Correction de l'examen : Int. cryptographie

Expliquez les termes suivants : /4pts

1- Monoalphabétique cipher : Une lettre est tjs chiffré par une même lettre dans le texte chiffré. (0,5 pts)

2- polyalphabétique cipher : Une lettre peut être chiffré par des lettres différentes ds le texte chiffré (0,5 pts)

3- symmetric cipher : La clé de déchiffrement Kd peut être déduite de la clé de chiffrement Ke. (0,5 pts)

4- Asymmetric cipher : Chaque personne possède 2 clés (Kpriv, Kpub) avec Kpriv ≠ Kpub
Kpub : clé de chiffrement
Kpriv : clé de déchiffrement. (0,5 pts)

5- one way function : $f : E \to F$ (fonction à sens unique)
par $x \in E$, il est facile de calculer $y = f(x)$.
mais, pour $y \in F$, il est très difficile de calculer $x = f^{-1}(y)$. (0,5 pts)

6- One-way function avec trappe : c'est une fonction avec information supplémentaire (trappe) pour calculer l'inverse. (0,5 pts)

Protocole Diffie-Hellman (Echange d'une clé commune) (2 pts)

Soit $G = \langle g \rangle$ un groupe cyclique avec $|G| = n$.
- Alice choisie une clé secrète a et calcule $A = g^a$ et envoi le résultat à Bob.
- Bob choisi une clé secrète b et calcule $B = g^b$ et envoi le résultat à Alice
- Alice calcule $(g^b)^a = g^{ab}$
- Bob calcule $(g^a)^b = g^{ab}$
- Alice et Bob ont la même clé $\boxed{g^{ab}}$

/1

Exercice 1 (4pts)

a/ Si $f : E \to F$ est une fonction de chiffrement (0,5pt)
et on a $x_1 \neq x_2$ $(x_1, x_2 \in E)$ avec $f(x_1) = f(x_2) = y$
On sait pas parquoi déchiffrer y par x_1
ou bien par x_2. Donc, il faut que f doit être injective.

b/ Un cryptosystème est un cinq-uplet $(P, C, K, \mathcal{E}, \mathcal{D})$
avec Ds notre cas :
. $P = C = \mathbb{Z}_{26}$ (2pts)
. $K = \mathbb{Z}_{26} \times \mathbb{Z}_{26} = \{(k_1, k_2) \mid 0 \leq k_1 \leq 25, 0 \leq k_2 \leq 25\}$

Pour la chaîne $W = w_0 w_1 w_2 \cdots w_i \cdots w_{n-1}$

On a $e_{(k_1,k_2)}(w_i) = \begin{cases} (w_i + k_1) \bmod 26 & \text{si } i \text{ est impaire} \\ (w_i + k_2) \bmod 26 & \text{si } i \text{ est paire} \end{cases}$
(position)

on aura $e(W) = e(w_0) e(w_1) e(w_2) \cdots e(w_i) \cdots e(w_{n-1})$

$= (w_0 + k_2)[26] \; (w_1 + k_1)[26] \cdots = c_0 c_1 c_2 \cdots c_{n-1}$

De même
$d(c_0 c_1 c_2 \cdots c_{n-1}) = (c_0 - k_2)[26] \; (c_1 - k_1)[26]$

* pour la clé $(K_1, K_2) = (2, 2)$ (1,5 pt)
On chiffre la chaine : Algebraforever

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Algebraforever $\hookrightarrow$ 0 | 11 | 6 | 4 | 1 | 17 | 0 | 5 | 14 | 17 | 4 | 21 | 4 | 17
position 0 1 2 3 4 5 6 7 8 9 10 11 12 13

/2

$= 2,2,2,\ldots,2$

$= 2|11|8|6|3|19|2|7|16|19|6|23|6|19$

CNIGDTCHQTGXGT

- L'espace des clés (0,5 pt)

$$\mathcal{K} = \{(K_1, K_2) \mid 0 \leq K_1 \leq 25,\ 0 \leq K_2 \leq 25\}$$

$$\Rightarrow |\mathcal{K}| = 26 \times 26 = 26^2.$$

Exercice 2 (4 pts)

Par le chiffre de Vigenère

"This is a secret" $\longleftrightarrow$ 19|7|8|18|8|18|0|18|4|2|17|4|19

\+ 2 5 4 7 2 5 4 7 2 5 4 7 2

19|12|12|25|10|23|4|25|6|7|21|11|4 (mod 26)

(1 pt) = **TMMZKXEZGHVLV**

Le chiffre est polyalphabétique

la même lettre "s" du plaintext et chiffre' différement : une fois par Z une fois par X une fois par Z ---

(0,25)

/3

Suppose we intercepted ciphertext where the most common letters are Z and I.

The most frequent letters in English are E and T

So we try $E \xrightarrow{E_{a,b}} Z$ $\quad T \xrightarrow{E_{a,b}} I$

$4 \longmapsto 25$ $\quad 19 \longmapsto 8$

Therefore $D_{a,b}(x) = cx + b \ [26]$

$$\begin{cases} D_{a,b}(25) = 4 \\ D_{a,b}(8) = 19 \end{cases} \Leftrightarrow \begin{cases} 25c + d \equiv 4 \ [26] \\ 8c + d \equiv 19 \ [26] \end{cases}$$

$\Leftrightarrow$ $17c \equiv -15 \equiv 11 \ [26]$

Since $17^{-1} \equiv 23 \ [26]$

We obtain $c \equiv 11 \cdot 23 \equiv 19 \ [26]$

$d \equiv 4 - 25 \cdot 19 \equiv 3 \ [26]$

Hence $D_{a,b}(y) = (19y + 3) \ [26]$

$\Rightarrow$ $E \leftrightarrow Z$ and $T \leftrightarrow I$

Using $(19, 23)$ as decryption key we obtain:

18 | 15 | 00 | 02 | 04 |

S P A C E $\longmapsto$ X Q H D Z

Exercice 3

a/ Fermat-Little theorem

Si p est un nbre premier et a est un entier non divisible par p alors on a $a^{p-1} \equiv 1 [p]$.

Exemple: Montrer que $8^{50} - 1$ est divisible par 11.

On a 11 est un nbre premier et 8 n'est pas divisible par 11, donc d'après FLT

$$8^{11-1} \equiv 8^{10} \equiv 1 [11]$$

et par suite $(8^{10})^5 \equiv 1 [11]$

$$\Rightarrow 8^{50} \equiv 1 [11] \Leftrightarrow 8^{50} - 1 \equiv 0 [11]$$

$\Leftrightarrow 8^{50} - 1$ est divisible par 11.

b/ KSA $p = 29$, $q = 31$

$\Rightarrow n = 29 \times 31 = 899$

$\varphi(n) = \varphi(31) \times \varphi(29) = (31-1)(29-1) = 30 \times 28 = 840$

We want to have e, d such that

$ed \equiv 1 [\varphi(n)] \Leftrightarrow ed \equiv 1 [840]$

/5

* pvs $d = 11$ solve $11e \equiv 1 \bmod 840$

Using Euclidean algorithm

$$840 = 76 \times 11 + 4$$

$$11 = 2 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

$$\Rightarrow \quad 1 = 4 - 1 \times 3 = 4 - 1(11 - 2 \cdot 4)$$

$$= 3 \cdot 4 - 11$$

$$= 3(840 - 76 \times 11) - 11$$

$$1 = 3 \cdot 840 - 229 \times 11$$

$$e = -229 + 840 \times 1 = \boxed{611}$$

public key: (899, 611)

private key: (899, 11)

Decrypt: 25 $\quad D(25) = 25^{11} \bmod 899$

$$25^{11} = (25^5)^2 \cdot 25 \bmod 899$$

$$= 687^2 \cdot 25 \bmod 899$$

$$\ldots = \boxed{749 \ [899]}$$

the Original message