PROTÉGEZ VOS PETITS SECRETS GRÂCE AUX NOMBRES PREMIERS

LE 14 JANVIER 2011 ***SCIENCE ÉTONNANTE***

Qu'on soit journaliste, avocat ou diplomate, il est parfois important de sécuriser ses données. Pour cela on utilise des méthodes de chiffrement. Mais comment ça fonctionne ?

Imaginons que vous soyez le chef de la diplomatie de votre pays, et que vos ambassadeurs aient besoin de vous envoyer des messages top secrets. **Afin d'échapper aux oreilles de l'ennemi et de Wikileaks, vous allez avoir besoin de coder ces messages**. Comment faire ?

La cryptographie basique

Pour cela, vous pouvez choisir une méthode simple, comme substituer une lettre par une autre dans l'alphabet. C'est le principe qu'utilisait César pour communiquer avec ses généraux. Les messages étaient codés de la manière suivante : chaque lettre est remplacée par la lettre située 3 cases plus loin dans l'alphabet : A devient D, B devient E, etc. En voici le principe en image pour coder le mot « BONJOUR » :

CODAGE

Message	B	O	N	J	O	U	R
	2	15	14	10	15	21	18
Chiffres + 3	5	18	17	13	18	24	21
Message codé	E	R	Q	M	R	X	U

DECODAGE

Message codé	E	R	Q	M	R	X	U
	5	18	17	13	18	24	21
Chiffres -3	2	15	14	10	15	21	18
Message décodé	B	O	N	J	O	U	R

Les méthodes de substitution simples sont malheureusement assez peu sûres car chaque lettre est toujours codée de la même manière : **on peut donc casser ces codes en faisant de la statistique** et en analysant les occurrences des lettres : ainsi en français, le E est la lettre qui doit revenir le plus souvent, suivie des lettres AIST, qui bien sûr sont elles-mêmes bien plus fréquentes que WXYZ.

La cryptographie à clé

Pour éviter cela, il faut un codage dans lequel une même lettre n'est pas toujours codée de la même manière. C'est le principe des **codes à clé**. Imaginons que l'on veuille encoder le mot « BONJOUR » et qu'on choisisse comme clé de cryptage le mot « DECO ». On convertit chaque lettre du mot et de la clé en chiffre (A=1, B=2, …,Z=26), on les additionne et on reconvertit les chiffres obtenus en lettre. Comme la clé est souvent un simple mot, on la répète autant de fois que nécessaire pour coder l'ensemble du message. Pour décoder, on fait la même chose mais en soustrayant la clé au message codé. En voici l'illustration :

CODAGE

Message	B	O	N	J	O	U	R
	2	15	14	10	15	21	18
Clé	D	E	C	O	D	E	C
	4	5	3	15	4	5	3
Addition	6	20	17	25	19	26	21
Message codé	F	T	Q	Y	S	Z	U

DECODAGE

Message codé	F	T	Q	Y	S	Z	U
	6	20	17	25	19	26	21
Clé	D	E	C	O	D	E	C
	4	5	3	15	4	5	3
Soustraction	2	15	14	10	15	21	18
Message décodé	B	O	N	J	O	U	R

Et vous voyez ici que les deux lettres O du mot « BONJOUR » sont bien codées par une lettre différente. On ne peut pas facilement casser ce code par des analyses statistiques.

Toutefois le codage à clé pose un autre problème car il s'agit d'un **codage symétrique : si vous savez coder les messages, alors vous savez aussi automatiquement les décoder**. Donc si un espion parvient à se procurer la clé que vous donnerez à votre ambassadeur, alors l'ennemi saura ensuite décrypter les messages qu'il vous enverra !

La cryptographie asymétrique

La solution pour s'en sortir est d'utiliser une méthode de **cryptographie asymétrique, c'est-à-dire où les procédures de codage et de décodage sont très différentes**, de sorte que quelqu'un qui sache encoder les messages ne sache pas pour autant les décoder. Comment est-ce possible ?

Un algorithme asymétrique fait appel à deux clés : **une clé dite « publique » qui sert à encoder le message, et une clé dite « privée » qui sert à le décoder**. Donc si vous êtes le chef de la diplomatie, vous expédiez une clé publique à votre ambassadeur, et vous gardez pour vous la clé privée correspondante. Vos diplomates pourront encoder les messages, mais s'ils se font voler la clé publique, l'ennemi ne pourra pas pour autant décoder vos communications, car seule la clé privée permet de le faire !

L'algorithme RSA

L'algorithme asymétrique le plus populaire s'appelle l'algorithme RSA, en référence à ses concepteurs Rivest Shamir et Adleman, qui l'ont inventé au MIT à la fin des années 70. Il est relativement simple car il ne fait appel qu'à des notions élémentaires d'arithmétique. Ceux qui veulent le calcul précis peuvent aller voir plus bas, mais pour ceux que les maths fatiguent, il est basé en gros sur le principe suivant : **vous choisissez deux nombres premiers P et Q, vous les multipliez pour obtenir un nombre N=P.Q. Le nombre N donne la clé publique, alors que la privée nécessite de connaître la décomposition en P et Q.**

Il est vrai qu'en théorie, la connaissance de la clé publique N permet de déduire la clé privée (P,Q) : il suffit de factoriser N. Sauf que factoriser un nombre peut être une opération très longue, même avec un gros ordinateur. Donc il suffit de choisir des nombres premiers suffisamment grands et en pratique la décomposition de N en P*Q sera très difficile et le codage RSA impossible à violer par le calcul (sauf en un temps égal au nombre de protons dans l'Univers…)

LE RSA EN PRATIQUE

L'algorithme RSA est assez difficile à utiliser pour chiffrer des grands messages, car bien que les opérations de base soient élémentaires (multiplication, puissance, division), les calculs peuvent se faire sur des nombres énormes et prendre pas mal de temps.

Néanmoins pour des codes de carte bleue ou des requêtes vers des sites internet, ça reste faisable. D'ailleurs le RSA est largement employé dans ce type d'applications.

Pour en revenir à nos ambassadeurs, la puissance et l'importance stratégique du RSA est telle qu'en France, il a longtemps été classé « **Arme de deuxième catégorie** » (catégorie à laquelle appartiennent entre autres les Rafales, les porte-avions et les sous-marins). Dans le même genre, le gouvernement américain l'a aussi classé comme arme et a interdit pendant longtemps l'exportation de l'algorithme en dehors du territoire. Évidemment interdire l'exportation d'un algorithme, ça paraît difficile, et des petits malins anarcho-libertaires se sont amusés à se transformer en « arme d'exportation illégale » en se faisant tatouer l'algorithme RSA. Très tendance sur la plage…

BONUS : Pour les violents, le détail de l'algorithme RSA

Choisissez deux nombres premiers P et Q (que vous gardez pour vous), prenons par exemple P=5 et Q=11.

Fabriquez le produit des deux N=P.Q, dans notre cas N=55.

*Choisissez un nombre E n'ayant pas de facteur premier commun avec (P-1).(Q-1) Dans notre cas puisque (P-1).(Q-1) = 40 = 2*2*2*5, on peut choisir par exemple E = 7.*

La paire (E,N) constitue la clé publique, que vous donnez à votre ambassadeur

*Choisissez ensuite un nombre D tel E.D modulo (P-1).(Q-1) = 1 par exemple dans notre cas D = 23 fait l'affaire car 7*23 modulo 40 = 1*

La paire (D,N) constitue la clé privée, que surtout vous gardez pour vous.

Comment se passe la procédure d'encodage ? Tout d'abord il vous faut ramener votre message à un nombre. Vous pouvez le faire par le moyen que vous voulez comme A=01 ; B=02 ; … ;Z =26 par exemple. Une fois votre message traduit sous la forme d'un nombre M, vous allez encoder ce nombre avec la clé publique (E,N) de la manière suivante :

> ***$C = M^E$ modulo N***

Pour décoder C (et donc retrouver M), il vous faut appliquer une opération différente, utilisant la clé privée (D,N) :

> ***C^D modulo N.***

Et c'est là que les maths des nombres premiers nous sont utiles, car elles permettent de prouver que ça marche c'est-à-dire que l'opération de décodage permet effectivement bien de retrouver le message M initial. On peut en effet démontrer que :

> ***$(M^E \text{ modulo } N)^D$ modulo N = M***

PHIL
le 14 janvier 2011 - 13:51 • SIGNALER UN ABUS - PERMALINK

Jghfdrttreyugcx345321556 :))))

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PATRICE BOCK
le 17 janvier 2011 - 9:48 • SIGNALER UN ABUS - PERMALINK

Applications pratiques RSA pour grand public, en logiciel libre :
- truecrypt permet de chiffrer des répertoires ou disques complets (utilisés par les pros de la sécurité et – j'espère – les journalistes qui se font "réquisitionner" leurs PCs)
- GnuPG : permet de chiffrer/déchiffrer/signer textes et fichiers, avec des add-ons qui permettent d'automatiser son utilisation dans les clients emails (pgp4win pour outlook par exemple)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

AZEE
le 19 janvier 2011 - 18:00 • SIGNALER UN ABUS - PERMALINK

Merci pour ce petit tour très intéressant dans ce vaste domaine de la cryptographie

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

THILP
le 8 février 2011 - 23:25 • SIGNALER UN ABUS - PERMALINK

Bonjour,

TrueCrypt n'utilise pas RSA : cet algorithme n'est intéressant que lorsqu'il doit y avoir communication de données (par exemple, client-banque). Sinon, c'est du gâchis : RSA exige des clefs bien plus grandes et une puissance de calcul terriblement plus importante que les algorithmes à clef privée comme AES. En vous y penchant un peu, vous constaterez que TrueCrypt laisse le choix de l'algorithme à l'utilisateur, mais seulement parmi des chiffrements symétriques : AES, Serpent et Twofish (et des combinaisons de ceux-ci).

Quant à l'utilisation en tant que solution de protection de disque, puisque c'est un logiciel « hors OS » (à la différence des chiffrements « natifs » des distributions Linux ou de BitLocker sous Windows), il ne peut pas démarrer (à ma connaissance) en même temps que le système ; ni, par conséquent, chiffrer tout le disque. Alors que le vol (appelons un chat un chat) de l'ordinateur d'un journaliste permet d'accéder non seulement aux fichiers du type « contenu de Mes documents » (que TrueCrypt est à même de chiffrer), mais aussi, par exemple, aux données de navigation (historique, cookies, etc.), au carnet d'adresse du logiciel de messagerie… ou aux certificats de révocation de clefs de GnuPG, par exemple, que vous n'aurez sans doute pas pensé à protéger !

En sécurité informatique, les (bons) outils ne font souvent que la plus petite part du travail ; la plus importante est du ressort de « ce qui se trouve entre la chaise et le clavier » et qui emploie ces outils, à bon escient ou n'importe comment. Les journalistes qui ne le savent pas doivent en prendre conscience avant de se barder de logiciels (aussi excellents que soient TrueCrypt et GnuPG, ce que je reconnais de bonne grâce), qui nuisent davantage qu'ils ne protègent lorsqu'ils sont mal employés, à cause du sentiment de sécurité que leur usage peut procurer.

Il existe une très bonne et variée documentation en matière de cryptologie sur Internet (sans oublier les bouquins de Bruce Schneier), dont la consultation est salutaire : la cryptanalyse se joue beaucoup des « apprentis-sorciers ». ;)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

1 ping

Tweets that mention Protégez vos petits secrets grâce aux nombres premiers » Article » OwniSciences, Société, découvertes et culture scientifique -- Topsy.com le 14 janvier 2011 - 15:07

[...] This post was mentioned on Twitter by Regis Deutsch and others. Regis Deutsch said: RT @owni: Protégez vos petits secrets grâce aux nombres premiers http://bit.ly/hZd9ew sur @owni sciences [...]