Université du Luxembourg 2004–2005

C.U.T. Informatique 3ème année mardi 14 décembre

Cryptographie
Examen

Jean-Sébastien Coron, Sébastien Varrette

Durée: 2 heures 30

Calculatrice interdite

Il sera tenu compte dans la notation de la clarté des explications et du soin apporté à la rédaction (propreté, organisation, respect de la langue française).

1 Généralités

1) Quelle différence y a t-il entre la cryptographie et la stéganographie ? Rappeler l'objectif général de la cryptographie et les quatre fonctionnalités offertes par la cryptographie, résumées dans le sigle "CAIN".
2) Rappeler le schéma général d'un système cryptographique à clé secrète et expliquer son fonctionnement. Quelle analogie est-il possible de faire entre ces systèmes et un objet courant ? Citer deux exemples de systèmes cryptographiques à clé secrète. Quelle différence y a t-il en cryptologie à clé secrète entre permutation et substitution ?
3) De même, rappeler le schéma général d'un système cryptographique à clé publique et expliquer son fonctionnement. Quelle différence y a t il avec les systèmes à clé secrète ? Quelle analogie est-il possible de faire entre un système à clé publique et un objet courant ? Citer un exemple de système cryptographique à clé publique.

2 Chiffrement affine

On définit la méthode de chiffrement suivante : à chaque lettre de l'alphabet on associe un entier entre 0 et 25. La lettre 'a' correspond à l'entier 0, la lettre 'b' correspond à l'entier 1, et ainsi de suite. Etant donnée une lettre correspondant à l'entier x, le chiffrement de x est la lettre correspondant à l'entier y tel que :

$$y = a \cdot x + b \mod 26$$

où les entiers a et b forment la clef de chiffrement (a, b). On doit avoir $0 \leq a < 26$, $0 \leq b < 26$ et $\text{PGCD}(a, 26) = 1$.
Par exemple, si on prend $a = 5$ et $b = 6$, le chiffrement de la lettre 'j' (correspondant à l'entier 9) est :

$$y = 5 \cdot 9 + 6 = 51 = 25 \mod 26$$

ce qui donne la lettre 'z'.
Ensuite, pour chiffrer un mot, on chiffre chaque lettre séparemment.

1) En prenant la clef de chiffrement $(7, 10)$ (soit $a = 7$ et $b = 10$), donner le chiffrement du mot 'bonjour'.

2) Quelles sont les valeurs de a qui sont possibles ?

3) Combien y a-t-il de clef possibles pour cette méthode de chiffrement ?

Etant donné un entier a et un entier n tels que PGCD(a, n), l'inverse de a modulo n est l'unique entier, noté a^{-1}, tel que $a \cdot a^{-1} = 1 \mod n$.

4) Soit un entier y, tel que y est le chiffrement de l'entier x, pour une clef (a, b). Montrer que l'on peut retrouver x à l'aide de la formule suivante :

$$x = a' \cdot y + b' \mod 26$$

pour des entiers a' et b' que l'on précisera, en fonction de a^{-1} et b. On appelera le couple d'entier (a', b') la clef de déchiffrement.

5) Donner la clef de déchiffrement correspondant à la clef de chiffrement $(7, 10)$.

On suppose qu'Alice veut transmettre à Bob le résultat d'un vote, en utilisant la méthode de chiffrement précédente. Le résultat du vote peut-être soit 'oui', soit 'non'. Alice et Bob s'entendent au préalable sur une clef de chiffrement (a, b), qu'ils sont les seuls à connaître. Si le résultat du vote est 'oui', Alice chiffre le mot 'oui' ; si le résultat du vote est 'non', Alice chiffre le mot 'non'. Ensuite, Alice envoie le chiffré à Bob. Bob, connaissant la clef de chiffrement, peut retrouver la clef de déchiffrement et déchiffrer le message pour obtenir le résultat du vote.

6) Expliquer comment un attaquant, nommé Eve, ne connaissant pas la clef du chiffrement, peut cependant retrouver le résultat du vote en observant la communication entre Alice et Bob.

3 Chiffrement de Vernam

1) Rappeler la table de vérité de l'opération XOR (aussi notée $\oplus$)

$\oplus$	0	1
0		
1		

Utiliser cette table de vérité pour calculer l'opération suivante :

$$\begin{array}{cc} & 1000011 \\ \oplus & 1101000 \\ \hline \end{array}$$

2) Rappeler le fonctionnement du chiffrement de Vernam (également appelé "One Time Pad"). A quelle(s) condition(s), en particulier sur le nombre d'utilisations de la clef, ce chiffrement est-il inconditionnellement sûr ?

3) Application : On utilise le code ASCII pour traduire en binaire le texte suivant : M="`RDV 14h`". On obtient la suite binaire :

```
M = 01010010 01000100 01010110 00100000 00110001 00110100 01101000
```

Donner la suite binaire résultant du chiffrement de Vernam du texte `RDV 14h` (converti en ASCII) avec la clef

```
K = 01100010 01101111 01101110 01101010 01101111 01110101 01110010
```

4 RSA

On désire utiliser l'algorithme RSA avec le module $n = 3 \cdot 11 = 33$, et l'exposant de chiffrement $e = 3$. Le chiffré c d'un message m est donc :

$$c = m^3 \mod 33$$

1) Quel est le chiffré du message $m = 7$?

2) Quelle est la valeur de l'exposant de déchiffrement d tel que pour tout m, si $c = m^3 \mod 33$, alors :

$$m = c^d \mod 33$$

5 Signature RSA

On désire utiliser l'algorithme RSA dans le cadre de la signature éléctronique d'un document M.
1) Rappeler le principe général de la signature RSA.
2) En pratique, on ne signe pas le message M directement mais plutôt un résumé "unique" de ce message obtenu à l'aide d'une fonction de hachage h : on ne signe donc pas M mais plutôt $h(M)$. Expliquer pourquoi.
3) On suppose maintenant que Alice souhaite signer par RSA un document M avec les mêmes paramètres de clef que pour l'exercice précédent. On suppose donc utiliser la clef publique (n, e)=(33,3) et la clef privée $(d, 3, 11)$ (où la valeur de d a été calculée dans l'exercice précédent) Elle utilise pour cela une fonction de hachage h et obtient $h(M) = 2$. Quelle est la valeur S de la signature éléctronique obtenue à partir de $h(M)$?
4) Bob recoit le document M' avec la signature S calculée précédemment. En effectuant le hachage de ce document par la fonction h. Il obtient $h(M') = 3$. Comment est-il sûr d'avoir reçu un document falsifié ?

6 DES

1) On rappelle que DES est une algorithme à clef secrète fonctionnant par blocs. Quelle est la taille d'un bloc à chiffrer par DES ? Même question sur la taille d'un bloc chiffré.
2) On dit que la taille des clefs dans DES est de 64 bits mais de 56 bits effectifs. Expliquer la nuance.
3) On rappelle dans la figure 1 le shéma général d'une ronde de DES. Rappeler la taille des élements L_i, R_i et de la sous-clef K_i
4) On fournit maintenant le contenu de la boite-S S_1.

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

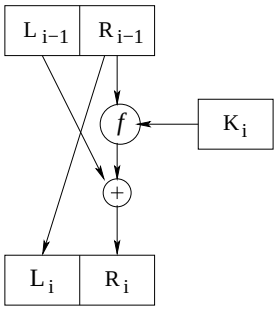

FIGURE 1 – Un tour de DES

On rappelle qu'il existe en fait 8 boîtes-S qui sont exploitées dans la fonction f mentionnée dans la figure 1. Chacune de ces boîtes-S prend en entrée une valeur B_i sur 6 bits et renvoit en sortie un nombre C_i sur 4 bits (i est le numéro de la boite-S).
On demande de calculer pour chaque valeur de B_1 listée dans le tableau suivant les valeurs C_1 correspondantes :

B_1	C_1
$24 =$ `011000`	
$45 =$ `101101`	
$7 =$ `000111`	
$54 =$ `110110`	

5) Pourquoi a-t-il fallu redéfinir un nouveau standard de chiffrement (AES) ?

7 Protocole d'échange de clefs de Diffie-Hellman

Décrire le protocole d'echange de clef de Diffie-Hellman. Quel problème mathématique garantit le secret de la clef échangée.

8 Architectures PKI

1) Rappeler la signification du sigle "PKI". Quel est l'intérêt des certificats numériques ? Décrire les éléments essentiels d'un certificat numérique : que comporte-t-il et pourquoi ?
2) Rappeler les principales fonctions d'une PKI.
3) Décrire brièvement les principaux acteurs d'une PKI.