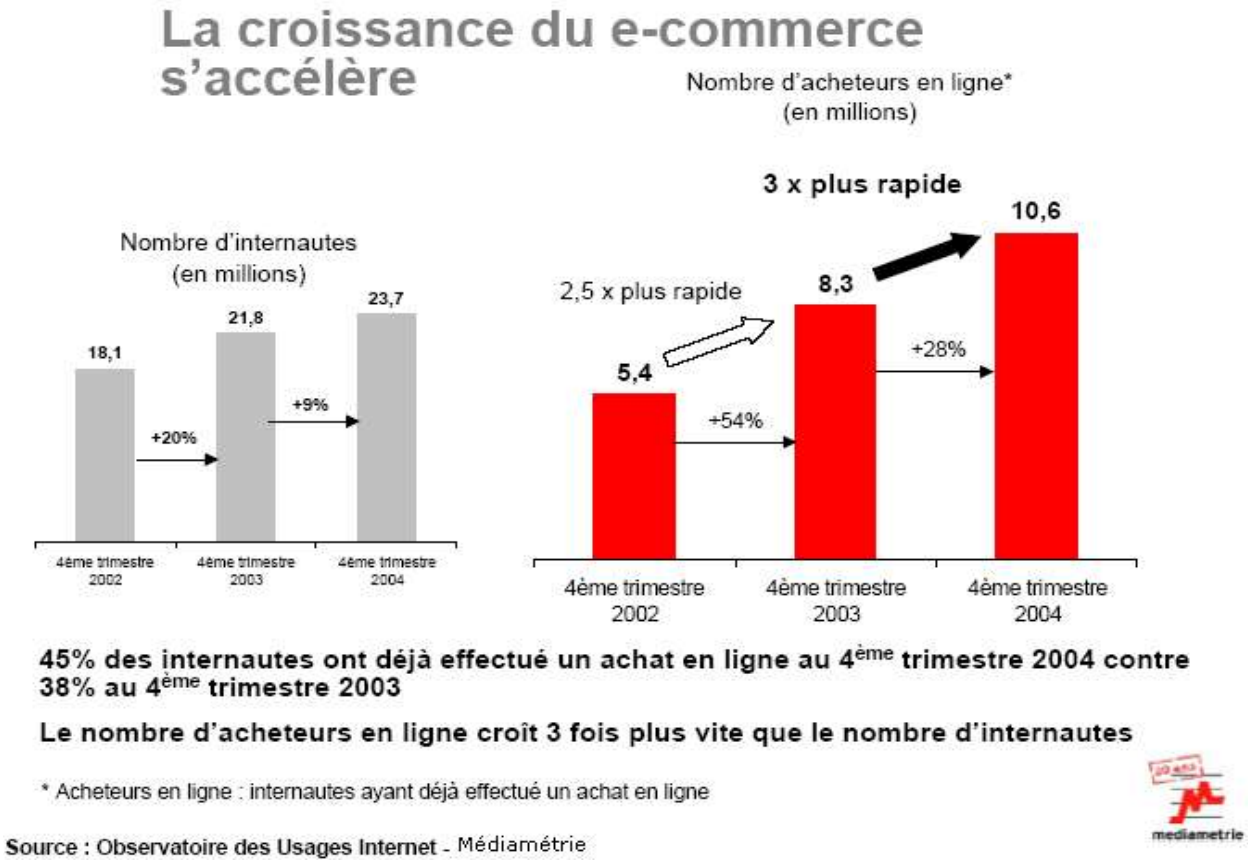
Source : NAIK,Dilip. *Internet standard and protocols.*

Etats-Unis : Microsoft Press, 1998. 333p.

3. Developpement des transactions électroniques

Après le développement de ce réseau des réseaux, des sites dédiés à la vente en ligne apparurent. Tout d'abord rejeté par les utilisateurs, peur de se faire voler ses

coordonnées bancaires, peur de ne pas recevoir le produit en bon état..,le commerce électronique ne commença réellement son ascension qu' en 2003. L'évolution des techniques de sécurité et des accès internet haut débit favorisa sa progression.



Ces graphes montrent bien que le commerce électronique est en plein essor. Les internautes font de plus en plus confiance aux commerçants en ligne et aux traitements des commandes.

Sources : Site du gouvernement français. Page visitée le 29/02/2005.

http://www.internet.gouv.fr/article.php3?id_article=1849

SHARMA, Vivek.SHARMA, Rajiv. *Développement de sites e-commerce.* France : CampusPress.2000. 609p.

II.Différents types de chiffrement

1. Chiffrement par substitution

Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités.
On distingue généralement plusieurs types de cryptosystèmes par substitution:

- La **substitution monoalphabétique** consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet
- La **substitution polyalphabétique** consiste à utiliser une suite de chiffres mono alphabétique réutilisée périodiquement
- La **substitution homophonique** permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères
- La **substitution de polygrammes** consiste à substituer un groupe de caractères (polygramme) dans le message par un autre groupe de caractères

Le chiffrement dit de César est un des plus anciens, dans la mesure où Jules César l'aurait utilisé. Le principe de codage repose sur l'ajout d'une valeur constante à l'ensemble des caractères du message, ou plus exactement à leur code ASCII(pour une version "informatique" de ce codage.

Il s'agit donc simplement de décaler l'ensemble des valeurs des caractères du message d'un certain nombre de positions, c'est-à-dire en quelque sorte de substituer chaque lettre par une autre. Par exemple, en décalant le message "*INFORMATIQUE*" de 3 positions, on obtient "*LQIRUPDWLTXH*". Lorsque l'ajout de la valeur donne une lettre dépassant la lettre Z, il suffit de continuer en partant de A, ce qui revient à effectuer un *modulo 26*.
A titre d'exemple, dans le film *L'odyssée de l'espace*, l'ordinateur porte le nom de *HAL*. Ce surnom est en fait *IBM* décalé de 1 position vers le bas...

On appelle clé le caractère correspondant à la valeur que l'on ajoute au message pour effectuer le cryptage. Dans notre cas la clé est C, car c'est la $3^{ème}$ lettre de l'alphabet.

Ce système de cryptage est certes simple à mettre en oeuvre, mais il a pour inconvénient d'être totalement symétrique, cela signifie qu'il suffit de faire une soustraction pour connaître le message initial. Une méthode primaire peut consister à une bête soustraction des nombres 1 à 26 pour voir si l'un de ces nombres donne un message compréhensible.
Une méthode plus évoluée consiste à calculer les fréquences d'apparition des lettres dans le message codé (cela est d'autant plus facile à faire que le message est long). Effectivement, selon la langue, certaines lettres reviennent plus couramment que d'autres (en français, par exemple, la lettre la plus utilisée est la lettre E), ainsi la lettre apparaissant le plus souvent dans un texte crypté par le chiffrage de César

correspondra vraisemblablement à la lettre E, une simple soustraction donne alors la clé de cryptage...

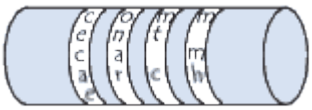
Source: BUCHMANN, Johannes A. *Introduction to cryptography*.
Etats-Unis : Springer. 2001. 335p.

2. Cryptage par transposition

Les méthodes de chiffrement par transposition consistent à réarranger les données à crypter de telle façon qu'elles soient incompréhensibles. Il s'agit généralement de réarranger géométriquement les données pour les rendre visuellement inexploitables.

La technique assyrienne

Cette technique de cryptage est vraisemblablement la première preuve de l'utilisation de moyens de chiffrement en Grèce dès 600 avant Jésus Christ pour dissimuler des messages écrits sur des bandes de papyrus.



Source de l'image : http://www.commentcamarche.net

La technique consistait à:

- enrouler une bande de papyrus sur un cylindre appelé **scytale**
- écrire le texte longitudinalement sur la bandelette ainsi enroulée (le message dans l'exemple ci-dessus est "comment ça marche")

Le message une fois déroulé n'est plus compréhensible ("cecaeonar mt c m mh"). Il suffit au destinataire d'avoir un cylindre de même rayon pour pouvoir le déchiffrer. en réalité un casseur (il existait des casseurs à l'époque...) peut déchiffrer le message en essayant des cylindres de diamètre successifs différents, ce qui revient à dire que la méthode peut être cassée statistiquement (il suffit de prendre les caractères un à un, éloignés d'une certaine distance).

Source: BUCHMANN, Johannes A. *Introduction to cryptography*.
Etats-Unis : Springer. 2001. 335p.

3. Chiffrement symétrique et asymétrique

Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou chiffrement à clé secrète) consiste à utiliser la même clef pour le chiffrement que pour le déchiffrement. Le chiffrement consiste alors à effectuer une opération entre la clé privée et les données à chiffrer afin de rendre ces dernières inintelligibles. Ainsi, le moindre algorithme (tel qu'un OU exclusif) peut rendre le système quasiment inviolable (la sécurité absolue n'existant pas).

Toutefois, dans les années 40, *Claude Shannon* démontra que pour être totalement sûr, les systèmes à clefs privées doivent utiliser des clefs d'une longueur au moins égale à celle du message à chiffrer. De plus le chiffrement symétrique impose d'avoir un canal sécurisé pour l'échange de la clé, ce qui dégrade sérieusement l'intérêt d'un tel système de chiffrement.

Ainsi, dans les années 20, Gilbert Vernam et Joseph Mauborgne mirent au point la méthode du « *one time pad* »(*méthode du masque jetable*), basée sur une clé privée générée aléatoirement, utilisée une et une seule fois, puis détruite. Ainsi à la même époque le Kremlin et la Maison Blanche étaient reliés par le fameux **téléphone rouge**, c'est-à-dire un téléphone dont les communications étaient cryptées par une clé privée selon la méthode du *masque jetable*. La clé privée était alors échangée grâce à la valise diplomatique (jouant le rôle de canal sécurisé).

Le chiffrement asymétrique quant à lui utilise deux clefs pour le cryptage du message. Elles existent toujours par paire (on parle souvent de bi-clés) :

- Une clé publique pour le chiffrement
- Une clé secrète pour le déchiffrement

Ainsi, dans un système de chiffrement à clé publique, les utilisateurs choisissent une clé aléatoire dont ils sont seuls connaisseurs (il s'agit de la *clé privée*). A partir de cette clé, ils déduisent chacun automatiquement un algorithme (il s'agit de la clé publique). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé.

Lorsqu'un utilisateur désire envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire (qu'il trouvera par exemple dans un serveur de clés tel qu'un annuaire). Ce dernier

sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître).

Sources : SALOMAA, Arto . *Public-key cryptogrphy.* Berlin : Springer. 1996.

MacOSXTech. *Introduction au chiffrement asymétrique.* http://www.macosxtech.com/dossiers/index.php?art=24

III. Sécurisation d'une transaction électronique

1. Le système SSL (Secure Sockets Layers)

SSL (Secure Sockets Layers), que l'on pourrait traduire par couche de sockets sécurisée) est un procédé de sécurisation des transactions effectuées via Internet mis au point par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur Internet. Le système SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, située entre la couche application et la couche transport (protocole TCP par exemple).

De cette manière, SSL est transparent pour l'utilisateur. Par exemple un utilisateur utilisant un navigateur Internet pour se connecter à un site de commerce électronique sécurisé par SSL enverra des données chiffrées sans avoir à s'en préoccuper.
La quasi intégralité des navigateurs supporte désormais le protocole SSL. Netscape Navigator affiche par exemple un cadenas verrouillé pour indiquer la connexion à un site sécurisé par SSL et un cadenas ouvert dans le cas contraire, tandis que Microsoft Internet Explorer affiche un cadenas uniquement lors de la connexion à un site sécurisé par SSL.

Source: MUNOZ, Sandrine. *La protection des échanges de données informatisées.*Thèse de doctorat. 1997. Nice.

Internet Explorer

Mozilla

Un serveur sécurisé par SSL possède une URL (Uniform Resource Locator) commençant par *https://*, où le "s" signifie bien évidemment *secured* (*sécurisé*).

Au milieu de l'année 2001, le brevet de SSL appartenant jusqu'alors à Netscape a été racheté par l'*IETF* (***I**nternet **E**ngineering **T**ask **F**orce*) et a été rebaptisé pour l'occasion **TLS** (***T**ransport **L**ayer **S**ecurity*).

Source: SALOMAA, Arto. *Public-key cryptography*. Berlin: Springer. 1996. 271p.

2. Le système SSH (Secure Shell)

Le protocole SSH est un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

- Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.
- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

La version 1 du protocole (SSH1) proposée dès 1995 avait pour but de servir d'alternative aux sessions interactives (shells) telles que Telnet, rsh, rlogin et rexec. Ce protocole possédait toutefois une faille permettant à un pirate d'insérer des données dans le flux chiffré. C'est la raison pour laquelle en 1997 la version 2 du protocole (SSH2) a été proposée en tant que document de travail (draft) à l'IETF (*The Internet Engineering Task Force*). Les documents définissant le protocole sont accessibles en ligne sur http://www.ietf.org/html.charters/secsh-charter.html.

Source: BARETT,Daniel J. SILVERMAN, Richard. *SSH:the secure shell*. Paris : O'Reilly. 2001. 540p

3. Le protocole S-HTTP (Secure HyperText Transfer Protocol)

S-HTTP (**S**ecure HTTP, traduisible par Protocole HTTP sécurisé) est un procédé de sécurisation des transactions HTTP reposant sur une amélioration du protocole HTTP mise au point en 1994 par l'EIT (**E**nterprise **I**ntegration **T**echnologies). Il permet de fournir une sécurisation des échanges lors de

transactions de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de tout autre information personnelle. Une implémentation de S-HTTP a été développée par la société Terisa Systems afin d'inclure une sécurisation au niveau des serveurs web et des navigateurs.

Contrairement à SSL qui travaille au niveau de la couche de transport,

S-HTTP procure une sécurité basée sur des messages au-dessus du protocole HTTP, en marquant individuellement les documents HTML à l'aide de "certificats". Ainsi, alors que SSL est indépendant de l'application utilisée et crypte l'intégralité de la communication, S-HTTP est très fortement lié au protocole HTTP et crypte individuellement chaque message.

Les messages S-HTTP sont basés sur trois composantes:

- Le message HTTP
- Les préférences cryptographiques de l'envoyeur
- Les préférences du destinataire

Ainsi, pour décrypter un message S-HTTP, le destinataire du message analyse les en-têtes du message afin de déterminer le type de méthode qui a été utilisé pour crypter le message. Puis, grâce à ses préférences cryptographiques actuelles et précédentes, ainsi que des préférences cryptographiques précédentes de l'expéditeur, il est capable de décrypter le message.

Source: PIETTE-COUDOL, Thierry. *Echanges électroniques, certification et sécurité*. Paris : Litec. 2000. 237p.

4. Le protocole SET (Secure Electronic Transaction)

SET est un protocole de sécurisation des transactions électroniques mis au point par Visa et MasterCard, et s'appuyant sur la méthode SSL.

SET est basé sur l'utilisation d'une signature électronique au niveau de l'acheteur et une transaction mettant en jeu non seulement l'acheteur et le vendeur, mais aussi leurs banques respectives.

Fonctionnement de SET :

Lors d'une transaction sécurisée avec SET, les données sont envoyées par le client au serveur du vendeur, mais ce dernier ne récupère que la commande. En effet, le numéro de carte bleue est envoyée directement à la banque du commerçant, qui va

être en mesure de lire les coordonnées bancaires de l'acheteur, et donc de contacter sa banque afin de les vérifier en temps réel.

Ce type de méthode nécessite une signature électronique au niveau de l'utilisateur de la carte afin de certifier qu'il s'agit bien du possesseur de cette carte.

Source: Le centre général des services internet. *Le protocole SET,* page visitée le 03/03/2005. http://www.cgsi.ca/SET.html

IV. Activité de veille documentaire

Tout d'abord, nous avons commencé par réfléchir sur le sujet proposé, l'informatique en 2005.Nous nous sommes donc orienter vers la sécurité des transactions électroniques car nous pensons que cette sécurité est en plein essor depuis des années et qu'elle ne cesse de s'améliorer. Ce sujet est d'actualité car le nombre d'achats effectués en ligne est en perpétuel augmentation.

Voici donc un résumé des recherches menées dans les périodiques que nous avons consulté, ainsi qu'une liste non exhaustive des moteurs de recherche utilisés.

Nous avons tout d'abord consulté les sites des périodiques comme « Le Monde » (http://www.lemonde.fr) ou « Libération » (http://www.liberation.fr/) pour suivre l'actualité sur notre sujet, plus particulièrement sur le commerce en ligne et sa sécurité grâce a la cryptographie.

Voici nos résultats :

Le Premier ministre Jean-Pierre RAFFARIN a visité mardi 1er février 2005 les installations de la société Pixmania, entreprise emblématique du succès du commerce électronique et du haut débit en France, en compagnie du Président de CISCO Systems, John CHAMBERS.
Article paru dans le quotidien « Le Monde », le 02/02/2005.

« Le Net retrouve la ligne »,article de presse réalisé par Christophe ALIX paru le 14 mars 2005.
Cet article montre le développement d'un des sites leader en ce qui concerne la vente de produits numériques.
(http://www.liberation.fr/page.php?Article=282250).

Pour compléter ces informations, nous avons donc effectuer une recherche sur

le catalogue SUDOC (**S**ystème **U**niversitaire de **DOC**umentation) sur le site http://cuivre.sudoc.abes.fr/. En rentrant le mot « cryptographie », nous avons obtenu 75 résultats et en entrant le mot e-commerce nous avons obtenu 122 résultats. Pour affiner ces recherches, nous avons ciblé nos recherches en ajoutant les mots « SSL », « sécurité », « protocole »...

Après avoir trouvé les livres,thèses et monographies qui correspondaient à notre sujet, nous avons effectuer des recherches sur certain moteur de recherche pour voir des précisions sur certains algorithmes et protocoles utilisés lors de transaction électronique. Nous avons donc pu réaliser l'importance des choix d'équations de recherche, car une recherche pas assez ciblée amène des résultats qui ne conviennent pas et une recherche trop ciblée amène très peu de résultat.

Conclusion

Alors que SSL et S-HTTP étaient concurrents, un grand nombre de personnes ont réalisé que les deux protocoles de sécurisation étaient complémentaires, étant donné qu'ils ne travaillent pas au même niveau. De cette façon, SSL permet de sécuriser la connexion Internet tandis que S-HTTP permet de fournir des échanges HTTP sécurisés.

De cette façon, la compagnie Terisa Systems, spécialisée dans la sécurisation des réseaux, formée par RSA Data Security et l'EIT, a mis au point un Kit de développement permettant à des développeurs de développer des serveurs Web implémentant SSL et S-HTTP (SecureWeb Server Toolkit), ainsi que des clients Web supportant ces protocoles (SecureWeb Client Toolkit).

Avec le protocole SET et les deux protocoles cités précédemment, la sécurisation est optimale. Le nombre de fraudes et de piratages est en baisse au vu des différentes technologies mises en place pour sécuriser l'échange de données. Comme nous l'avons vu en première partie, le nombre d'acheteurs en ligne est en augmentation, ce qui dénote une confiance des internautes vis à vis du commerce électronique.

Malgré ces différentes solutions, l'échange de données entre le marchand et le client n'est pas sûr a 100 % mais s'y rapproche de plus en plus. Un jour peut être, nous atteindrons la certitude d'une sécurité totale et personne ne pourra entraver le traitement confidentiel des données.

Bibliographie

Livres	**BARETT,Daniel J. SILVERMAN, Richard**. *SSH:the secure shell*. Paris : O'Reilly. 2001. 540p. **BUCHMANN, Johannes A**. *Introduction to cryptography*. Etats-Unis : Springer. 2001. 335p. **NAIK,Dilip**. *Internet standard and protocols.* Etats-Unis : Microsoft Press, 1998. 333p. **SHARMA, Vivek**. **SHARMA, Rajiv**. *Développement de sites e-commerce.* France : CampusPress.2000. 609p.

Monographies	**PIETTE-COUDOL, Thierry** . Échanges électroniques, certification et sécurité. Paris : Litec. 2000 **SALOMAA, Arto** . Public-key cryptography. Berlin : Springer. 1996.

Thèses	**DELPECH, Vincent.** D*ématérialisation et sécurité des transactions.* 1996 Thèse de doctorat,Bordeaux 4. **MUNOZ, Sandrine**. *La protection des échanges de données informatisées.* 1997. Thèse de doctorat. Nice.

Sources internet	Dictionnaires en ligne.(Visitée le 08/02/05) http://www.yourdictionary.com http://www.granddictionnaire.com ETIC. *ARPANET,l'ancêtre d'internet.* (Visitée le 16/02/05) http://www.funoc.be/etic/doss001/art001.html IETF. *Secure Shell.* (Visitée le 15/03/05) http://www.ietf.org/html.charters/secsh-charter.html L'encyclopédie informatique libre. (Visitée le 19/02/05) http://www.commentcamarche.net Le centre général des services internet. *Le protocole Set*.(Visitée le 26/02/05) http://www.cgsi.ca/SET.html Le Trésor de la Langue Française Informatisé, site consulté le 8 février 2005. http://atilf.atilf.fr MacOSXTech. *Introduction au chiffrement asymétrique.* http://www.macosxtech.com/dossiers/index.php?art=24 Netscape. *SSL 3.0 Specification.*(Visitée le 11/03/05) http://wp.netscape.com/eng/ssl3/ Site du gouvernement français. *Commerce électronique : les français achètent plus souvent qu' avant. (Visitée le 20/03/05)* http://www.internet.gouv.fr/article.php3?id_article=1849 Site du gouvernement français. *Tableau de bord du commerce électronique. (Visitée le 22/02/05)* http://www.men.minefi.gouv.fr/webmen/themes/eco/tbce91204.pdf Wikipedia,l'encyclopédie libre et gratuite. *Secure Shell.(Visitée le 26/02/05)* http://fr.wikipedia.org/wiki/SSH