Sécurité Informatique

1CS

Contrôle Final

Partie Exercices

Exercice1 *(5 points)*

Soit le message $m1 = 11$ à chiffrer avec le crypto système RSA défini avec la clé publique $(e, N) = (3, 187)$. Donner le chiffré $c1$ de $m1$.

Sachant que $N = p \times q$, avec $p = 11$. Déchiffrer $c2 = 23$,

Exercice 2 *(2 points)*

On désire chiffrer le texte suivant par la méthode de Vigenère.

«$Les\ problèmes\ de\ sécurité\ qu'on\ peut\ rencontrer\ sur\ un\ réseau\ d'entreprise\ ou\ sur\ l'Internet\ relèvent\ d'abord\ de\ la\ responsabilité\ des\ victimes\ avant\ d'être\ imputables\ aux\ hackers$ »

Dont la clé est la suivante : « **Faille de sécurité sur internet** »

1. Donner le chiffré de « $Les\ problèmes\ de\ sécurité$ ».
2. On voudrait chiffrer le message en entier, que proposez-vous, comme méthode, pour le faire rapidement ?

Exercice 3 *(4 points)*

Une des opérations utilisée dans la MixCulumn de l'AES est la multiplication dans GF(2^8). Soit une donnée A sur 8 bits $(a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$, on désire réaliser un circuit permettant de faire la multiplication, dans le corps le Galois GF(2^8), par la valeur 05.

- Proposer un circuit (à base de portes Xor) permettant de faire cette opération. Expliquer la conception de ce circuit.
- Donner le nombre de portes et la latence de ce circuit.
- Calculer la multiplication de 8F par 05.

On donne le polynome irréductible P(x)= (x^8+ x^4+ x^3+ x +1).

Exercice n° 1

1- soit le message $m_1 = 11$, clé $(e, N) = (3, 187)$

C_1 est le chiffré de m_1

$C_1 = m_1^e \bmod N = 11^3 \bmod 187 = \boxed{22}$ 1pt

2/ Déchiffre $C_2 = 23$.

On calcul d'abord la clé privé d.

$e.d = 1 \bmod \varphi(n)$; $\varphi(n) = (p-1)(q-1)$.

$p = 11$, et $p.q = 187 \Rightarrow q = \frac{187}{11} = 17$.

$\varphi(n) = 160 \Rightarrow d.3 = 1 \bmod 160$.

$\Rightarrow \boxed{d = 107}$ 2pts

$M_2 = C_2^d \bmod N = 23^{107} \bmod 187 \boxed{= 56}$ 2pts

Exercice n° 2.

1- Le chiffré par Vigenère du texte : "Les problèmes de sécurité" avec la clé "Faille de sécurité sur internet"

L	e	s	p	r	o	b	l	è	m	e	s	d	e	s	é	c	u	r	i	t	é	.				
F	a	i	l	l	e	d	e	s	e	c	u	r	i	t	e	s	u	r	i	n	t	e	r	n	e	t
Q	E	A	A	C	S	E	P	W	Q	G	M	U	M	L	I	U	O	I	Q	S	X	mod 26				
R	F	B	B	D	T	F	Q	X	R	H	N	V	N	M	J	V	P	J	R	H	Y	mod 27				

1pt

Scanned by CamScanner

Suite Exo 2.

2- Pour le chiffrement rapide on utilise une table comme suit :

	A	B	. . . .	Z
A	B	C	D . .	
B	.			
:				
Z	A			

1pt

qui sera adressable par les 2 lettres à additionner cette table s'appelle le tableau de Vigenère.

Exercice n°3

1- le circuit pour le calcul de $B.\{0S\}$.

Soit $B(a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$.

qui est représenté par le polynome suivant.

$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x_1 + b_0$.

Scanned by CamScanner

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

$\times$

$$x^2 + 1$$

$$b_7x^9 + b_6x^8 + b_5x^7 + b_4x^6 + b_3x^5 + b_2x^4 + b_1x^3 + b_0x^2$$

$+$

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

$$b_7x^9 + b_6x^8 + (b_7+b_5)x^7 + (b_6+b_4)x^6 + (b_3+b_5)x^5 + (b_2+b_4)x^4 + (b_3+b_1)x^3 + (b_0+b_2)x^2 + b_1x + b_0$$

$+$

$$b_7x^9 + b_7x^5 + b_7x^4 + b_7x^2 + b_7x$$

$$b_6x^8 + (b_7+b_5)x^7 + (b_6+b_4)x^6 + (b_3+b_5+b_7)x^5 + (b_2+b_4+b_7)x^4 + (b_3+b_1)x^3 + (b_0+b_2+b_7)x^2$$

$$+ (b_1+b_7)x + b_0$$

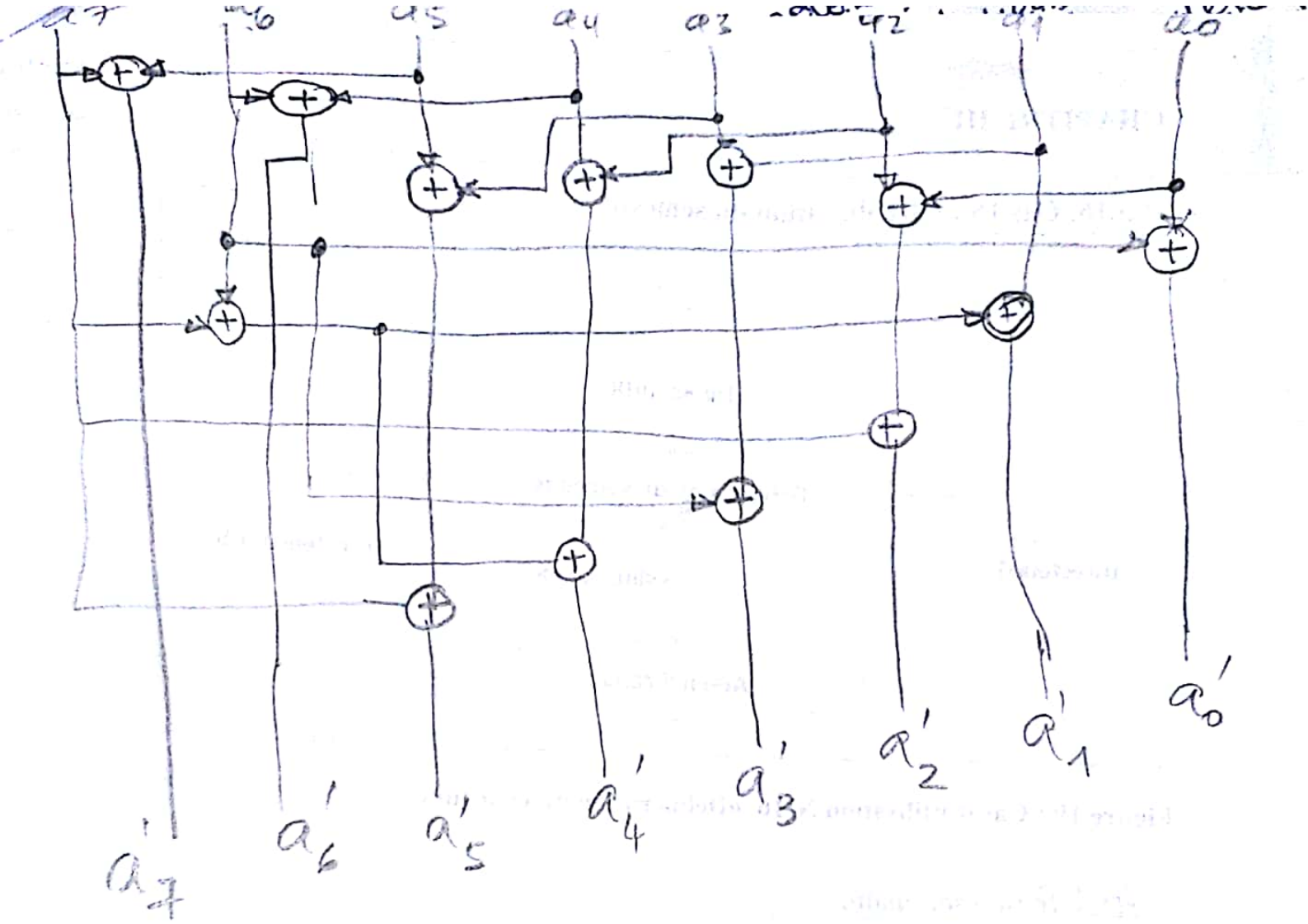
$$b_6x^8 + b_6x^4 + b_6x^3 + b_6x + b_6$$

$S_7 = b_7 + b_5$, $S_6 = b_6 + b_4$, $S_5 = b_3 + b_5 + b_7$, $S_4 = b_2 + b_4 + b_7 + b_6$, $S_3 = b_3 + b_1 + b_6$

$S_2 = b_0 + b_2 + b_7$, $S_1 = b_1 + b_7 + b_5$, $S_0 = b_0 + b_6$

$$\text{XI} \times 05 = \text{X5}$$

Scanned by CamScanner



13 parts

Scanned by CamScanner

(0.5pt) **10.** J'ai en ma possession un message m que je ne souhaite pas encore divulguer, mais dont je veux pouvoir prouver dans quelques années que je le connaissais déjà en 2015 (horodatage). Pour cela, il me suffit de publier dès aujourd'hui...

- ○ A Un chiffrement de m avec ma clé publique.
- ○ B Un chiffrement de m avec ma clé privée.
- ○ C L'image de m par une fonction de hachage.

Questions de cours

(1pt) 1. Expliquer ce qu'est un (MAC) *Message Authentication Code* ?

...C'est une fonction de hachage munie d'une clef, qui permet de vérifier l'intégrité et la provenance du message en même temps.....

(1pt) 2. La transformation Inverse mixcolumn **InvMixColumn** dans le processus de déchiffrement AES est plus lente que la MixColumn du chiffrement. Donner les raisons de cette lenteur. .

...Les termes de la matrice **InvMixColumn** sont plus grands que ceux de la **MixColumn**. Et comme la multiplication, dans GF(2^8), par une grande valeur est plus complexe qu'avec une faible valeur. Ce qui induit un délai plus important

(1pt) 3. La première étape dans l'utilisation du MD5, consiste à faire le bourrage, explique ce que c'est ?

..... On bourre le message d façon à ce que la taille de celui-ci devienne un multiple de 512 bits. On ajoute alors au message M un bit à 1, puis autant de 0 que nécessaire pour arriver à 64 bits de moins que le prochain multiple de 512. En fin on ajoute un entier de 64 bits donnant la longueur du message original.

(1pt) 4. Expliquer ce que c'est une fonction à sens unique munie d'une trappe (donner un exemple) ?

Une fonction unidirectionnelle est une fonction ***y = f(x)*** *telle que, si l'on connaît la valeur* ***y****, il est pratiquement impossible de calculer* ***x****.*
On dit que cette fonction est munie d'une ***trappe*** *s'il existe une fonction* ***x = g(y, z)*** *telle que, si l'on connaît* ***z****, il est facile de calculer* ***x*** *à partir de* ***y****.* ***z*** *est appelée trappe. Exemple de fonction le* ***RSA***

Scanned by CamScanner