Réunion du Groupe RéSIST

Cryptographie à clé publique de la théorie à l'utilisation

François Arnault

Université de Limoges, LACO, UMR CNRS 6090

25 mars 2002

Une chaîne de risques

- Problèmes mathématiques fondamentaux
- Formalisation de la sécurité
- La théorie sous jacente
- Les contraintes d'implémentation
- La normalisation
- Les risques indirects
- Evolution de l'état de l'art
- L'utilisation finale

Chiffrement à clé publique

RSA

- Clé privée : $\boldsymbol{p}$, $\boldsymbol{q}$, $\boldsymbol{d}$
- Clé publique : $\boldsymbol{N}= pq$, $\boldsymbol{E}= d^{-1} \bmod (p-1)(q-1)$

$$c = m^E \bmod N, \qquad m = c^d \bmod N.$$

El Gamal

- Clé privée : $\boldsymbol{b}$
- Clé publique : $\boldsymbol{p}$, $\boldsymbol{g}$ d'ordre $p-1$ modulo p, $\boldsymbol{B}= g^b \bmod p$

$$K = g^k \bmod p, \qquad c = mB^k \bmod p, \qquad m = cK^{-b} \bmod p.$$

- Problème du logarithme discret (modulo p) :

Etant donné $A \in [1 \,..\, p-1]$, trouver $a \in [1 \,..\, p-1]$ tel que

$$A = g^a \bmod p.$$

Factorisation et logarithme discret

- La sécurité repose sur des problèmes mathématiques
  — Factorisation (RSA), Logarithme Discret (El Gamal, DSS)
- Progrès en factorisation
  — RSA-155 (août 99), RSA-158 (janvier 02)
- Progrès dans le logarithme discret
  — DLog GF(2^{607}) (février 02)

RSA 155 (512 bits)

```
Factorization of a 512-bits RSA key using the Number Field Sieve
----------------------------------------------------------------
On August 22, 1999, we found that the 512-bits number

RSA-155 =
1094173864157052742180970732204035761200373294544920599091384213147634\
9984288934784717997257891267332497625752899781833797076537244027146743\
531593354333897

can be written as the product of two 78-digit primes:

102639592829741105772054196573991675900716567808038066803341933521790711307779
*
106603488380168454820927220360012878679207958575989291522270608237193062808643

The number RSA-155 is taken from the RSA Challenge list
(see http://www.rsa.com/rsalabs/html/factoring.html).
```

Logarithme dans $GF(2^{607})$

```
From: Emmanuel Thomé <thome@lix.polytechnique.fr>

Let K be the splitting field over GF(2) of the irreducible polynomial
f(X)=X^607+X^9+X^7+X^6+X^3+X+1

Let P(X) be the polynomial over GF(2) with the following binary
representation (LSB first):
0000000: 54 65 73 20 79 65 75 78 20 73 6f 6e 74 20 73 69
0000010: 20 70 72 6f 66 6f 6e 64 73 20 71 75 27 65 6e 20
0000020: 6d 27 79 20 70 65 6e 63 68 61 6e 74 20 70 6f 75
0000030: 72 20 62 6f 69 72 65 0a 4a 27 61 69 20 76 75 20
0000040: 74 6f 75 73 20 6c 65 73 20 73 6f 6c 65 69 6c 73
0000050: 20 79 20 76 65 6e 69 72 20 73 65 20 6d 69 72 65
0000060: 72 0a

We can verify that P(X) is congruent to X^l mod f(X), where:
l:=4789114616619466967536724879749551759470781009498974017377062140439743\
0543970903739336135936970649474601608959493147659399495433873340533222590\
124498269177310650885248209789392038650635;
```

Différents objectifs de sécurité

- Sécurité de la clé privée

  — repose sur la factorisation ou le logarithme discret.

- Sécurité de la fonction à sens unique

  — repose sur le problème RSA ou sur le problème Diffie-Hellman.

- Sécurité sémantique

  — vraie protection de l'information.

Sécurité sémantique (I)

- Etant donnés :
  - — deux clairs m_0 et m_1,
  - — et le chiffré correspondant à l'un d'eux $c = \mathrm{ENC}(m_b)$,
  - — un attaquant ne peut déterminer b.
- La donnée de c et des paramètres publics
  - — ne permet de calculer **aucune** information sur le clair.

Différents problèmes mathématiques

- Problème RSA : Trouver m tel que

$$m^e \equiv c \text{ modulo } N.$$

- Problème Diffie-Hellman : Calculer

$$C = g^{ab} \bmod p$$

à partir de

$$A = g^a \bmod p \text{ et } B = g^b \bmod p.$$

- Equivalence entre RSA et la factorisation non prouvée
  — et peut-être fausse (Boneh, Venkatesan).
- Equivalence entre DL et DH non prouvée
  — mais probablement vraie (Maurer).

- Rabin repose sur la factorisation.

Sécurité Sémantique (II)

- Pour El Gamal, repose sur un problème décisionnel :

Problème Décisionnel de Diffie-Hellman (DDH) :

A partir de

$$A = g^a \bmod p, B = g^b \bmod p \text{ et } C = g^c \bmod p,$$

déterminer si $c \equiv ab$ modulo $p - 1$.

Alternative

- Sécurité sémantique sous des hypothèses plus rassurantes
  — Blum-Goldwasser (résidualité quadratique).

Sécurité sémantique (III)

OAEP (PKCS#1, v2)

- Padding pour sur RSA (ou Rabin), sûr dans le modèle de l'oracle d'aléa.
  - — Module N de longueur n,
  - — k_0 bits d'aléa r,
  - — k_1 bits de redondance,
  - — $n - k_0 - k_1$ bits pour le message m :

$$c = \mathrm{RSA}_k\Big((m \,\|\, 0^{k_1}) \oplus g(r) \;\Big\|\; r \oplus h\big((m \,\|\, 0^{k_1}) \oplus g(r)\big)\Big)$$

où $g : \{0,1\}^{k_0} \to \{0,1\}^{n-k_0}$ et $h : \{0,1\}^{n-k_0} \to \{0,1\}^{k_0}$.

Courbes elliptiques

Logarithme discret (sur E, engendrée par G)

Etant donné $A \in E$, trouver $a \in [1 \,..\, \#E]$ tel que

$$A = aG.$$

Diffie-Hellman (sur E, engendrée par G)

Calculer

$$C = abG$$

à partir de

$$A = aG \text{ et } B = bG.$$

Pas d'attaque sous-exponentielle pour le moment.

- Calculs plus rapides, clés plus courtes.
- Et si ?

Petits exposants (RSA)

Petit exposant secret

[BD] D. Boneh, G. Durfee
Cryptanalysis of RSA with private key d less than $n^{0.292}$
IEEE Transactions on Information Theory 46 (2000), no. 4, 1339-1349

[Wiener] M.J. Wiener
Cryptanalysis of short RSA secret exponents
IEEE Transactions on Information Theory 36 (1990), no. 3, 443-551

Petit exposant public

• Attaque de Håstad :

envoi de messages semblables à plusieurs destinataires.

• Attaque de Franklin/Reiter :

envoi de messages semblables à un seul destinataire.

Normes (PKCS#1, v1)

Le message utile m est formatté avant chiffrement :

$$M = 00 \parallel 02 \parallel \text{aléa} \parallel 00 \parallel m.$$

- Rendre les messages indistinguables (sécurité sémantique)
- Contrer les attaques à messages choisis
- Rendre le chiffrement non malléable
- Se prémunir d'autres attaques (Håstadt, ...)

Normes (PKCS#1, v1)

Attaque de Bleichenbacher

— Attaque à messages choisis.

— Lors du déchiffrement, un message d'erreur est généré lorsque le message clair ne vérifie pas le format imposé.

— C'est l'information apportée par ce message d'erreur (et non le message clair) qui suffit pour mener l'attaque.

Attaque de Coron/Joye/Naccache/Pailler

— Attaques à messages clairs, restreintes à certains types de messages.

Normes (ISO/IEC-9796)

Redondance pour signatures RSA

- Attaque de De Jonge/Chaum
- Attaque de Coron/Naccache/Stern
- Attaque de Grieu (à messages choisis)
- Attaques de Girault/Misarsky
- Attaque de Coppersmith/Halevi/Jutla

Implémentation

Risques cryptographiques parallèles

• Générateurs aléatoires.

La qualité de l'aléa est primordiale. Bug de SSH [B. Perrot].

• Canaux cachés.

Difficiles à détecter.

Risques non cryptographiques

• Attaques physiques :

Attaques sur la consommation de courant, sur le temps de calcul, par dysfonctionnement provoqué, par exploration matérielle.

• Buffers overflows et bugs divers.

Evolution de la taille des clés

Prévoir

• La loi de Moore.

La vitesse des processeurs double tous les m mois (eg. $m = 18$), à prix constant.

• Les progrès algorithmiques.

— Le coût d'une attaque à clé publique (factorisation, logarithme discret) est réduit de moitié tous les c mois (eg. $c = 18$). Relativement régulier pour ces problèmes classiques, avec sauts sporadiques. Actualité : Bernstein.

— Au contraire, pas de croissance (?) pour les courbes elliptiques. Idem pour le logarithme discret dans un sous-groupe (DSS).

• L'accroissement des moyens financiers.

Le budget d'un attaquant double toutes les b années (eg. $b = 10$).

Evolution de la taille des clés (II)

Année :	1982	1992	2002	2012	2022	2032
Taille en bits :						
Symétrique	56	64	72	80	87	95
RSA / Log. discret	417	682	1028	1464	1995	2629
DSS (q)	102	114	127	141	154	168
C. elliptiques			135	149	164	179

- Source : A.K. Lenstra & E.R. Verheul
  Selecting Cryptographic Key Sizes
  J. of Cryptology 14 (2001), 255–293

Risques divers

- Négligence
- Obsolescence
- Mauvaise analyse de l'environnement

  — Carte bancaire.

Le dernier problème

L'utilisateur final !

- C'est lui qui crée (?) et manipule les clés secrètes (et les mots de passe associés).

  — Maladresse,

  — Manque de sensibilisation,

  — Manque de vigilance,

  — Manque de formation.

Conclusion

- Des problèmes mathématiques très étudiés
- Des notions de sécurité fortes
- Des solutions théoriques variées et nuancées
- La théorie essaie de rattraper la pratique
- Nécessité de finalisation minutieuse des produits
- Importance d'une analyse de risques précise
- La formation des différents acteurs
  - concepteurs, developpeurs, utilisateurs...

Bibliographie (I)

[Bernstein] D. Bernstein
http://cr.yp.to/papers/nfscircuit.ps

[Bleich] D. Bleichenbacher
A chosen ciphertext attack against protocols based on the RSA encryption standard PKCS #1
LNCS 1462 (Crypto'98), Springer, 1--12

[BD] D. Boneh, G. Durfee
Cryptanalysis of RSA with private key d less than n^{0.292}
IEEE Transactions on Information Theory 46 (2000), no. 4, 1339--1349

[BV] D. Boneh, R. Venkatesan
Breaking RSA may not be equivalent to factoring
LNCS 1403 (Eurocrypt'98), Springer, 59--71

[FR] M.K. Franklin, M. Reiter
A linear protocol failure for RSA with exponent three
"Rump session", Crypto'95

Bibliographie (II)

[Hastad] J. Hastad
On using RSA with low exponent in a public key network
LNCS 218 (Crypto'85) , Springer, 403--408

[LV] A.K. Lenstra, E.R. Verheul
Selecting Cryptographic Key Sizes
J. of Cryptology 14 (2001), 255--293

[Maurer] U.M. Maurer
Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms
LNCS 839 (Crypto'94), Springer, 271--281

[Wiener] M.J. Wiener
Cryptanalysis of short RSA secret exponents
IEEE Transactions on Information Theory 36 (1990), no. 3, 443--551

[teRiele] H. te Riele
ftp://ftp.cwi.nl/pub/herman/GNFSrecords/GNFS-512