La Cryptographie et la Confiance Numérique

Abderrahmane Nitaj
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Basse-Normandie

23 mars 2013

Résumé

Dans le monde numérique d'aujourd'hui, l'information n'a plus de frontières et les technologies basées sur Internet et Intranet ouvrent les systèmes informatiques au monde extérieur. Ainsi, l'information est accessible presque instantanément, augmentant ainsi les risques de piratage, de destruction et d'espionnage. Pourtant, les techniques cryptographiques modernes permettent de sécuriser efficacement les systèmes informatiques, les communications et l'information. Dans le but de promouvoir la confiance numérique, nous analysons dans ce texte les liens étroits qui existent entre la sécurisation des communications par des moyens cryptographiques et les principales lois qui protègent la vie privée ainsi que les systèmes informatiques.

1 Introduction

L'informatique est omniprésente dans tous les domaines et tous les secteurs. Nous sommes dans une ère qu'on peut qualifier d'ère du tout numérique. Les passeports, les cartes bancaires, les badges de stationnement, certains votes, l'achat en ligne, la majorité des communications, sont des exemples du monde numérique. Internet est de plus en plus utilisé pour s'inscrire à un concours, pour acheter un billet d'avion ou de train, pour réserver un hotel, pour communiquer, pour envoyer un message ou un mandat, pour stocker des données sur un serveur distant, pour des transactions bancaires, etc... Notre ordinateur personnel, notre station de travail ne sont plus isolés, mais reliés au monde entier. Des questions naturelles se posent alors : y a-t-il un risque à utiliser Internet ? L'informatique est-elle sécurisée ? Bref, faut-il avoir confiance dans les moyens de protection ?

La sécurité informatique est l'ensemble des moyens mis en œuvre pour protéger un système contre les menaces accidentelles ou intentionnelles. Ceci comprend l'aspect physique (pannes, dégâts matériels, vols, ...), et l'aspect logiciel (bugs, virus, piratages, ...). La sécurité informatique est importante pour établir la confiance numérique. De même la cryptographie est importante pour consolider la sécurité informatique. Ces trois notions qui sont la confiance numérique, la sécurité informatique et la cryptographie sont étroitement liées. La sécurité informatique et donc la confiance numérique s'établissent autour des points suivants qui sont centraux en cryptographie.

1. L'authentification : être sûr de l'identité de la partie avec laquelle je communique.

2. **La confidentialité** : Je chiffre les données que je transmets.
3. **L'intégrité** : être assuré que les données que je transmets ne seront pas altérées.
4. **La non répudiation** : Aucune transaction ne peut être niée.

La cryptographie est une science ancienne qui est née en même temps que l'écriture. Plusieurs civilisations avaient utilisé la cryptographie, Egypte, Chine, Inde, Civilisation Romaine, Civilisation Arabo-musulmane, Renaissance, et elle est prépondérante dans les temps modernes. Tout le monde connait l'histoire populaire d'Ali Baba dans les Mille et Une Nuit et comment il pouvait ouvrir et fermer la grotte des 40 voleurs à l'aide des mots de passe : "Sésame, ouvre-toi" et "Sésame, ferme-toi".

Dans n'importe quel pays, le développement numérique est bénéfique pour les personnes, pour l'économie, et pour le développement en général. Malheureusement, la cybercriminalité à suivi le développement numérique. Pour faire face à ce fléau mondial, des lois ont été promulguées pour garantir l'intégrité des réseaux, pour assurer la protection de la vie privée et pour lutter contre la piraterie et le vol. Toutes ces lois et ces mesures ont pour objectif d'établir la confiance numérique dans la société.

On donne ici un bref résumé des techniques cryptographiques mises en œuvre pour assurer la sécurité des données transitant par les voies de communication et pour établir la confiance numérique. Dans la partie 2, on donne quelques principes cryptographiques. Dans la partie 3, on discute des dangers de la cybercriminalité. Dans la partie 4, on rappelle quelques lois visant à protéger les personnes physiques. Dans la partie 5, on rappelle quelques lois contre la cybercriminalité et on conclut dans la partie 6.

2 La cryptographie

La cryptographie moderne a commencé dans les années 1970 quand Diffie et Hellman [5] ont proposé une méthode d'échange de clés et quand Rivest, Shamir et Adleman [13] ont proposé le premier système cryptographique à clé publique. Actuellement, il existe trois types de cryptographie.

1. **La cryptographie symétrique ou à clé secrète** : C'est la même clé qui sert à chiffrer un texte et à le déchiffrer. Le principal inconvénient de la cryptographie asymétrique est le partage de la clé. Les principaux systèmes dans cette famille sont DES (Data Encryption Standard) et AES (Advanced Encryption Standard).
2. **La cryptographie asymétrique ou à clé publique** : Dans la cryptographie dite asymétrique, deux clés sont utilisées, une clé secrète et une clé publique. Pour envoyer un message au propriétaire de la clé secrète, il suffit de chiffrer ce message avec la clé publique correspondante. Seul le détenteur de la clé secrète pourra alors déchiffrer le message. Les principaux cryptosystèmes asymétriques utilisés actuellement sont RSA, ElGamal, Diffie-Helleman et ECC.
3. **La cryptographie hybride** : C'est un mélange des deux types de cryptographie précédents. Un message est chiffré par la méthode symétrique à l'aide d'une clé secrète, puis cette clé est chiffrée à son tour par la méthode asymétrique, puis envoyée au destinataire. Le destinataire commence par déchiffrer la clé et ensuite utiliser cette clé pour déchiffrer le message.

La cryptographie asymétrique a beaucoup d'applications. En particulier, elle est utilisée pour transmettre des clés et pour authentifier un message. La sécurité de la cryptographie asymétrique est basée sur une multitude de problèmes mathématiques difficiles comme par exemple le problème de la factorisation (pour RSA) et le problème du logarithme discret (pour Diffie-Hellman et ElGamal).

Les communications par Internet sont sécurisées par des protocoles utilisant des procédés de cryptographie hybride. Les organismes qui se chargent d'assurer l'authentification des interlocuteurs à travers Internet s'appellent des autorités de certification.

2.1 L'Autorité de Certification

Dans un échange sécurisé de données électroniques par un protocole tel que TLS, les algorithmes de chiffrement asymétrique sont basés sur le partage de clés publiques entre les différents utilisateurs. L'organisme qui se charge de garantir l'authenticité et la validité des clés partagées par les différents utilisateurs est une Autorité de Certification. C'est un organisme de confiance compétent pour délivrer et gérer des certificats et en assurer la validité. Les champs les plus significatifs des certificats numériques sont les suivants :

- Rôles du certificat.
- Le numéro de série.
- Algorithme de signature.
- Algorithme de hachage.
- L'émetteur du certificat.
- Dates de début et de fin de validité.
- Objet du certificat.
- La clé publique du titulaire du certificat.
- Utilisation de la clé.

En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) assure la mission d'autorité en matière de sécurité des systèmes d'information. Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques. Elle est chargée d'organiser la délivrance des labels de sécurité à des produits et à des prestataires de services de confiance. On dénombre actuellement plus de vingt autorités de certification en France.

Au Maroc, conformément à la loi n°53-05 [16], l'Agence Nationale de Réglementation des Télécommunications (ANRT) a choisi Barid eSign comme plateforme nationale de production de certificats électroniques. L'ANRT a délivré de même un certificat de conformité à Gemalto Classic TPC IM CC pour la carte à puce TPC, qui est une carte à puce destinée aux applications basées sur la cryptographie à clé publique. D'autre part, Maroc Numeric 2013 a créé le label e-thiq@ qui vise à instaurer la confiance dans l'achat en ligne, pour promouvoir le commerce électronique et encourager la confiance numérique au Maroc.

2.2 TLS

TLS (Transport Secured Layer) est un protocole d'échange d'informations sécurisées à travers Internet. Il propose trois fonctionnalités essentielles : l'authentification par une autorité de certification, la confidentialité par un algorithme de chiffrement, et l'intégrité par une signature numérique. TLS est ainsi basé sur la cryptographie hybride et permet

d'établir un lien sécurisé entre un client et un serveur. Le fonctionnement de TLS entre un client et un serveur peut se résumer comme ci-dessous.

1. TLS établit le lien entre le client et le serveur en s'authentifiant auprès du serveur. Le client demande au serveur de s'authentifier au moyen d'un certificat. Le client envoie également la liste des systèmes de cryptage qu'il supporte.
2. Le serveur envoie un certificat signé par une autorité de certification. Ce certificat contient la clé publique du serveur. Il envoie également la référence du système de cryptage compatible avec le client.
3. Le client vérifie ensuite la validité du certificat du serveur, puis crée une clé secrète. Le client chiffre cette clé secrète à l'aide de la clé publique du serveur, la signe avec sa propre clé privée asymétrique puis l'envoie au serveur.
4. Le serveur déchiffre la clé secrète à l'aide de sa propre clé secrète asymétrique, puis à l'aide de la clé publique du client. La clé secrète est donc commune au client et au serveur. Cette première phase s'appelle le "handshake" ou poignée de main.
5. Maintenant, les transactions peuvent commencer au moyen d'un sous protocole appelé "Record" ou enregistrement.
6. La fermeture de la connexion est protégée par des messages spéciaux.

Plusieurs protocoles et schémas cryptographiques entrent en jeu dans TLS comme par exemple RSA, AES, SHA-1, DSA, HMAC, etc... TLS est considéré comme sûr et n'a subi que de très peu d'attaques sans réelles conséquences. On peut dire sans hésitation que TLS est un point essentiel dans la confiance numérique.

2.3 HTTPS

La plupart des pages web ne sont pas sécurisées. L'adresse url de ces pages commence par "`http://www.`". La sécurisation commence généralement au moment d'une connexion requise pour accéder à un compte. Dans ce cas, l'adresse se transforme en "`https://`" et est accompagnée par une clé fermée. HTTP est formé des initiales 'Hyper Text Transfer Protocol' et 's' est l'initiale de secured, qui veut dire que le site est sécurisé, généralement par TLS (Transport Layer Security). On peut alors voir comment le site est sécurisé en cliquant sur l'image de la clé et demander d'afficher le certificat qui permet de vérifier l'identité du site. On se trouve alors en présence d'un certain nombre de renseignements sur le certificat. Parmi les renseignements, on trouve le chiffrement public utilisé, la taille de la clé publique et l'algorithme de signature des certificats. La clé publique correspond généralement au cryptosytème RSA avec des tailles de 1024 ou 2048 bits. La clé publique contient donc un entier du type $N = pq$ ou p et q sont des entiers inconnus. Puisque le problème de la factorisation est réputé difficile, il est pratiquement impossible de retrouver les deux nombres p et q. Bien entendu, il existe plusieurs méthodes qui peuvent recouvrir p et q mais avec une très faible probabilité. Les sites "`https://`" sont donc très sécurisés.

La table ci-dessous donne des renseignements sur les protocoles cryptographiques de certaines plateformes assez répandues.

Service	Google Apps	Facebook	Tweeter	Amazon
Certification	Google Internet Authority	VeriSign Trust Network	VeriSign Class 3	VeriSign Class 3
Connexion	TLS	TLS	TLS	TLS
Authentification	SHA1	SHA1	SHA1	SHA1
Echange de clés	RSA	RSA	RSA	RSA
Clé publique	1024	1024	2048	2048

3 La cybercriminalité

La mondialisation d'Internet a facilité l'émergence d'une nouvelle forme de délinquance, exercée à distance : la cybercriminalité. Elle s'attaque aussi bien aux personnes physiques et morales qu'aux systèmes informatiques des états et des institutions publiques et privées. La cybercriminalité peut prendre plusieurs formes : vol de mots de passe, destruction de ressources, usurpation d'identité, escroquerie, fraude, espionnage industriel, piratage de logiciels, atteinte aux droits d'auteur, cyberterrorisme, cyberguerre, etc...

3.1 Les Infections Informatiques

Les infections informatiques sont nombreuses et généralement nocives. Ce sont des programmes informatiques qui peuvent être stockés dans des systèmes d'exploitation, des logiciels ou des pages web. Ils s'exécutent automatiquement pour différentes tâches, suivant le type de l'infection. Dans certains cas, les infections informatiques visent particulièrement des cibles bien choisies d'un pays pour perturber, voire saboter le fonctionnent normal d'un service publique ou privé ou d'une centrale sensible. Ces infections informatiques sont alors considérées comme des cyber-attaques dans des cyber-guerres. Les infections informatiques sont de plusieurs natures : les vers (worm), les virus, les chevaux de Troie (trojan), les backdoors (portes dérobées), les spywares (logiciels espions), les keyloggers (enregistreurs de touches du clavier), etc...

Un virus informatique est un programme qui se dissimule dans des fichiers ou dans le code exécutable contenu dans le secteur de démarrage du disque. Il peut infecter un ordinateur ou toute machine similaire et en prendre le contrôle dans un but, généralement malveillant. Il peut se répandre d'ordinateur à ordinateur à travers tout moyen d'échange de données numériques comme les fichiers joints des emails, les clefs USB, les cédéroms et les réseaux informatiques.

Les Spywares et les keyloggers sont des logiciels qui collectent des données personnelles avant de les envoyer à un tiers. Ils peuvent transmettre par exemple les mots de passe, les codes bancaires et les habitudes de navigation de l'utilisateur.

Un cheval de Troie est un programme qui s'installe de façon illicite par l'intermédiaire d'un mail ou d'une page web infectée. Il peut servir ensuite à espionner l'ordinateur, à envoyer des spams ou à faciliter l'accès à l'ordinateur à un pirate.

Un Backdoor ou porte dérobée est un point d'accès à un système d'exploitation, conçu par les concepteurs de logiciels à l'insu de l'utilisateur. Un backdoor permet par la suite une introduction facile dans le système.

3.2 Le phishing

Nous avons tous reçu un jour un email avec un avertissement solennel du type :

```
Ceci est pour vous informer que votre compte de messagerie a dépassé
sa limite de stockage. ..., que votre compte e-mail sera supprimé
de notre serveur. ... Cliquez sur le lien ci-dessous pour mettre
à jour ... http://click-here-to-upgrade.webs.com/
Si nous n'avons pas reçu une mise à jour de vous, ils vont détruire
votre boîte aux lettres
Merci.
La page System Administrator@
```

Bien entendu, quand on clique sur le lien, on nous demande de remplir un formulaire en ligne avec notre nom, notre prénom, notre date de naissance et notre code d'accès à notre boîte aux lettres. Ceci est un message typique de phishing ou hameçonnage : c'est une technique utilisée par des fraudeurs pour obtenir des renseignements confidentiels. Le but est de réutiliser ces données personnelles afin de perpétrer une usurpation d'identité ou de contrôler une boîte aux lettres avec toute sa contenance. D'autres types de phishing peuvent se présenter avec des logos bien connus comme celui de la police ou d'un service social bien connu.

3.3 Le piratage informatique

Le piratage informatique est un fléau mondial et les pirates redoublent à chaque fois d'ingéniosité pour contourner les systèmes de sécurité. Voici quelques faits récents de piraterie informatique :

- L'autorité de certification néerlandaise DigiNotar a été piraté en 2011 et plus de 500 certificats frauduleux ont été générés et distribués par les pirates dont un pour intercepter les communications Gmail de milliers d'utilisateurs.
- En 2011, la division sécurité de RSA a subi des attaques qui ont probablement dérobé des informations stratégiques sur la technologie d'authentification SecurID remettant en cause son intégrité.
- En mai 2012, des pirates se sont introduits dans les réseaux informatiques de la présidence de la république française.
- En 2012, suite à la fermeture du site Megaupload par la justice américaine, le groupe Anonymous a piraté plusieurs sites dont celui de Sony Music, d'Universal Music, du FBI et du département de la justice américaine.

3.4 Le cas de Skype

Skype est un logiciel qui permet de communiquer par audio, vidéo ou messagerie instantanée par l'intermédiaire d'Internet. Il a été inventé en 2003 et acheté par Microsoft

en 2012 pour remplacer Windows Live Messenger. L'utilisation de Skype d'ordinateur à ordinateur est gratuite mais nécessite d'être enregistré chez l'éditeur du logiciel. Il est largement utilisé à des fins personnelles mais son utilisation professionnelle pose des problèmes de sécurité. En effet, un certain nombre de notions bien établies par ailleurs pour la sécurité des utilisateurs ne sont pas présentes avec Skype.

- Le respect de la confidentialité des informations transmises n'est pas garanti : écoute de la communication, récupération des informations personnelles.
- Le code source de Skype n'est pas public. Il est difficile d'analyser le fonctionnement de Skype et la méthode utilisée par garantir sa sécurité.
- L'utilisateur n'a pas accès aux paramètres de chiffrement.
- Possibilité de récupération de virus ou de logiciels malveillants.
- Tout ordinateur sur lequel Skype est activé peut devenir un relais pour les autres utilisateurs (peer to peer).
- Skype est difficile à bloquer par un anti-virus ou un pare-feu.

Par ailleurs, dans la page officielle de Skype [17], on peut trouver une grande liste des informations personnelles que Skype peut recueillir et utiliser : données d'identification, informations du profil, données d'identification électronique, informations bancaires et de paiement, produits ou services commandés et fournis, url des vidéos, contenu des messages, informations de géolocalisation des opérateurs mobiles, informations sur l'appareil mobile, etc... Pour toutes ces raisons, Skype a été interdit dans les universités, les centres de recherches et les écoles supérieures en France depuis 2005.

Malgré tout, Skype est devenu un outil de communication pratique et certaines précautions doivent être prises : le poste utilisé ne doit pas contenir de données sensibles, doit être muni d'un bon antivirus et le mot de passe pour Skype doit être différent des autres mots de passe.

4 La confiance numérique : la loi pour la protection des personnes physiques

L'utilisation massive d'Internet et la multiplication des attaques informatiques sur les systèmes et les réseaux ont poussé chaque état dans le monde à légiférer en adoptant plusieurs lois relatives à la sécurité informatique. Ces lois concernent essentiellement les éléments suivants : la contrefaçon, le piratage, l'envoi de spams, le phishing, les arnaques et les fraudes.

4.1 En France

En France, le code pénal contient plusieurs lois relatives aux transactions par Internet. L'utilisation de la cryptographie est libre sauf pour une utilisation à mauvais escient. La loi suivante est un exemple typique du code pénal en France qui a pour but de protéger les communications privées.

```
Article 226-15

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder
ou de détourner des correspondances arrivées ou non à destination et
adressées à des tiers, ou d'en prendre frauduleusement connaissance,
est puni d'un an d'emprisonnement et de 45 000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi,
d'intercepter, de détourner, d'utiliser ou de divulguer des
correspondances émises, transmises ou reçues par la voie des
télécommunications ou de procéder à l'installation d'appareils conçus
pour réaliser de telles interceptions."
```

4.2 Au Maroc

Les nouvelles technologies de l'information et de la communication se développent rapidement au Maroc. Aujourd'hui, la technologie numérique est considérablement utilisée dans les administrations, les universités et les instituts de recherche. L'Internet est devenu familier d'une grande partie des foyers marocains et le nombre des internautes croît de façon exponentielle. Une étude d'Afrinic [2] montre que le Maroc a obtenu 24% des adresses IP délivrées en Afrique en 2011, occupant ainsi la troisième place après l'Egypte avec 31% et l'Afrique du Sud avec 26%. La cybercriminalité et les attaques informatiques ont naturellement suivi le développment des nouvelles technologies (voir [6] et [3] pour plus de détails). Le Maroc a alors renforcé sa lutte contre la cybercriminalité en ratifiant un certain nombre de traités internationaux et surtout en adoptant de nouvelles lois relatives à l'utilisation des nouvelles technologies. C'est ainsi que la loi n° 09-08 [14], relative à la protection des personnes physiques est entrée en vigueur en 2012. C'est une loi qui encourage l'établissement de la confiance numérique, comme stipulé par exemple par l'article 61 de cette loi.

```
Loi n° 09-08, Article 61

Est puni d'un emprisonnement de six mois à un an et d'une amende
de 20.000 à 300.000 DH ou de l'une de ces deux peines seulement,
tout responsable de traitement, tout sous-traitant et toute
personne qui, en raison de ses fonctions, est chargé (e) de
traiter des données à caractère personnel et qui, même par
négligence, cause ou facilite l'usage abusif ou frauduleux des
données traitées ou reçues ou les communique à des tiers non
habilités.

Le tribunal pourra, en outre, prononcer la saisie du matériel ayant
servi à commettre l'infraction ainsi que l'effacement de tout ou
partie des données à caractère personnel faisant l'objet du
traitement ayant donné lieu à l'infraction.
```

5 La confiance numérique : la loi contre la cybercriminalité

Un grand nombre de lois nationales et internationales tentent de protéger les utilisateurs contre les attaques informatiques et la cybercriminalité. Ces lois contribuent à l'établissement de la confiance numérique dans tous les secteurs où des moyens informatiques sont mis en œuvre. C'est ainsi que les pays européens ont adopté en 2001 une convention qui traite la cybercriminalité, en particulier les infractions portant atteinte aux droits d'auteur, la fraude liée à l'informatique, la pornographie enfantine, ainsi que les infractions liées à la sécurité des réseaux.

5.1 En France

En France par exemple, la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 contient des dispositifs contre la cybercriminalité. De même, la Loi Godfrain du 5 janvier 1988 relative à la fraude informatique a introduit les articles 323-1 à 323-7 [10] dans le code pénal, concernant notamment la suppression ou la modification de données.

```
France : Art. 323-3.
En vigueur depuis le 29 Mars 2012,
Modifié par LOI n°2012-410 du 27
mars 2012 - art. 9.

Le fait d'introduire frauduleusement des données dans un système de
traitement automatisé, ou de supprimer ou de modifier frauduleusement
les données qu'il contient est puni de cinq ans d'emprisonnement et
de 75 000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de
traitement automatisé de données à caractère personnel mis en œuvre
par l'Etat, la peine est portée à sept ans d'emprisonnement et à
100 000 euros d'amende.
```

5.2 Au Maroc

Avec le plan Maroc Numeric 2013, le Maroc a pour vision d'équiper et développer Internet dans 100% des écoles, collèges et lycées, et de promouvoir la confiance numérique pour le développement économique du pays. Pour atteindre ces objectifs, Maroc Numeric 2013 a mis en place des initiatives importantes :

- Promouvoir et sensibiliser les acteurs de la société à la sécurité des systèmes d'information.
- Mettre à niveau et renforcer le cadre législatif.

En effet, le Maroc a mis en place un ensemble de textes juridiques contre la cybercriminalité qui visent donc l'instauration de la confiance numérique dans les services en lignes. Ces lois comprennent différents aspects comme par exemple les infractions relatives aux systèmes de traitement automatisé des données, l'échange électronique de données, les

droits d'auteurs, etc. C'est ainsi que la loi n° 07-03 [15], qui est entrée en vigueur en 2003, vise à protéger particulièrement les systèmes informatiques :

```
Maroc : Loi n° 07-03, Article 607-6.

Le fait d'introduire frauduleusement des données dans un système de
traitement automatisé des données ou de détériorer ou de supprimer
ou de modifier frauduleusement les données qu'il contient, leur mode
de traitement ou de transmission, est puni d'un an à trois ans
d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une
de ces deux peines seulement.
```

6 Conclusion

Un système informatique, relié par Internet au reste du monde ne peut pas être protégé à 100%. Cela ne doit pas freiner l'utilisation des moyens numériques. Il faut protéger au mieux les systèmes informatiques, par des outils cryptographiques sophistiqués.

En résumé, la cryptographie est au service de la protection des données et la sécurisation de l'information. C'est donc un pilier important de la confiance numérique. Malgré cela, il faut se rappeler que la sécurité parfaite n'existe pas dans le monde numérique où l'activité humaine est importante, comme l'a si bien dit Eric Schmidt, CEO de Google en 2009 :

```
Eric Schmidt, Google

Si vous faites quelque chose et que vous ne voulez que personne ne le
sache, peut-être devriez-vous déjà commencer par ne pas le faire,
```

mais encore mieux le poète Al-Shanfara il y plus de 1500 ans :

قَالَ الشَّنْفَرَى

وَلِي دُونَكُمْ أَهلُونَ، سَيِّدُ عَمَلَّسٍ وَ أَرْقَطُ زُهْلُولٌ وَ عَرْفَاءُ جَيْأَلُ

هُمُ الأَهْلُ لَا مُستَودَعُ السِّرِّ ذَائِعٌ لَدَيْهِمْ وَ لَا الجَانِي بِمَا جرَّ يُخْذَلُ

Références

[1] Advanced Encryption Standard, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, November 2001.

[2] Afrinic, Annual report 2011. http://www.afrinic.net/multimedia/download/annual_report.pdf

[3] M. Chiny, A. Abou El Kalam, A. Ait Ouahman, Evaluation de la cybercriminalité au Maroc, Cas d'un établissement universitaire ENSA de Marrakech, JNS2, 2012. http://www.ensa.ac.ma/jns2/doc/presentations/Evaluation_de_la_cybercriminalite_au_Maroc.pdf

[4] Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC (1977).

[5] W. Diffie, E. Hellman, New Directions in Cryptography, IEEE Trans- actions on Information Theory, 22, 5 (1976), pp. 644–654.

[6] A. El Azzouzi, La Cybercriminalité au Maroc, 2010. http://www.hamza.ma/Cybercriminalite_au_maroc.pdf

[7] T. El Gamal, A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory IT-31, pp. 496-473, 1976.

[8] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48, 1987, pp. 203–209.

[9] N. Lasfar, Maroc Numeric 2013, la confiance numérique, http://www.salon-ecommerce.ma/pdf/pres/MCINET_Lasfar_31_Mai.pptx

[10] Legifrance, http://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719

[11] J. Hoffstein, J. Pipher, and J. H. Silverman, NTRU : A Ring Based Public Key Cryptosystem in Algorithmic Number Theory. Lecture Notes in Computer Science 1423, Springer-Verlag, pages 267-288, 1998.

[12] V.S. Miller, Use of elliptic curves in cryptography, CRYPTO 85, 1985.

[13] R. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol. 21 (2), 120–126 (1978)

[14] Royaume du Maroc, Loi n° 09-08, http://www.sgg.gov.ma/Projet_loi_09.08_Ar.pdf http://www.sgg.gov.ma/Projet_loi_09.08_Fr.pdf

[15] Royaume du Maroc, Loi n° 07-03, http://www.avocatsdumaroc.com/fr/pdf/textes%20de%20lois/CODE_PENAL/6.pdf

[16] Royaume du Maroc, Loi n° 53-05, http://www.egov.ma/SiteCollectionDocuments/Loi%20n%C2%B053-05%20relative%20%C3%A0%20l%27%C3%A9change%20%C3%A9lectronique%20de%20donn%C3%A9es%20juridiques.pdf

[17] Skype, Politique de confidentialité de Skype, http://www.skype.com/fr/legal/privacy/