Image Cover Sheet

CLASSIFICATION	SYSTEM NUMBER
UNCLASSIFIED	506970

TITLE

UN APERCU SUR LA CRYPTOGRAPHIE DANS LE MONDE INTERNET

System Number:

Patron Number:

Requester:

Notes:

DSIS Use only:

Deliver to:

DEFENCE RESEARCH ESTABLISHMENT
CENTRE DE RECHERCHES POUR LA DÉFENSE
VALCARTIER, QUÉBEC

DREV - N - 9705
Unlimited Distribution / Distribution illimitée

Un aperçu sur la cryptographie dans le monde Internet

par
Jean Savoie

December/décembre 1997

Approved by / approuvé par

Gabriel Arès

Section Head / Chef de section

17 nov. 97

Date

ABSTRACT

This document is an introduction to public-key cryptography and to its mathematical bases. We are interested in cryptography, which is the science of encoding and decoding as a mean to achieve message integrity, authentication, and non-repudiation, when interlocutators communicate over Internet. We consider the notion of key (code) and introduce public-key cryptosystems. We consider the public-key cryptosystem, RSA and analyze a concrete example. Finally, we answer some numbers or cryptography related questions.

RÉSUMÉ

Ce document est une introduction à la cryptographie à clé publique et à ses fondements mathématiques. Nous nous intéressons à l'utilisation de la science de l'encodage et du décodage qui est la cryptographie pour obtenir, lors de communications via le réseau Internet, l'intégrité des messages et l'authentification et la non répudiation des interlocuteurs. Nous abordons la notion de clé (code) et introduisons la notion de clé publique. Le système à clé publique RSA est décrit à l'aide d'un exemple donné en termes concrets. Pour terminer, des réponses sur diverses questions reliées aux nombres et à la cryptographie sont données.

TABLE DES MATIÈRES

FICHE DE SYNTÈSE

La sécurité dans les communications sur le réseau Internet pour les forces canadiennes ainsi que pour le public en général est un élément fondamental de la nouvelle technologie des communications. Il est donc important de comprendre sur quoi est basé la sécurité de ce moyen de communication pour évaluer les risques associés à son usage. Par le biais d'un exemple où Bob envoie un message secret à Alice via le réseau Internet, nous abordons les principaux problèmes de sécurité dans les communications faites sur ce réseau et montrons comment on peut solutionner ces problèmes par l'usage de la cryptographie à clé publique.

Dans un système cryptographique à clé publique, chaque personne possède deux clés (codes): une clé privée que seulement celle-ci connaît et une clé publique qui est connue de tous ceux qui le désire. Par un tel système, lorsque Bob envoie un message secret à Alice, il encode le message avec la clé publique d'Alice. Celle-ci pourra le décoder avec sa clé privée qui est la seule clé pouvant le décoder. Ainsi, le message de Bob à Alice peut être acheminé confidentiellement. D'autre part, nous pouvons obtenir beaucoup plus d'un tel système. Nous pouvons obtenir une preuve de l'intégrité des messages et une preuve non répudiable de l'identité des auteurs respectifs. Par exemple, Alice obtient une preuve de l'intégrité du message en vérifiant que le message décodé ne contient pas de parties inintelligibles (toute modification du message en entraîne).

Un regard plus pointu est jeté sur un système à clé publique particulier basé sur l'important algorithme RSA. Nous en donnons un exemple d'application en termes concrets et en expliquons les bases mathématiques. Nous montrons qu'une clé publique RSA est en fait un couple de nombres entiers (P, n) où n est le produit de deux nombres premiers secrets très grands p et q et où P est relativement premier avec n. Nous montrons aussi que la sécurité de l'algorithme RSA est basée sur la difficulté de mettre en facteur des nombres très grands (de retrouver p et q à partir de n).

Pour terminer, des réponses sur diverses questions reliées aux nombres et à la cryptographie sont données. Entre autres choses, nous montons sur quoi est basé la sécurité de l'algorithme RSA, comment les clés publiques sont calculées et comment de grands nombres premiers peuvent être construits.

En conclusion, cet ouvrage se veut un outil de vulgarisation pour le groupe CCIW (Command and Control Information Warfare) au CRDV et pour les forces canadiennes en général sur (1) les services offerts par les systèmes à clé publique, (2) les systèmes à clé publique basés sur l'algorithme RSA et (3) les fondements mathématiques de ce dernier algorithme.

Ce travail a été entreprit au CRDV entre septembre 1996 et novembre 1996 sous le vecteur 5b, "Future Multi-Environment Electronic War ", Work Unit 5bf12, "C2IS IW Safeguards ".

LISTE DES ACRONYMES

DES	Data Encryption Standard
ICP	Infrastructure à Clé Publique
MD	Message Digest
RSA	Rivest, Shamir, and Aldeman

1.0 INTRODUCTION

Considérons le problème suivant où une personne appelée Bob veut envoyer via le réseau Internet un message secret à une autre personne appelée Alice. Alors comment peut-il procéder pour garder son message secret tout en sachant qu'une espionne nommée Lucie peut intercepter tous ses messages par écoute électronique ou autrement?

Il y a diverses façons de résoudre ce problème. La façon la plus évidente est peut-être celle où Bob encode son message en utilisant un code secret (clé secrète) qu'il partage seulement avec Alice, mais il peut cependant procéder autrement et utiliser un système cryptographique à clé publique. Nous allons principalement nous intéresser ici à cette dernière façon qui sera dans un avenir rapproché un élément essentiel pour la sécurité des communications dans le monde Internet. Nous aborderons la notion de systèmes cryptographiques à clé publique dans le cadre de l'exemple où Bob envoie un message secret à Alice. De plus, nous expliquerons les bases mathématiques de l'important système à clé publique utilisé dans le cadre de cet exemple.

2.0 CRYPTOGRAPHIE ET SECURITÉ INFORMATIQUE

La cryptographie qui est la science du codage et du décodage, offre à Bob et Alice divers moyens d'échanger des messages de façons sûres. Nous allons ici en aborder une qui est employée dans le monde Internet.

2.1 SYSTÈME À CLÉ PUBLIQUE

Lorsque Bob veut envoyer un message encodé à Alice, il peut partager une clé commune avec elle. S'il procède de la même façon pour envoyer des messages à Pierre, Joseph, Aline ..., avec chacun d'entre eux il doit partager une clé. Ainsi, si m personnes veulent communiquer entre elles en utilisant cette procédure, il doit y avoir $m*(m-1)/2$ clés en circulation. Par exemple, pour faire communiquer 1000 personnes entre elles, nous avons besoin de 499500 clés. Nous voyons donc que cette façon de procéder entraîne un problème important de gestion de clés.

Pour éviter le problème de la multitude de clés, il existe les systèmes à clé publique où chaque usager possède seulement 2 clés, une clé publique P et une clé privée (ou secrète) S. Ainsi, si Bob désire envoyer un message à Alice, il lui envoie son message encodé avec la clé publique d'Alice. Celle-ci pourra le décoder en utilisant sa clé privée qu'elle seule connaît. Par conséquent, si m personnes veulent communiquer secrètement entre elles, elles ont besoin de seulement $2*m$ clés, donc seulement 2000 clés pour 1000 personnes.

2.2 ALGORITHME RSA

Rivest, Shamir et Aldeman ont inventés un algorithme (RSA) largement utilisé, qui est la base de plusieurs systèmes à clé publique. Nous allons donner ici un aperçu de cet algorithme. Construisons tout d'abord une clé publique et une clé privée pour Alice, et montrons ensuite comment fonctionne l'algorithme RSA.

- Alice choisit deux nombres premiers p et q. Ces deux nombres sont gardés secrets et ne sont divulgués à personne (ex. $p=7$, $q=11$). Ici p et q sont petits, mais en pratique les

nombres p, q sont très grands (de l'ordre de 2^{256} au moins) pour rendre presque impossible la connaissance de p et q connaissant seulement $n=p*q$,

- Posons

$$n=pq\ (\ n=77)\ et\ \Phi(n)=(p-1)(q-1)\ (\Phi(n)=60=2*2*3*5).$$

Alice choisit alors un nombre quelconque P qui est relativement premier avec $\Phi(n)$ (c.à.d. P et $\Phi(n)$ n'ont pas de facteur commun). P est alors la clé publique d'Alice (en général P est petit). Il est à noter que P et n ne sont pas secrets. Prenons $P=7$ dans le cadre de notre exemple. Ce P a ainsi aucun facteur commun avec $\Phi(n)=60$ et est petit. Remarquons qu'ici P et p sont égaux, mais cela n'est que fortuit.

- La clé secrète est définie comme l'unique valeur S plus petite que n telle que

$$S*P\ mod\ \Phi(n)=1.$$

Dans l'exemple que nous avons considéré ci-haut, nous avons que

$S=43$ est la clé secrète (privée) d'Alice.

Remarquons que $S*P=43*7=301$ et

$S*P\ mod\ \Phi(n)=301 mod\ 60$=le reste de la division par 60 de $301=1$.

Donc,

$$S*P\ mod\ \Phi(n)=1.$$

Maintenant Alice possède une clé publique $P=7$ et une clé secrète $S=43$. Ainsi, Bob peut lui envoyer un message, mais il doit tout d'abord transformer son message en une suite de nombres où chaque nombre est plus petit que $n=77$. Par exemple, son message pourrait être la suite

$$6\ 24\ 3\ 18\ 51\ 38\ 4\ 57\ 32\ 5\ 39\ 16\ 4\ 50\ 35\ 36\ 22\ 32.$$

Cette dernière suite est la représentation du message de Bob avant l'encodage. (Voir la section suivante pour avoir un exemple de représentation numérique d'un texte). Remarquons que toute personne peut lire son message s'il le laisse sous cette forme, car sa façon de transformer les messages en suites de nombres n'est pas secrète . Maintenant, Bob encode son message en évaluant la suite

$$6^P\ mod\ 77,\ 24^P\ mod\ 77,\ldots\ ,32^P\ mod\ 77$$

où $P=7$ est la clé publique d'Alice. Le résultat obtenu est :

$$41\ 73\ 31\ 35\ 72\ 3\ 60\ 29\ 32\ 47\ 74\ 58\ 60\ 8\ 7\ 64\ 22\ 32.$$

Cette suite de nombres est celle reçue par Alice. Pour la décoder, elle évalue tout d'abord la suite

$$41^S \bmod 77,\ 73^S \bmod 77 \ldots, 32^S \bmod 77$$

où $S=43$ est sa clé secrète, pour obtenir :

$$6\ 24\ 3\ 18\ 51\ 38\ 4\ 57\ 32\ 5\ 39\ 16\ 4\ 50\ 35\ 36\ 22\ 32$$

qui est la suite que Bob avait avant l'encodage.

Maintenant, montrons pourquoi le RSA fonctionne. Le RSA est basé sur le théorème d'Euler disant que

$$a^{\Phi(n)} \bmod n = a^{60} \bmod 77 = 1$$

pour tout entier a relativement premier avec n.

Voyons ce qui se produit lors de l'encodage et du décodage par le RSA. Considérons tout d'abord $a=6$, le premier élément de la suite initiale de Bob. Nous savons que son encodage donne $6^P \bmod 77 = 6^7 \bmod 77 = 41$. Pour décoder 41, il suffit d'évaluer $41^S \bmod 77$. En utilisant les propriétés de l'opérateur *mod* (voir section 3.3), nous obtenons que

$$41^S \bmod 77 = 41^{43} \bmod 77 = (6^7 \bmod 77)^{43} \bmod 77$$

$$= 6^{(7*43)} \bmod 77 = 6^{(5*60+1)} \bmod 77 = (6^{60} \bmod 77)^5\, 6^1 = 1^5\, 6 = 6.$$

Ainsi, nous obtenons à nouveau la valeur a qui est 6. Remarquons que dans la dernière équation nous avons $6^{60} \bmod 77 = 1$ par le théorème d'Euler.

En général, si a est un nombre plus petit que n (c.à.d. $a<77$ pour l'exemple ci-haut) et a représente une partie du message initial que Bob veut transmettre à Alice, alors $b=a^P \bmod n$ est l'encodage de cette partie de message. Quand Alice recevra ce message encodé, il lui suffira d'utiliser sa clé secrète S et de calculer

$$b^S \bmod n = a^{S*P} \bmod n = a$$

pour obtenir cette partie du message original de Bob.

2.3 ENVOI D'UN MESSAGE SECRET DE BOB À ALICE

Supposons maintenant que Bob veuille envoyer le message « ce message est secret » à Alice en utilisant un algorithme (simplifié) semblable au RSA avec $p=7$ et $q=11$. Notons que Bob ne peut envoyer que des messages avec des lettres minuscules et des espaces avec cet algorithme simplifié. Tout d'abord, Bob remplace chaque lettre ou espace par une suite de cinq chiffres contenant seulement des 0 ou des 1.

Par exemple, espace=*00000*, a=*00001*, b=*00010*, c=*00011*, d=*00100*, e=*00101*, f=*00110*, g=*00111*, h=*01000*, i=*01001*, j=*01010*, k=*01011*, l=*01100*, m=*01101*, n=*01110*, o=*01111*, p=*10000*, q=*10001*, r=*10010*, s=*10011*, t=*10100*, u=*10101*, v=*10110*, w=*10111*, x=*11000*, y=*11001*, z=*11010*. Remarquons que cette relation entre les lettres et les chiffres n'est pas secrète.

Ainsi le message « ce message est secret » devient la suite de 21 nombres de 5 chiffres suivante :

00011 00101 00000 01101 00101 10011 10011 00001 00111 00101 00000 00101 10011 10100 00000 10011 00101 00011 10010 00101 10100.

Comme $n=77>2^6=64$, nous réécrivons la suite de *1* et de *0* précédente par bloc de *6* en rajoutant *3* zéros à la fin pour avoir un multiple de *6* de chiffres. De cette façon nous transformons une suite de 21 nombres en une suite plus courte de 18 nombres dont chacun a une représentation décimale plus petite que $n=77$. Cela devient :

000110 010100 000011 010010 110011 100110 000100 111001 010000 000101 100111 010000 000100 110010 100011 100100 010110 100000.

Sous la forme décimale, ces *18* nombres de *6* chiffres deviennent la suite suivante de *18* nombres :

6 24 3 18 51 38 4 57 32 5 39 16 4 50 35 36 22 32.

La dernière suite est une représentation du message de Bob avant l'encodage.

Faisons maintenant une digression pour expliquer le pourquoi de la dernière étape. Si nous avions eu n = 2 000 000, nous aurions eu $n>2^{20}$ et ainsi la suite initiale de 21 nombres aurait été transformée en prenant les 0 ou 1 par bloc de 20 en une suite de

seulement 6 nombres plus petit que n. De cette façon plus n est grand plus la suite est courte.

Remarquons que toute personne peut lire le message de Bob s'il le laisse sous cette dernière forme. Maintenant Bob encode son message en évaluant la suite
$6^P \bmod 77,\ 24^P \bmod 77,\ldots\ ,32^P \bmod 77$ où $P=7$ est la clé publique d'Alice. Le résultat obtenu est :

$$41\ 73\ 31\ 35\ 72\ 3\ 60\ 29\ 32\ 47\ 74\ 58\ 60\ 8\ 7\ 64\ 22\ 32.$$

Cette dernière suite de nombres est reçue par Alice. Celle-ci peut la lire en évaluant
$41^S \bmod 77,\ 73^S \bmod 77,\ldots\ ,32^S \bmod 77$ où $S=43$ est sa clé secrète. Elle obtient alors :

$$6\ 24\ 3\ 18\ 51\ 38\ 4\ 57\ 32\ 5\ 39\ 16\ 4\ 50\ 35\ 36\ 22\ 32$$

qui est la suite que Bob avait avant l'encodage. En faisant maintenant les opérations initiales inverses de Bob, elle obtient le message « ce message est secret ».

2.4 SYSTÈME À CLÉ PUBLIQUE POUR FIN D'INTÉGRITÉ ET AUTHENTIFICATION

Alice reçoit un message signé par Bob. Comment peut-elle être sûre que ce message provient bien de Bob et que ce message n'a pas été modifié en cours de route ?

Si elle connaît la clé publique de Bob, ils pourraient procéder de la façon suivante. Bob encode son message en utilisant une méthode quelconque (le message peut ne pas être codé aussi). Prenant le résultat obtenu après cette opération, il l'encode à l'aide de sa clé privée et annexe le tout. Quand Alice reçoit le message et son annexe, elle utilise la clé publique de Bob pour décoder l'annexe. Si l'annexe décodé et le message sont identiques, alors il s'agit bien d'un message de Bob car seulement lui connaît sa clé privée qui est la seule clé ayant pu encoder l'annexe de la sorte. De plus, Alice est certaine que le message n'a pas été modifié en cours d'acheminement.

Remarquons que cette façon de procéder oblige Bob à faire de longs calculs avec sa clé privée. Il y un moyen de diminuer cela. Après avoir encodé son message, Bob construit un résumé de son message (à l'aide d'un algorithme comme MD 5 par exemple, voir [1]) et l'encode avec sa clé privée. Lorsque Alice reçoit le tout, elle calcule le résumé du message

et le compare avec le décodage de l'annexe obtenu à partir de la clé publique de Bob. S'ils correspondent, Alice obtient la même assurance que précédemment.

Si Alice ne connaît pas la clé publique de Bob, elle doit s'assurer que Bob et sa clé publique correspondent bien. Pour ce faire, elle peut consulter un organisme certifiant qu'une clé publique donnée appartient bien à une personne donnée. Au Canada, le système ICP (Infrastructure à clé publique) du gouvernement fédéral sera d'ici 1998 l'organisme central de certification. Il sera basé sur le système Entrust de Nortel Telecom qui est déjà en opération.

2.5 SYSTÈME À CLÉ PUBLIQUE POUR FIN DE NON RÉPUDIATION (SIGNATURE ÉLECTRONIQUE)

Bob fait une offre d'achat sur la maison d'Alice. Comment Alice peut-elle faire pour prouver que Bob a bien fait cette offre en utilisant un système à clé publique?

Il suffit de demander à Bob de faire un résumé de l'offre, de l'encoder à l'aide de sa clé privée et d'annexer le tout à l'offre d'achat. Ainsi, il est facile de prouver à quiconque que Bob a bien fait cette offre d'achat. Cette personne n'a qu'à faire un résumé de l'offre et à le comparer au décodage de l'annexe avec la clé publique de Bob. Si elles correspondent, celà prouve que Bob a bien fait cette offre car seulement lui connaît sa clé privée qui est l'unique clé pouvant encoder le résumé de la sorte.

Bien entendu, Bob doit garder sa clé privée secrète car sinon toute personne connaissant celle-ci pourrait forger une offre d'achat au nom de Bob. Nous dirons qu'ici Bob a fait une signature électronique de l'offre d'achat.

3.0 QUELQUES RÉPONSES

3.1 QU'EST-CE QU'UN NOMBRE PREMIER ?

p est un nombre premier s'il est un entier divisible que par 1 et lui même, et est différent de 1. Les premiers nombres premiers sont *2, 3, 5, 7, 11, 13, 17, 19, ...* Remarquons qu'il n'existe pas de plus grand nombre premier. De plus, dans l'intervalle *(0,x),* il existe approximativement $x/ln(x)$ nombres premiers.

3.2 QUELLES SONT LES PROPRIÉTÉS DE L'OPÉRATEUR MODULO (MOD) ?

Par définition

$a \bmod n$= le reste de la division de a par n.

Par exemple $9 \bmod 4=1$, $17 \bmod 5=2$ et $307 \bmod 40=27$. L'opérateur modulo possède la propriété suivante :

$$(ab) \bmod n=((a \bmod n)*(b \bmod n)) \bmod n.$$

Cette propriété permet de simplifier les calculs. Par exemple calculons $2^{50} \bmod 5$. Tout d'abord, nous avons

$$2^1 \bmod 5=2,\ 2^2 \bmod 5=4,\ 2^4 \bmod 5=((2^2 \bmod 5)(2^2 \bmod 5)) \bmod 5$$
$$=(4*4) \bmod 5=1,$$
$$2^8 \bmod 5=(2^4 \bmod 5)(2^4 \bmod 5) \bmod 5=(1*1) \bmod 5=1.$$

D'une façon similaire, nous avons aussi

$$2^{16} \bmod 5=2^{32} \bmod 5=1.$$

Comme $50=32+16+2$, nous obtenons donc que

$$2^{50} \bmod 5=((2^{32} \bmod 5)(2^{16} \bmod 5)(2^2 \bmod 5)) \bmod 5=(1*1*4) \bmod 5=4.$$

De cette façon, nous pouvons calculer rapidement des valeurs de type a^p où p est grand. Cela est très utile dans l'algorithme RSA.

3.3 POURQUOI L'ALGORITHME RSA EST-IL SÛR ?

Remarquons que si nous pouvons trouver les deux nombres p et q tels que $n=p*q$, (factoriser n), nous pouvons facilement trouver la clé secrète d'Alice. En effet, connaissant

p et q, nous connaissons $\Phi(n)=(p-1)(q-1)$. Maintenant en utilisant l'algorithme de la division d'Euclide (voir question 4), nous pouvons trouver l'unique $S<n$ tel que

$$S*P \bmod \Phi(n)=1.$$

Comme il est très difficile de factoriser de grands nombres, il est très difficile de trouver S pour ensuite déchiffrer le message. Pour ce qui est du message de Bob à Alice, il est facile de factoriser $n=77=7*11$, car n est petit. Donc il est facile de trouver S pour déchiffrer le message de Bob. En pratique, nous avons que $n>2^{512}$.

3.4 COMMENT TROUVER LA CLÉ SECRÈTE $S=43$ D'ALICE

Nous appliquons la méthode d'Euclide (voir [3, 4]) avec $\Phi(n)=60$ et $P=7$. Nous divisons 60 par 7 pour obtenir le reste 4, puis divisons 7 par 4 pour obtenir le reste 3, et puis divisons 4 par 3 pour obtenir le reste 1. Le processus se termine quand le reste est 1. Ce processus est toujours possible, car $\Phi(n)$ et P sont relativement premier. En résumé, nous avons obtenu jusqu'à maintenant que

$$60=8*7+4,\ 7=1*4+3,\ 4=1*3+1.$$

De là, nous obtenons que

$$1=4-1*3,\ 3=7-1*4.$$

Donc, $1=4-1*(7-1*4)=-7+2*4$ (c. à .d. $1=-1*7+2*4$). D'autre part, nous avons $4=60-8*7$. Nous en déduisons que

$$1=-7+2*(60-8*7)=2*60-17*7 \text{ (c.à.d. } 1=2*60-17*7)$$

et ainsi $17*7=2*60-1$. Donc, $17*7=-1 \bmod 60$. Pour remplacer le -1 par 1 dans la dernière équation, nous remplaçons 17 par $60-43$ pour obtenir $60*7-43*7=-1 \bmod 60$ et

$$-43*7=-1 \bmod 60.$$

En multipliant par -1, nous obtenons le résultat désiré qui est

$$43*7=1 \bmod 60.$$

En général, comme $\Phi(n)$ et P sont relativement premier, en procédant comme nous l'avons fait plus haut, il est toujours possible d'écrire le nombre 1 comme $1=S*P\pm k*\Phi(n)$ avec $1<S<\Phi(n)$ et k un entier. Ainsi, il est possible de calculer la clé secrète S dans tous les cas.

3.5 COMMENT TROUVER DES NOMBRES PREMIERS *p* TRÈS GRANDS

Dans la pratique on choisit au hasard un nombre très grand p à l'aide d'un générateur de nombres aléatoires ou autrement. Pour voir si p est vraiment premier, on utilise une méthode probabiliste. Par exemple, on choisit des nombres aléatoires $a_1, a_2, \ldots a_n$ plus petit que p et on évalue $(a_i)^{(p-1)/2} \bmod p$ pour $i=1,\ldots n$. Si chaque résultat donne 1 ou -1, on accepte p comme un nombre premier, sinon il n'est pas premier et on choisit un autre p jusqu'à ce que le processus se termine. Puisque la probabilité que pour un nombre a on ait $(a)^{(p-1)/2} \bmod p$ égal 1 ou -1 lorsque p est non premier est plus petite que ½, la probabilité que le p choisi par la méthode précédente ne soit pas premier est plus petite que $(½)^n$. Ainsi pour $n=50$, il y a au plus 1 chance sur 100000000000000 (10^{14}) que p ne soit pas premier.

3.6 COMMENT S'ASSURER QU'UN NOMBRE EST VRAIMENT ALÉATOIRE (CHOISI AU HASARD)

Ce n'est pas un problème facile. Une façon simple consiste à prendre une pièce de monnaie bien balancée et à la lancer n fois en inscrivant un 1 pour un pile et un 0 pour une face après chaque lancer. Le résultat pour $n=10$ pourrait être la suite suivante

$$1100100100.$$

Cette suite représente un nombre en base 2. En utilisant la base 10, ce nombre égale 1604. Par contre, cette façon de procéder est difficilement applicable aux ordinateurs car pour que la suite de 1 et de 0 soit vraiment aléatoire, il ne faut pas qu'il y ait un moyen de prédire avec une probabilité supérieure à ½ les termes (0 ou 1) de la suite connaissant les précédents. Ainsi, si l'ordinateur utilise une fonction déterministe pour calculer la suite de 0 et de 1, le nombre obtenu n'est pas aléatoire.

Diverses techniques peuvent être appliquées pour obtenir des nombres presques aléatoires. Par exemple, le programme PGP (Pretty Good Privacy) utilise l'espacement de temps entre les touches d'un usager tapant sur son clavier d'ordinateur durant quelques secondes et une phrase secrète de cet usager pour trouver sa clé privée et sa clé publique. De plus, PGP utilise ces dernières informations pour le choix des clés DES. Certaines

méthodes utilisent la vitesse de rotation du disque dur. Mais, pour chaque méthode utilisée, il doit y avoir une étude extensive de celle-ci pour être certain que les clés construites ne sont pas qu'un sous-ensemble restreint des clés possibles, car la clé secrète pourrait être compromise par une attaque par force brute (par l'essai de toutes les clés qui appartiennent à l'ensemble des clés qui peuvent être construites). Dans la même veine, s'il existe un sous-groupe de clé qui est beaucoup plus probable que les autres, une attaque par force brute sur les clés de ce sous-groupe pourrait souvent être efficace.

3.7 EST-CE QUE LE RSA EST RAPIDE ?

Comme l'encodage par l'algorithme RSA est relativement lent (*100* à *1000* fois moins rapide) relativement à des systèmes (symétriques) à clé unique comme le DES (Data Encryption Standard), lorsque le document à encoder est long il est préférable de procéder autrement. Pour transmettre un document important, Bob encode une clé DES de *64* bits qu'il a construite et qui ne sera utilisée qu'une seule fois en utilisant la clé publique d'Alice. Le reste du document est encodé à l'aide de cette clé DES. Lorsqu'Alice reçoit le message de Bob, elle utilise sa clé privée S pour obtenir la clé DES qui a servi à l'encodage du reste du document. Elle est la seule personne qui peut lire cette clé. De là, elle peut décoder le reste du document.

3.8 EST-CE QUE LA CRYPTOGRAPHIE SE LIMITE AU RSA ET AU DES ?

Evidemment non. Ces deux algorithmes sont très utilisés mais il en existe une multitude d'autres. La cryptographie qui est la science qui étudie les codes est en plein développement. Par exemple, il se fait beaucoup de recherches sur les codes correcteurs qui sont des codes qui peuvent s'autocorriger après une erreur de transmission. Pour plus de détails sur les codes correcteurs, voir [5] qui est un ouvrage important sur le sujet.

4.0 CONCLUSIONS

Dans cette note technique, nous avons étudié les systèmes à clé publique en général et le système RSA en particulier qui est le plus courant. Nous avons analysé les bases mathématiques du système RSA et décrit son fonctionnement. Les systèmes à clé publique lorsqu'ils sont associés à un organisme de certification comme l'IPC sont importants puisqu'ils permettent d'offrir les services: de confidentialité, d'intégrité, authentification et de non répudiation pour les communications. Ces systèmes peuvent être améliorés par l'ajout d'un système symétrique comme DES (Data Encryption Standard) et par l'utilisation de résumés. De plus, sans organisme de certification, le service de non répudiation ou de signature électronique n'est pas assuré.

RÉFÉRENCES

1. Schneier, B., "Applied Cryptography ", John Wiley & Sons, New York, 1994.

2. Ford, W., "Computer Communication Security", Prentice Hall, Toronto, 1994.

3. Koblitz, N., "A Course in Number Theory and Cryptography", Springer-Verlag, 1994.

4. De Konick, J. M., and Mercier, M., "Introduction à la Théorie des Nombres", Modulo, 1994.

5. MacWilliams, F. J., and Sloane, N. J. A., "The Theory of Error Correcting Codes", North-Holland Mathematical Library, 1977.

DISTRIBUTION INTERNE

DREV N - 9705

1 - Deputy Chief

1 - Chief Scientist

6 - Document Library

1 - Dr. J. Savoie (auteur)

1 - Dr. G. Otis

1 - Mr. G. Thibault

1 - Dr. S. Dahel

1 - Mr. J.-C. Labbé

1 - Mr. G. Picard

1 - Mr. R. Charpentier

1 - Dr. J. Gélinas

1 - Mr. D. Gouin

1 - Dr. G. Vézina

1 - Mr R. Fortin

1 - Mrs S. Lam

1 - Mrs I. Abi-Zeid

1 - Mr P. Labbé

1 - Mr D. Demers

1 - LCdr S. Dubois

DISTRIBUTION EXTERNE

DREV N - 9705

1 - DSIS

1 - DRDB

Attn: Mr. V. Taylor

1 - DSACCIS

1 - DSAA

SANS CLASSIFICATION
COTE DE SÉCURITÉ DE LA FORMULE
(plus haut niveau du titre, du résumé ou des mots-clefs)

FICHE DE CONTRÔLE DU DOCUMENT

1. PROVENANCE (le nom et l'adresse)

CRDV
2459 boul. Pie-XI Nord
Val-Bélair QC G3J 1X5

2. COTE DE SÉCURITÉ (y compris les notices d'avertissement s'il y a lieu)

SANS CLASSIFICATION

3. TITRE (Indiquer la cote de sécurité au moyen de l'abréviation (S,C, R ou NC) mise entre parenthèses, immédiatement après le titre.)
UN APERCU SUR LA CRYPTOGRAPHIE DANS LE MONDE INTERNET (SC)

4. AUTEURS (Nom de famille, prénom et initiales. Indiquer les grades militaires, ex.: Bleau, Maj. Louis E.)

SAVOIE, Jean

5. DATE DE PUBLICATION DU DOCUMENT (mois et année)	6a. NOMBRE DE PAGES	6b. NOMBRE DE RÉFÉRENCES
October 1997	21	5

7. DESCRIPTION DU DOCUMENT (La catégorie du document, par exemple rapport, note technique ou mémorandum. Indiquer les dates lorsque le rapport couvre une période définie.)

Note technique

8. PARRAIN (le nom et l'adresse)

CRDV
2459 boul. Pie-XI Nord, Val-Bélair QC G3J 1X5

9a. NUMÉRO DU PROJET OU DE LA SUBVENTION (Spécifier si c'est un projet ou une subvention)	9b. NUMÉRO DE CONTRACT
5 BF12	N/A

10a.NUMÉRO DU DOCUMENT DE L'ORGANISME EXPÉDITEUR	10b. AUTRES NUMÉROS DU DOCUMENT
N- 9706	N/A

11. ACCÈS AU DOCUMENT (Toutes les restrictions concernant une diffusion plus ample du document, autres que celles inhérentes à la cote de sécurité.)

- [X] Diffusion illimitée
- [ ] Diffusion limitée aux entrepreneurs des pays suivants (spécifier)
- [ ] Diffusion limitée aux entrepreneurs canadiens (avec une justification)
- [ ] Diffusion limitée aux organismes gouvernementaux (avec une justification)
- [ ] Diffusion limitée aux ministères de la défense
- [ ] Autres (préciser) :

12. ANNONCE DU DOCUMENT (Toutes les restrictions à l'annonce bibliographique de ce document. Cela correspond, en principe, aux données d'accès au document (11). Lorsqu'une diffusion supplémentaire (à d'autres organismes que ceux précisés à la case 11) est possible, on pourra élargir le cercle de diffusion de l'annonce.)

Tous

SANS CLASSIFICATION
COTE DE LA SÉCURITÉ DE LA FORMULE

13. SOMMAIRE (Un résumé clair et concis du document. Les renseignements peuvent aussi figurer ailleurs dans le document. Il est souhaitable que le sommaire des documents classifiés soit non classifié. Il faut inscrire au commencement de chaque paragraphe du sommaire la cote de sécurité applicable aux renseignements qui s'y trouvent, à moins que le document lui-même soit non classifié. Se servir des lettres suivantes: (S), (C), (R) ou (NC). Il n'est pas nécessaire de fournir ici des sommaires dans les deux langues officielles à moins que le document soit bilingue.)

(SC) Ce document est une introduction à la cryptographie à clé publique et à ses fondements mathématiques. Nous nous intéressons à l'utilisation de la science de l'encodage et du décodage qui est la cryptographie pour obtenir lors de communications via le réseau Internet, l'intégrité des messages et l'authentification et la non répudiation des interlocuteurs. Nous abordons la notion de clé (code) et introduisons la notion de clé publique. Le système à clé publique RSA est décrit à l'aide d'un exemple donné en termes concrets. Pour terminer, des réponses sur diverses questions reliées aux nombres et à la cryptographie sont données.

14. MOTS-CLÉS, DESCRIPTEURS OU RENSEIGNEMENTS SPÉCIAUX (Expressions ou mots significatifs du point de vue technique, qui caractérisent un document et peuvent aider à le cataloguer. Il faut choisir des termes qui n'exigent pas de cote de sécurité. Des renseignements tels que le modèle de l'équipement, la marque de fabrique, le nom de code du projet militaire, la situation géographique, peuvent servir de mots-clés. Si possible, on doit choisir des mots-clés d'un thésaurus, par exemple le "Thesaurus of Engineering and Scientific Terms (TESTS) ". Nommer ce thésaurus. Si l'on ne peut pas trouver de termes non classifiés, il faut indiquer la classification de chaque terme comme on le fait avec le titre.)

CRYPTOGRAPHIE
SYSTÈME CRYPTOGRAPHIQUE À CLÉ PUBLIQUE
ALGORITHME RSA

#506970