Corrigé-type + Barème

Réponse à l'exercice 1

1) Le module RSA $n = p \times q = 37 \times 43 = 1591$. 0.5 pt

   L'indicatrice d'Euler est $\varphi(n) = (p-1)(q-1) = 36 \times 42 = 3^3 \times 2^3 \times 7 = 1512$. 0.5 pt

2) La plus grande valeur de l'exposant de chiffrement utilisable dans ce cas est $e = 5$ parce que $PGCD(e, \varphi(n)) = PGCD(5, 1512) = 1$. Les nombres pairs $2, 4, 6$ et 8 ne sont jamais valides parce qu'ils ne sont pas premiers avec $\varphi(n)$. Les nombres impairs $3, 7$ et 9 ne sont pas premiers avec $\varphi(n)$. 1.0 pt

3) La clé publique d'Alice est $(n, e) = (1591, 5)$. 1.0 pt

   L'exposant de déchiffrement d doit vérifier $e \times d \equiv 1 \mod \varphi(n)$ et en utilisant l'algorithme d'Euclide étendu, nous obtenons :
   $1512 \times (-2) + 5 \times (605) = 1$. L'exposant de déchiffrement est : $d = 605 \mod 1512$.

i	r_i	q_i	α_i	β_i
1	1512	–	1	0
2	5	302	0	1
3	2	2	1	-302
4	1	2	-2	605
5	0	–	–	–

   La clé privée d'Alice est $(n, d) = (1591, 605)$. 1.5 pt

4) (a) La valeur de c :
   $m = 20$ et $c = m^e \mod n = 20^5 \mod 1591 = 20 \times 20^4 \mod 1591 = 20 \times 900 \mod 1591 = 18000 \mod 1591$. Ainsi $c = 499$. 1.0 pt

   (b) **La confidentialité** est le seul objectif de sécurité atteint dans ce cas. 0.5 pt

5) Le message clair m correspondant au cryptogramme $c = 23$:
   $c = 23$ et $m = c^d \mod n = 23^{605} \mod 1591 = 23^{252} \times 23^{252} \times 23^{101} \mod 1591 = 23^{101} \mod 1591 = 23 \times 23^4 \times 23^{32} \times 23^{64} \mod 1591 = 23 \times 1416 \times 1358 \times 195 \mod 1591 = \mod 1591$. Ainsi $m = 1562$. 1.0 pt

6) Les objectifs de sécurité atteints dans ce cas sont **La confidentialité** et **l'authentification**. 1.0 pt

Réponse à l'exercice 2

1) Le générateur g :
   On teste d'abord pour 2 :

$2^0 = 1 \mod 37$	$2^1 = 2 \mod 37$	$2^2 = 4 \mod 37$	$2^3 = 8 \mod 37$	$2^4 = 16 \mod 37$
$2^5 = 32 \mod 37$	$2^6 = 27 \mod 37$	$2^7 = 17 \mod 37$	$2^8 = 34 \mod 37$	$2^9 = 31 \mod 37$
$2^{10} = 25 \mod 37$	$2^{11} = 13 \mod 37$	$2^{12} = 26 \mod 37$	$2^{13} = 15 \mod 37$	$2^{14} = 30 \mod 37$
$2^{15} = 23 \mod 37$	$2^{16} = 9 \mod 37$	$2^{17} = 18 \mod 37$	$2^{18} = 36 \mod 37$	$2^{19} = 35 \mod 37$
$2^{20} = 33 \mod 37$	$2^{21} = 29 \mod 37$	$2^{22} = 21 \mod 37$	$2^{23} = 5 \mod 37$	$2^{24} = 10 \mod 37$
$2^{25} = 20 \mod 37$	$2^{26} = 3 \mod 37$	$2^{27} = 6 \mod 37$	$2^{28} = 12 \mod 37$	$2^{29} = 24 \mod 37$
$2^{30} = 11 \mod 37$	$2^{31} = 22 \mod 37$	$2^{32} = 7 \mod 37$	$2^{33} = 14 \mod 37$	$2^{34} = 28 \mod 37$
$2^{35} = 19 \mod 37$	$2^{36} = 1 \mod 37$			

   Ceci qui prouve que 2 est un générateur de $\mathbb{Z}_{37}^{\times}$: $g = 2$. 1.5 pt

2) Clé publique :
   Calculons d'abord $h = g^x \mod p = 2^{17} \mod 37$. Donc : $h = 18 \mod 37$.
   La clé publique est : $(p, g, h) = (37, 2, 18)$. 1.5 pt

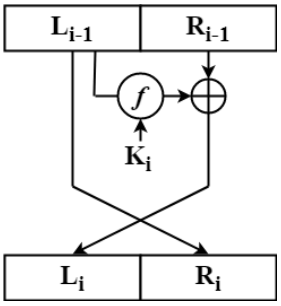
3) Nous avons : $m = 27$ et $k = 29$, alors : $c_1 = g^k \mod p = 2^{29} \mod 37 = 24$ et $c_2 = m \times h^k \mod p = 27 \times 18^{29} \mod 37 = 27 \times 20 \mod 37 = 22$. $c = (c_1, c_2) = (24, 22)$ 1.5 pt

4) Nous avons : $c = (21, 33)$. $\boxed{\alpha = p - x - 1 = 37 - 17 - 1 = 19}$. **0.5 pt**

$m = c_1^{\alpha} \times c_2 \mod p = 21^{19} \times 33 \mod 37 = 21 \times 33 \mod 37$. $\boxed{m = 27}$. **1.0 pt**

Réponse à l'exercice 3

Un schéma de Feistel modifié comme illustré par la figure suivante prend en entrée un bloc clair et le découpe en deux parties de longueurs égales nommées L_{i-1} et R_{i-1}. Il produit en sortie un bloc chiffré sous forme de deux parties de même longueur nommées L_i et R_i.



1) L'opération de chiffrement est donnée par : $\begin{cases} L_i = R_{i-1} \oplus f(L_{i-1}; K_i) \\ R_i = L_{i-1} \end{cases}$ **1.5 pt**

2) L'opération de déchiffrement est donnée par : $\begin{cases} L_{i-1} = R_i \\ R_{i-1} = L_i \oplus f(R_i; K_i) \end{cases}$ **1.5 pt**

3) Le résultat de chiffrement du bloc $m = (5AEC)_{16}$ et $k = (84)_{16}$:
$m = (5AEC)_{16} = (0101101011101100)_2$ et $k = (84)_{16} = (10000100)_2$.
Ainsi, $L_{i-1} = 01011010$ et $R_{i-1} = 11101100$.
$\begin{cases} L_i = 11101100 \oplus (\overline{01011010 \oplus 10000100}) = 11101100 \oplus \overline{11011110} = 11101100 \oplus 00100001 = 11001101 \\ R_i = 01011010 \end{cases}$
Alors : $\boxed{c = 1100110101011010} = (\text{CD5A})_{16}$ **1.5 pt**

4) Le résultat de déchiffrement du bloc $c = (D27B)_{16}$ et $k = (E6)_{16}$:
$c = (D27B)_{16} = (1101001001111011)_2$ et $k = (E6)_{16} = (11100110)_2$.
Ainsi, $L_i = 11010010$ et $R_i = 01111011$.
$\begin{cases} L_{i-1} = R_i = 01111011 \\ R_{i-1} = L_i \oplus f(R_i; K_i) = 11010010 \oplus \overline{01111011 \oplus 11100110} = 11010010 \oplus \overline{10011101} \end{cases}$
$\Longrightarrow \begin{cases} L_{i-1} = 01111011 \\ R_{i-1} = 11010010 \oplus 01100010 = 1011000 \end{cases}$
Alors : $\boxed{m = 0111101110110000} = (\text{7BB0})_{16}$ **1.5 pt**