SYSTEMES ASYMETRIQUES

LCL FILIOL Eric

ESAT/DEASR/SSI
Laboratoire de virologie et de cryptologie

et

INRIA projet Codes - France

PLAN

- Introduction
- Fonctions à sens unique.
- Complexité
- R.S.A.
- Fonctions de hachage.
- Conclusion

INTRODUCTION

Cryptologie $\Longrightarrow$ essor récent.

- Depuis 40 ans développement :
  - ☞ des télécommunications, de l'informatique et des échanges internationaux.
- Situation changée :
  - ☞ existence de nouveaux besoins.
  - ☞ existence de nouveaux moyens.
  - ☞ besoin de nouvelles règles du jeu.

INTRODUCTION (2)

Entre 1976 et 200, éclosion d'idées "nouvelles".

- W. Diffie - M.E. Hellman *New Directions in Cryptography*. Transactions on Information Theory, IT-22, Nov. 1976.

- R. Rivest - A. Shamir - L. Adleman *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*. Coomunications of the ACM, Vol. 21, 2, 1978.

Fonctions à sens unique

Soit une fonction $f : A \longrightarrow B$.

- Connaissant $x \in A$, il est facile de calculer l'image $f(x)$.
- Connaissant $f(x)$, il est difficile de trouver x.

f est dite AVEC TRAPPE, si de plus :

- Connaissant $f(x)$ et une information supplémentaire (CLEF de la TRAPPE), il est alors facile de retrouver x.

Fonctions à sens unique : exemples

- Boite à lettres.
- Urne.
- Tirelire
- Tronc d'église.
- Souricière.

Fonctions à sens unique : candidats

- R.S.A. (factorisation/primalité)
- Logarithme discret.
- Knapsack (pb du sac à dos)
- Equations quadratiques, cubiques.
- Théorie des graphes, des codes,....

- Plus de 130 systèmes ont été proposés.

Complexité d'algorithme

- C'est le nombre d'opérations élémentaires exigées par l'algorithme pour résoudre une instance de problème de taille n
  - ☞ Notion de complexité en PIRE CAS.
  - ☞ Notion de complexité en MOYENNE.
- Cette complexité est une fonction de la taille n.
- On ne s'intéresse qu'au comportement ASYMPTOTIQUE de cette fonction.

Un millier / Un million / Un milliard	2^{10} / 2^{20} / 2^{30}
Nombre de secondes dans un jour / dans une année	$2^{16,4}$ / 2^{25}
Nombre d'humains sur Terre	$2^{32,5}$
Âge de la Terre en années / en secondes	2^{32} / 2^{57}
Âge de l'univers en années / en secondes	2^{34} / 2^{59}
Nombre d'atomes dans la Terre	2^{170}
Nombre d'atomes dans le Soleil	2^{190}
Nombre d'atomes dans la galaxie	2^{233}
Nombre d'atomes dans l'univers	2^{265}

LE R.S.A.

- p et q deux nombres premiers très grands et $n = p.q$
- $\phi(n) = (p-1)(q-1)$
- e tel que gcd$(e, \phi(n)) = 1$
- calcul de $d = e^{-1}$ mod $\phi(n)$

Annuaire

- (n, e) clef publique.
- (p, q, d) clef secrète.

CHIFFREMENT R.S.A.

Chiffrement

- message $m \rightarrow \underbrace{m^e}_{c}$ mod n
- **On chiffre avec la clef PUBLIQUE !!!**

Déchiffrement

- $c^d = (m^e)^d = m^{e.d} = m^1 = m$ (Calculs faits mod n)

Paramètres :

$p = 11, q = 13, n = 143.$

$\phi(n) = 10 \times 12 = 120.$

$e = 7$, alors $d = 103$ car $7 * 103 = 1 + 6 \times 120$

Chiffrement :

$x = 4$, alors $c = 4^7 \mod 143 = 82$ car $4^7 = 16384 = 82 + 114 \times 143$

et on vérifie alors que $82^{103} = 4 \mod 143$

SIGNATURE R.S.A.

Signature

- Message m émis par A.
- $S_A(m) = m^{d_A}$ mod n_A
- **On signe avec la clef SECRETE !!!**

Vérification

- Calcul de $v = (S_A(m))^{e_A}$ mod n_A
- Si $v = m$ on accepte la signature.
- Sinon on la refuse.

Echange public de clef secrète (Diffie - Hellman)

Soit G un groupe cyclique et a un générateur de G.

- A tire x au hasard, calcule et envoit α à B tel que

$$\alpha = a^x$$

- B reçoit α. Il tire y au hasard et calcule β qu'il envoie à A

$$\beta = a^y$$

- A calcule $K = \beta^x$ et B calcule $K' = \alpha^y$.
- $K = K'$.
- PROBLEME : pas d'authentification.

Fonctions de hachage

DEFINITION *Une application* $H : \mathbb{F}^{\infty} \longrightarrow \mathbb{F}^{n}$ *est une fonction de hachage si*

1. *Calculer* $H(x)$ *à partir de* x *est facile.*
2. H *est "sans collision" : connaissant* x *et* $H(x)$*, il est difficile de trouver* $x' \neq x$ *tel que* $H(x') = H(x)$*.*

- H est nécessairement non-injective.
- Intérêt : au lieu de signer x, il suffit de signer $H(x)$ (gain de temps et d'espace).

Les propriétés "sens inverse difficile" sont quantifiables. Les complexités génériques sont :

- pré image : $O(2^h)$
- seconde pré image : $O(2^h)$
- collision : attention $O(2^{h/2})$
  $\Rightarrow$ paradoxe des anniversaires

Un attaquant contre l'une des propriétés sera efficace si sa complexité de succès est significativement inférieure.

Expérience : une urne contient n boules numérotées de 1 à n. On tire au hasard q boules successivement et avec remise. La probabilité dite de collision, notée $\mathrm{Col}(n,q)$, qu'au moins une boule soit apparue au moins deux fois vaut

$$\begin{aligned}\mathrm{Col}(n,q) &= 1-\prod_{i=1}^{q-1}\left(1-\frac{i}{n}\right)\\ &\approx 1-\exp\left(-\frac{q(q-1)}{2n}\right) \text{ si } q \ll n\end{aligned}$$

On montre que $\mathrm{Col}(n,q) \geq 1/2$ dès que $q \geq 1.17\sqrt{n}$.

Exemple pour les anniversaires. La probabilité que, dans un groupe de 23 pesonnes, au moins deux aient la même date anniversaire est supérieure à $1/2$.

On se donne une fonction de hachage H.

- Méthode du préfixe : $M_K(x) = H(K||x)$
  taille de message fixe
- Méthode du suffixe $M_K(x) = H(x||K)$.
  Son niveau de sécurité ne dépend pas de la taille de la clé.
- Enveloppe : $M_K(x) = H(K||x||K)$
- La construction recommandée : $\mathrm{HMAC}_K(x) = H(K||H(K||x))$.
  "Double application" de la méthode du préfixe. Répond au modèle de sécurité le plus fort.

Construction de MAC avec primitives blocs

Les primitives blocs ont été inventées initialement pour créer des fonctions de chiffrement. Conséquemment, en tant qu'objets mathématiques, elles ont certaines propriétés (notamment statistiques, et de "ressemblance" avec des fonctions aléatoires) qui permet de créer des modes de fonctionnement spécialement dédié à l'intégrité.

On se donne une primitive bloc E_K, n taille du bloc.

Le principe est d'utiliser des modes chaînés.

La base : CBCMAC (taille de message fixe)

Entrées : message $x = (x[1], \ldots, x[n])$, clé K :

$$\begin{aligned} y[1] &= E_K(x[1]) \\ y[2] &= E_K(x[2] \oplus y[1]) \\ &\ldots \\ y[n] &= E_K(x[n] \oplus y[n-1]) \end{aligned}$$

Alors $y[n] = \mathrm{CBCMAC}_K(x)$

Remarque Ce mécanisme s'appelle CBCMAC en raison du chaînage analogue à celui du chiffrement CBC. On observera que les équations correspondent à ce que l'on écrirait pour les chiffrement CBC de la trame $x[1], \ldots, x[n]$ avec $IV = 0^n$. Cela dit, cette ressemblance mathématique n'est pas cryptographique : le mécanisme décrit ci-dessus n'assure pas la confidentialité, puisque $(x[1], \ldots, x[n])$ est transmis.

Conclusion : Critique de la cryptologie à clef publique

- Repose sur la théorie de la complexité
  - ☞ Repose sur la conviction (non prouvée) que $P \neq NP$.
- Systèmes reposant sur des propriètés mathématiques.
  - ☞ La présence de structures est en général signe de faiblesse.
- Ne résout que partiellement le problème de la gestion des clefs (annuaire, ADK,...)
- Systèmes très lents par rapports aux systèmes symétriques.
  - ☞ Le chiffrement RSA est 1000 fois plus lent que le chiffrement DES.