Cryptographie Publique

Introduction:

La majorité des algorithmes sont ***à clef privée***. D'où une difficulté : Les deux interlocuteurs doivent se mettre d'accord sur ***le choix de la clef privée*** qu'ils utiliseront l'un et l'autre.

D'où l'idée de système ne nécessitant pas de ***clef privée commune*** :

_ Systèmes ***à clefs publiques.***

_ Ou encore des algorithmes sans clef commune.

Système RSA:

L'idée d'un système ***à clef publique*** est d'utiliser un algorithme difficilement inversible de telle sorte que ***tout le monde puisse coder***, mais qu'il n'y ait ***qu'une personne qui puisse décoder.***

A/ Historique :

Cette méthode a été créée en 1977 par Rivest, Shamir et Adleman, d'où le nom de RSA.

B/ Théorie :

Etude Préalable de l'expediteur :

p et q premiers ; n=p*q ; ?(n)=(p-1)*(q-1) ; k<?(n) et k premier avec ?(n) ; ? tel que k*? ?1 [?(n)]. Les nombres k et n sont publiés : Ce sera ***la clef publique*** et ? sera ***la clef secrète.***

Codage :

Pour chacun des nombres "m", Bob calcule "c"=m^k mod [n] et envoie ces nombres "c" à Alice.

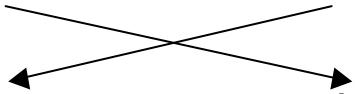
Décodage :

Alice calcule $c^?$ mod [n] et elle retrouve "m".

C/ Echange de clef :

On peut ainsi se communiquer des clefs afin d'utiliser un ***codage symétrique*** (c'est à dire un système ***à clef privée***). Soient k et n ***publics*** :

Alice :	**Bob :**
aléa : $x < n$	aléa : $y < n$
$X = k^x \bmod [n]$	$Y = k^y \bmod [n]$
$Y^x \bmod [n] = C$	$X^y \bmod [n] = C$



Alice et Bob pourront communiquer avec un ***algorithme à clefs privée*** en utilisant la clef C.

D/ Application :

p=389 ; q=167 ; k=17 . On calcule n=64 963 et ?(n)=64 408 et on trouve ? =26 521. Application. Cela fonctionne également dans l'autre sens ; dans le cadre d'***une signature***.

Cette méthode de calcul prend du temps. Pour des applications plus sérieuses, on sera amené à introduire une procédure d'***exponantiation modulaire*** bien plus rapide.

E/ Exemple de piratage :

Pour de petits nombres, il est très facile de pirater un code RSA ... Il suffit de factoriser "n" : On trouve p et q, et on en déduit ? et on peut pirater.

La fiabilité du RSA repose sur l'écart entre la ***difficulté de factorisation*** et la ***facilité à trouver de grands nombres premiers***.

Conclusion:

La cryptographie ***à clefs publiques*** permet donc de communiquer en sécurité ou encore de s'échanger des clefs. Mais peu de méthodes sont couramment utilisées ; celle du RSA est la plus connue. Il en existe d'autres méthodes, purement théoriques, ou encore des méthodes ***sans clefs privée commune*** qui ne connaissent pas d'application pratique ... alors est-ce impossible ou est-ce que certaines idées n'ont tout simplement pas été approfondies ?

Bibliograghie :

_ Science et Avenir ; n°580 de juin 1995, article « L'aventure des codes secrets ».
_ Tangente ; Hors série n°6 de mai 1998, article « Secret des nombres ».
_ Pirate magazine ; nombreux articles.
_ La Recherche ; numéro spécial nombres, n°278 de juillet/août 1995, article « Nombres premiers ».
_ Quadrature ; n°9 de juillet/août 1991, article « La cryptographie à clefs publiques ».
_ 15 leçons de Maple de Jean-Claude Leickman.
_ SMAI (Société des mathématiques appliquées et industrielles) n°8, chapitre « Cryptographie ».
_ Cryptographie Théorie et Pratique de Douglas Stinson, Thomson Publishing.
_ Cryptographie Appliquée de Bruce Schneier, Thomson Publishing.
Et sur Internet : Site du PGP et site de Machiavel.