Semaine 13 : Sécurité

1 Principes de base

a) Contre laquelle des menaces de la colonne de gauche est dirigé chacun des types de défenses de la colonne de droite ?

- Destruction d'informations
- Démenti d'action
- Manipulation d'informations
- Usurpation d'identité
- Vol d'informations

- Authentification
- Responsabilité
- Disponibilité
- Confidentialité
- Intégrité

b) Les crypto-systèmes symétriques à clés secrètes et les crypto-systèmes asymétriques à clés publiques offrent tous des mécanismes de défense contre deux types de menaces : lesquels ?

c) Les crypto-systèmes asymétriques à clés publiques offrent en plus un mécanisme de défense contre un troisième type de menace : lequel ?

2 Cryptographie asymétrique

Cocher les affirmations correctes concernant la cryptographie à clés publiques :

- [ ] Chaque participant dispose de deux clés, l'une secrète et l'autre publique et utilise sa clé secrète pour chiffrer les messages confidentiels.
- [ ] La cryptographie à clés publiques permet de chiffrer des données, mais pas de leur appliquer des signatures numériques.
- [ ] La cryptographie à clés publiques est plus performante que la cryptographie à clés symétriques.
- [ ] Des messages chiffrés avec une clé publique ne peuvent être déchiffrés que si l'on connaît la clé secrète correspondante. Retrouver cette clé secrète à partir de la clé publique est un problème pratiquement incalculable.
- [ ] Des messages chiffrés avec une clé secrète peuvent être déchiffrés avec n'importe quelle clé publique.
- [ ] Chaque participant dispose de deux clés, l'une secrète et l'autre publique et utilise sa clé secrète pour déchiffrer les messages confidentiels.

3 One-Time Pad

On considère ici un système « One-Time Pad » utilisant pour clé `1001001001100101`.

a) Avec ce système, coder le message `0100110001110011`.

b) Avec ce système, décoder le message `0100110001110011`.

4 RSA – Confidentialité

Un assistant envoie votre note au professeur concerné par mail encrypté en RSA. La clé publique du professeur est $(7, 55)$ et le message envoyé (c.-à-d. encrypté) est 25.

Quelle est votre note ?

5 RSA – Responsabilité

Pour assurer l'authenticité des messages contenant les notes, le professeur demande à l'assistant de signer ses messages (toujours en utilisant le système RSA et toujours de façon confidentielle). Sachant que la clé publique de l'assistant est à présent $(3, 15)$ et celle du professeur $(7, 77)$,

a– Quel message envoie l'assistant pour la note 4 ?

b– Quelle note correspond au message transmis 41 ?

c– Un message signé 27 a-t-il bien été envoyé par l'assistant ?

Pour aller plus loin

6 Synthèse

Cet exercice nécessite une bonne calculatrice ou d'écrire/d'utiliser de petits programmes en C++.

On souhaite envoyer de façon efficace, confidentielle et garantie (signée et intègre) le message suivant :

VIVE ICC !

a) Pour chacun de ces adjectifs (efficace, confidentielle, signée, intègre), quelle technique peut-on utiliser ?

b) Commencez par comprimer ce message à l'aide d'un code de Huffman, en prenant ici en compte les espaces.

Quel est le message comprimé ?

Pour fixer la suite de façon unique, on classera par ordre alphabétique les lettres de même nombre d'apparitions en considérant l'espace au début de l'alphabet et le point d'exclamation à la fin. Puis on affectera des codes commençant par `0` (donc tous les codes de même longueur seront en fait classés par ordre croissant en binaire lorsque l'on lit de tableau des lettres à coder (ordonné comme indiqué ci-dessus)).

c) On utilise pour la suite un système RSA. On choisit $p = 97$, $q = 137$ et $d = 55$.

Quelle est notre clé publique ?

d) Notre destinataire à pour clé publique : $(1929, 3337)$

— En tranches de combien de bits découpe-t-on notre message comprimé (obtenu à question b)) ?
— Encryptez le message.

Note : par convention, on remplit la fin du message de départ avec des espaces (ce qui devrait correspondre à le remplir avec des `0`).

e) On souhaite de plus signer notre message.

Qu'envoie-t-on ? [1]

f) Enfin, on veut se prémunir contre toute manipulation (intégrité). Doit-on faire quelque chose de plus ? (si oui : quoi ?)

7 DES

On utilise ici le système de cryptage DES avec $n = 4$, $d = 3$ et f donnée par :

$$f(x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3, y_4) = \begin{pmatrix} x_1\, y_1 \oplus x_2\, y_2 \oplus x_4\, y_4 \oplus x_5 \\ x_1\, y_4 \oplus x_3\, y_2 \oplus x_5\, y_1 \oplus x_2 \oplus y_3 \oplus x_4 \\ (x_1 \oplus x_3 \oplus x_5 \oplus y_2) \cdot y_1 \\ (x_2 \oplus x_4 \oplus y_4) \cdot y_3 \end{pmatrix}$$

toutes les opérations s'effectuant bien entendu en binaire (sans retenue pour le $\oplus$).

Les clés ont donc $(d-1) \cdot 5 = 10$ bits. Nous choisirons la clé $K = K_1\, K_2 = \texttt{0110110110}$.

a) Avec ce système, coder le message `0100110001110011`.

b) Avec ce système, décoder le message `0100110001110011`.

8 PGP

Cet exercice nécessite une bonne calculatrice ou d'écrire un petit programme.

PGP est un système de cryptographie hybride combinant un algorithme à clé publique (RSA) et un algorithme à clé secrète (IDEA en l'occurrence). En ce qui concerne l'utilisateur cependant, PGP se comporte comme un crypto-système à clé publique.

1. en tout cas au début. Il ne sera pas possible de finir la signature, mais expliquez le début.

Son principe est le suivant : une clé secrète est générée puis est utilisée pour coder le message. Cette clé secrète est elle-même codée en utilisant RSA. Le message envoyé est la concaténation de la clé secrète codée et du message codé.

Supposons ici que le système à clé secrète utilisé soit un One-Time Pad décimal (c.-à-d. pour chaque chiffre une addition modulo 10 de la clé) agissant sur des blocs de 6 chiffres d'une suite de chiffres. Un texte est lui-même transformé en suite de chiffres par la convention '_' =00, 'A'=01, 'B'=02, ...

Exemple : Texte=« UN TEST » → '21140020051920' et si la clé secrète est « 123456 », cela donne comme message codé '211400 200519 20' + '123456 123456 12' = '33485632396532'.

Sachant que votre clé publique RSA est $(21, 172'831)$ et votre clé privée est $16'381$, décoder le message
`58423`
`172377142371193650132152144058354857182771143462133277 23`
où par convention le cryptage RSA de la clé secrète est sur la première ligne.