Révision générale

Correction de l’examen

de l’année universitaire 2019-2020

Exercice 1.

On cherche à déchiffrer avec le code RSA. On prend p=11, q=19 et e=7.

1) Sur quelle difficulté calculatoire est basé le code RSA ? Expliquer le lien entre cette difficulté et le déchiffrement RSA.

- **RSA** est basé sur la difficulté calculatoire de la factorisation des grands entiers. Etant donné n=pq avec p et q premiers très grands, il est difficile à partir de n de trouver les valeurs de p et q.

- Puisque d est l'inverse de e modulo $\varphi(n)$, donc connaitre d revient à connaitre $\varphi(n) = (p-1)(q-1)$

Receveur

Emetteur

choisit p et q
e premier avec $p-1$ et $q-1$

M

calcule $n = p \times q$
d tel que $ed \equiv 1 \pmod{\varphi(n)}$

envoie (n, e) à Bob $\xrightarrow{(n,e)}$

$\xleftarrow{C}$ calcule $C = M^e \pmod{n}$ et l'envoie à Alice

calcule $C^d \pmod{n}$
et en déduit M

Connaitre p & q → connaitre $\varphi(n)$→ connaitre d → connaitre M

2) Préciser la clé privée et la clé publique.

- Alice choisit deux nombres premiers :
  p = ***11*** et q = ***19*** alors n = pq donne n = ***209***.
  $\varphi(n) = 10*18 = \mathbf{180}$.
  Alice choisit par exemple ***7*** qui est premier avec $\varphi(n) = \mathbf{180}$.

  <u>La clé publique est (7, 209).</u>

- D'après l'algorithme d'Euclide étendu, on trouve $d = e^{-1}[\varphi(n)] = 103$
  (on vérifie que 7 * 103 = 721 a bien pour reste 1 dans la division par 180).

  <u>La clé secrète est 103.</u>

3) Chiffrer le message M=12.

4) Décoder le message chiffré C=123.

3) Bob a reçu la clé publique (7, 209) et doit calculer m^e (*modulo n*) soit 12^7 (*modulo 209*).
Il trouve ***12*** et envoie cette valeur à Alice**.**

4) Alice reçoit ***123.*** Elle utilise sa clé secrète d=103 pour calculer 123^d (*modulo n*) soit 123^{103} (*modulo 209*).
Elle trouve ***63***.

Exercice 2. On cherche à déchiffrer le mot « OQ » à l'aide du chiffrement de Hill (26 caractères), et en utilisant la matrice suivante :

$$A = \begin{pmatrix} 2 & 5 \\ 17 & 1 \end{pmatrix}$$

1) La matrice A est-elle inversible dans Z/26Z ? Si oui trouver son inverse.

Det(A) = -83 [26] = 21 [26]

Pgcd (26,21)=1, donc 21 est inversible dans Z/26Z, et par suite A est inversible dans Z/26Z

$$A^{-1} = \frac{1}{21}\begin{pmatrix} -1 & 5 \\ 17 & -2 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 19 & 10 \end{pmatrix} [26]$$

2) Décoder le groupe de lettres « OQ ».

SI on veut décoder le groupe de lettres OQ : cela correspond au couple $\begin{pmatrix}14\\16\end{pmatrix}$.

$$\begin{pmatrix}5 & 1\\19 & 10\end{pmatrix}\begin{pmatrix}14\\16\end{pmatrix} \equiv \begin{pmatrix}8\\10\end{pmatrix}[26]$$

Le groupe décodé est donc IK.

Exercice 3. 1) Alice et Bob veulent s'échanger une clé K, mais ils ne disposent pas de canal sécurisé pour cela. Expliquer comment cet échange est possible avec le protocole de Diffie et Hellman.

	Alice	Bob
Étape 1 :	Alice et Bob choisissent ensemble un grand nombre premier p et un entier $1 \leq a \leq p-1$. Cet échange n'a pas besoin d'être sécurisé.	
Étape 2 :	Alice choisit secrètement x_1.	Bob choisit secrètement x_2.
Étape 3 :	Alice calcule $y_1 = a^{x_1} \pmod p$.	Bob calcule $y_2 = a^{x_2} \pmod p$.
Étape 4 :	Alice et Bob s'échangent les valeurs de y_1 et y_2. Cet échange n'a pas besoin d'être sécurisé.	
Étape 5 :	Alice calcule $y_2^{x_1} = (a^{x_2})^{x_1} = a^{x_1 x_2} \pmod p$ et appelle ce nombre K, la clé secrète à partager avec Bob.	Bob calcule $y_1^{x_2} = (a^{x_1})^{x_2} = a^{x_1 x_2} \pmod p$ et appelle ce nombre K, la clé secrète à partager avec Alice.

2) Alice et Bob ont choisi un nombre premier p=23 et une base a=5. Alice choisit un nombre secret $x_1 = 6$ et Bob choisit à son tour un nombre secret $x_2 = 15$. Quelle est la clé d'échange ?

$$K = a^{x1.\,x2}\ [\text{mod } p] = 5^{6x15}\ [23] = 2\ [23]$$

La clé secrète est donc K=2

Exercice 4. On considère l'anneau $\mathbb{Z}/15\mathbb{Z} = \{0, 1, 2, \ldots, 14\}$ des entiers modulo 15.
1) Enumérer tous les éléments de $\mathbb{Z}_{15}{}^{*}$ (les éléments inversibles de $\mathbb{Z}/15\mathbb{Z}$)

$\bar{k}$ est inversible dans $\mathbb{Z}/15\mathbb{Z} \Leftrightarrow$ PGCD(k, n) = 1.

Les éléments inversibles de $\mathbb{Z}/15\mathbb{Z}$ sont donc :

$$1,\ 2,\ 4,\ 7\ ,\ 8\ ,\ 11\ ,\ 13\ ,\ 14$$

2) On définit le procédé de chiffrement multiplicatif sur $\mathbb{Z}/15\mathbb{Z}$ de la façon suivante : $E_a(x) = ax$ mod 15 (l'entier a est la clé)
a) Quelle condition doit vérifier a pour que le déchiffrement soit possible ? Déduire le nombre de clés possibles.

A doit être inversible dans $\mathbb{Z}/15\mathbb{Z}$.

D'après la question précédente, il y a 8 clés possibles.

NB. Puisque la clé a=1 ne permet pas de coder, on peut dire qu'il y a en réalité 7 clés possibles.

b) A partir de l'algorithme d'Euclide étendu, trouver l'inverse de 11 dans $\mathbb{Z}/15\mathbb{Z}$.

L'algorithme donne les coefficients de Bézout :

$$1 = (15 \times 3) + (11) \times (-4)$$

L 'inverse de 11 dans $\frac{\mathbb{Z}}{15\mathbb{Z}}$ est donc -4 = 11 [15]

c) Déchiffrer C= 10 pour a=11.

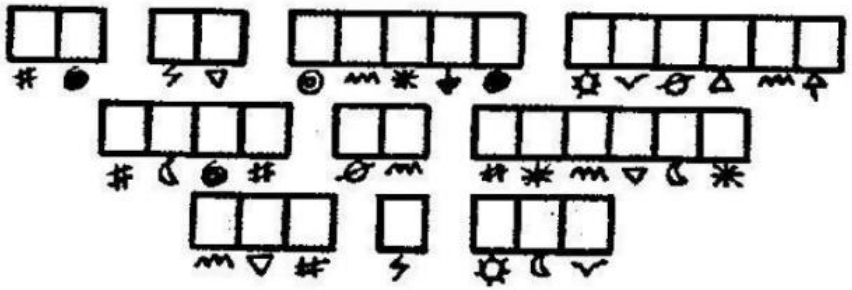
$C = E_a(x) = ax\ [15] \Rightarrow D_a(C) = a^{-1}\ c\ [15]$

Donc $D_{11}(10) = 11^{-1}\ x\ 10\ [15] = 11 \text{ x } 10 = 110 = 5\ [15]$

Que dit Pat à Mickey ?

Fréquences d'apparition des lettres en Français

E	S	A	I	N	T	R	U	L	O	D
14.69%	8.01%	7.54%	7.18%	6.89%	6.88%	6.49%	6.12%	5.63%	5.29%	3.66%



Solution. *”Tu as perdu Mickey tout ce tresor est ˙a moi”*