Université Batna 2 -Mostefa Ben Boulaïd

- Faculté de Technologie –

Département D'Electronique

3éme Année Licence Télécommunication 2017-2018

Solution EXAMEN

Sécurité de l'information

Responsable : Dr. Hadef Mahmoud

Exercice 01 (8 points)

Le RSA est une technique de codage asymétrique. Le RSA utilise deux nombres primaires, *p* et *q*, une clé de chiffrement publique **<e,n>** et une clé de déchiffrement privée **<d,n>.**

1) Les étapes principales pour générer la clé publique et la clé privée du RSA 2.5 points

1. Choisir p et q, deux nombres premiers distincts (généralement très larges)
2. Calculer leur produit n = p*q → module de chiffrement
3. Calculer ϕ(n) = (p - 1)*(q -1)
4. Choisir un entier naturel e premier avec ϕ(n) et strictement inférieur à ϕ(n), appelé exposant de chiffrement ;
5. Calculer l'entier naturel d, inverse de e modulo ϕ(n), et strictement inférieur à ϕ(n), appelé exposant de déchiffrement tel que : e*d ≡ 1 mod(ϕ(n))

2) Le RSA utilise la clé publique <e,n> pour le chiffrement comme suit : 1 point

$$C \equiv M^e \bmod(n)$$

et le RSA utilise la clé privée **<d,n>** pour le déchiffrement comme suit :

$$M \equiv C^d \bmod(n)$$

3) Pour **<e,n> = <5,91>** les valeurs de *p, q* et *e* suivantes : $p = 7$, $q = 13$, $e = 5$ 0.5 point

a. On Calcule La valeur positive la plus petite du ***d*** qui fonctionne comme la clé privée de l'algorithme du RSA

- le produit ϕ(n) = (p - 1)*(q -1)= 6*12 = 72 0.25 point
- On calculer d tel que : e*d ≡ 1 mod(ϕ(n)) donc 5d≡ 1 mod(72)
  29* 5*d≡ 29 mod(72) → d≡ 29 mod(72)
  d≡ 29 mod(192)

  d=29 1.25 point

b. Supposons que le message naturel **M1 = 3** doit être encodé en utilisant la paire de la clé publique

i. Trouvez le message chiffré **C1** qui correspond au message **M1**.
C 1≡ $M1^e$ mod(n) → C1 ≡ 3^5 mod(91) → C1 ≡61mod(91) donc on peut prendre C1=61 0.5 point

ii. Pour vérifier que le message déchiffré du **C1** est le message **M1** on calcule

$$C1^d \equiv ? \bmod(n)$$

$61^0 \equiv 1[91]$ $61^{6k} \equiv 1[91]$

$61^1 \equiv 61[91]$ $61^{6k+1} \equiv 9[91]$

$61^2 \equiv 81[91]$ $61^{6k+2} \equiv 81[91]$

$61^3 \equiv 27[91]$ $61^{6k+3} \equiv 27[91]$

$61^4 \equiv 9[91]$ $61^{6k+4} \equiv 9[91]$

$61^5 \equiv 3[91]$ $61^{6k+5} \equiv 3[91]$

$61^6 \equiv 1[91]$

puisque 29=6*4+5 donc

$61^{29} \equiv 3 \bmod(91)$ 0.5 point

Supposons que le message naturel **M2 = 11** doit être encodé en utilisant la paire de la clé publique

iii. Trouvez le message chiffré **C2** qui correspond au message **M2**.
C $2 \equiv M2^e \bmod(n) \rightarrow C2 \equiv 11^5 \bmod(91) \rightarrow C2 \equiv 72 \bmod(91)$ donc on peut prendre C2=72 0.5 point

iv. Pour vérifier que le message déchiffré du **C2** est le message **M2** on calcule

$C2^d \equiv ? \bmod(n)$

$72^0 \equiv 1[91]$ $72^{12k} \equiv 1[91]$

$72^1 \equiv 72[91]$ $72^{12k+1} \equiv 72[91]$

$72^2 \equiv 88[91]$ $72^{12k+2} \equiv 88[91]$

$72^3 \equiv 57[91]$ $72^{12k+3} \equiv 57[91]$

$72^4 \equiv 9[91]$ $72^{12k+4} \equiv 9[91]$

$72^5 \equiv 11[91]$ $72^{12k+5} \equiv 11[91]$

$72^6 \equiv 64[91]$ $72^{12k+6} \equiv 64[91]$

$72^7 \equiv 58[91]$ $72^{12k+7} \equiv 58[91]$

$72^8 \equiv 81[91]$ $72^{12k+8} \equiv 81[91]$

$72^9 \equiv 8[91]$ $72^{12k+9} \equiv 8[91]$

$72^{10} \equiv 30[91]$ $72^{12k+10} \equiv 30[91]$

$72^{11} \equiv 67[91]$ $72^{12k+11} \equiv 67[91]$

$72^{12} \equiv 1[91]$

puisque 29=12*2+5 donc

$72^{29} \equiv 11 \bmod(91)$ 0.5 point

Supposons que nous ne connaissons pas *p* et *q* mais on a la clé publique <5,91>, est ce que il est possible de trouver la clé de déchiffrement privée **<d,n>,** dans ce cas justifiez votre réponse.
Oui → petit n=7x13 donc $\phi(n) = (p - 1)*(q - 1) = (11-1)*(5-1)= 72 \rightarrow 5*d \equiv 1 \bmod(72)$
Donc d=29 0.5 point

Exercice 02 (6 points)

1. Les opérations d'un tour du technique DES de cryptographie symétrique 4 points

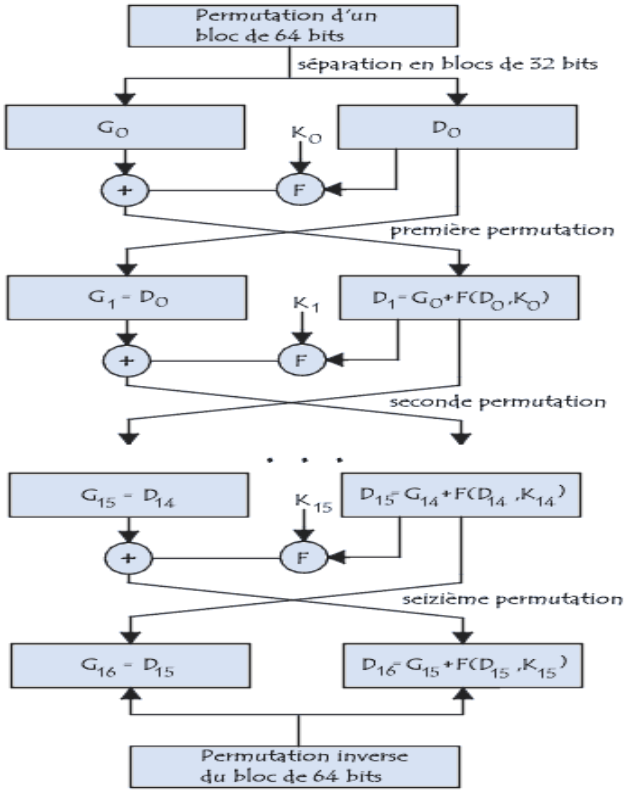
Dans chaque tour les opérations suivantes sont appliquées :

1. Le block de 64 bits (permuté) est divisé en deux blocks, chacun a 32 bits.

2. 48 bits sont sélectés à partir de la clé de 64 bits.
3. On dénote le demi-block gauche pendant le tour i par $L_i$et de demi block droite par R_i et les 48 bits sélectés de la clé pendant le même tour par Ki.
4. L'opération qui s'applique chaque tour est la suivante :

$$L_i = R_{i-1} \dots \dots \dots (1)$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \dots \dots \dots (1)$$



2. Dans la technique de cryptographie DES, pourquoi doit-on à chaque tour diviser Le block de 64 bits (permuté) en deux blocks, chacun de 32 bits? → Pour la faisabilité du déchiffrement sinon on ne peut pas déchiffrer le message reçus **2 point**

Exercice 03 (6 points)

Le message reçus est le suivant :

PVV ZNWTO KT JEYQVCO WJ RWFU GKFB

1) On peut trouver le mot clé en utilisant Le diagonaln du tableau de **Vigenère et puisque le** message chiffré de la clé avec la clé elle-même est **SCIU** donc on aura 16 possibilités des mots clés suivantes **(3 points)**

JBEX	JBEK	JBRX	JBRK
JOEX	JOEK	JORX	JORK
WBEX	WBEK	WBRX	WBRK
WOEX	WOEK	WORX	**WORK**

2) Déterminer le message initial envoyé **3 points**

Message initial → **THE PRICE OF SUCCESS IS HARD WORK**

La clé utilisée → **WORKWORKWORKWORKWORKWORKWOR**

Le message chiffré → PVVZNWTOKTJEYQVCOWJRWFUGKFB