durée 1h30, aucun document autorisé

Exercice 1 chiffrement de végenère

question 1 (sur 1 point)

Chiffrez le texte suivant à l'aide de la méthode de Vigénère et de la clef « salut »:
« ilétaitunpetitnavire »

question 2 (sur 1 point)

Qu'apporte le chiffrement de vigénère en matière de sécurité par rapport à une simple substitution alphabétique ?

Vigénère apporte un plus car une même lettre peut être chiffrée différemment dans le texte ce qui complique l'analyse statistique. Vigènere est donc plus solide.

Remarque: il y a des attaques connues conctre Vigènere: déterminer d'abord la taille de la clef puis faire des attaques statistiques. Cf TD.

Exercice 2 chiffrement par bloc

question 1

Décrivez les méthodes de chiffrement par bloc ECB et CBC (donnez le schéma de chiffrement et déchiffrement ainsi que les formules de chiffrement et déchiffrement);

cf cours

question 2

Citez les forces et les faiblesses de la méthode ECB (performances, sécurité) .

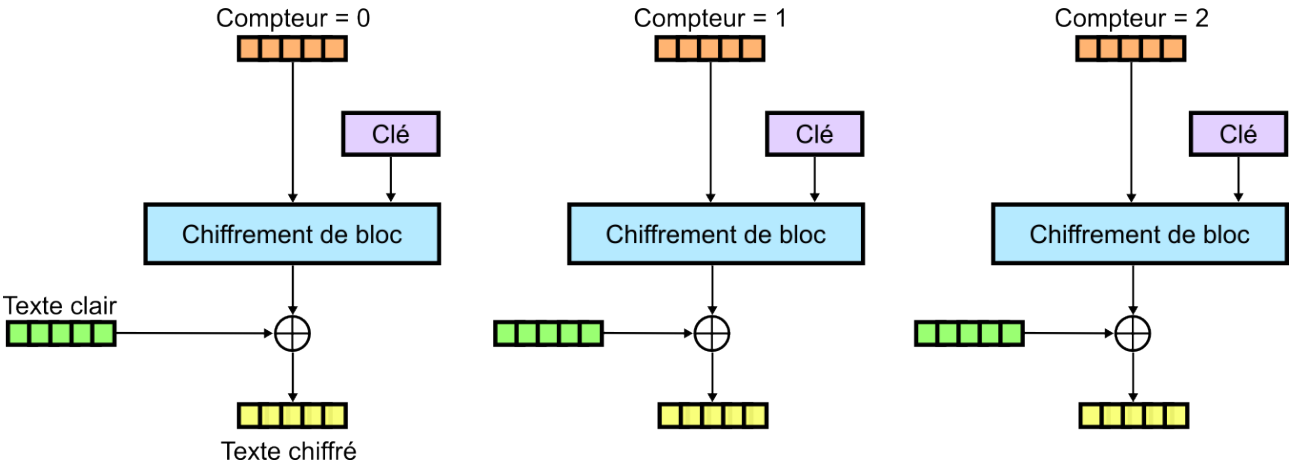
Cf cours. A noter qu'il donner des éléments concrets. Dire « ECB est mauvais d'un point de vue sécurité » n'apporte aucune information utile et aucun point.

question 3

On suppose qu'un bloc est vérollé lors du transfert. Indiquez pour chacune de ces deux méthodes combien de blocs seront vérollés au déchiffrement. Vous justifierez votre réponse.

Cf cours. Il faut justifier la réponse par une explication rapide (le plus simple, c'est la formule de déchiffrement).

Exercice 3 chiffrement par bloc



question 1

On considère le mode de chiffrement par bloc CounTeR (CTR) décrit par le schéma ci-dessus.

Le chiffrement se fait de la façon suivante : compteur=compteur+1; ci=E(k, compteur) ⊕ mi

Donner la procédure de déchiffrement ainsi que la formule de déchiffrement.

Chiffrement :

compteur=compteur+1

Ci=Mo XOR compteir

déchiffrement :

compteur=compteur+1

mi=Ci XOR E(compteur)

On a tendance à prendre ses désirs pour des réalités et de nombreux étudiants ont voulu faire intervenir la fonction de déchiffrement ce qui est inutile et faux. Ici, on génère une sorte de flux pseudo-aléatoire que l'on combine avec le message en clair. Pour déchiffrer, il suffit de générer le même flux et de le combiner avec le message chiffré.

question 2

Citez les forces et les faiblesses de la méthode CTR (performances, sécurité) et proposez des améliorations.

Forces:

- **calcul parallélisable des E(compteur)**
- **précalcul possible des E(compteur)**
- **2 blocs en clair identiques d'un même fichier donneront des versions chiffrées différentes**

Faiblesses :

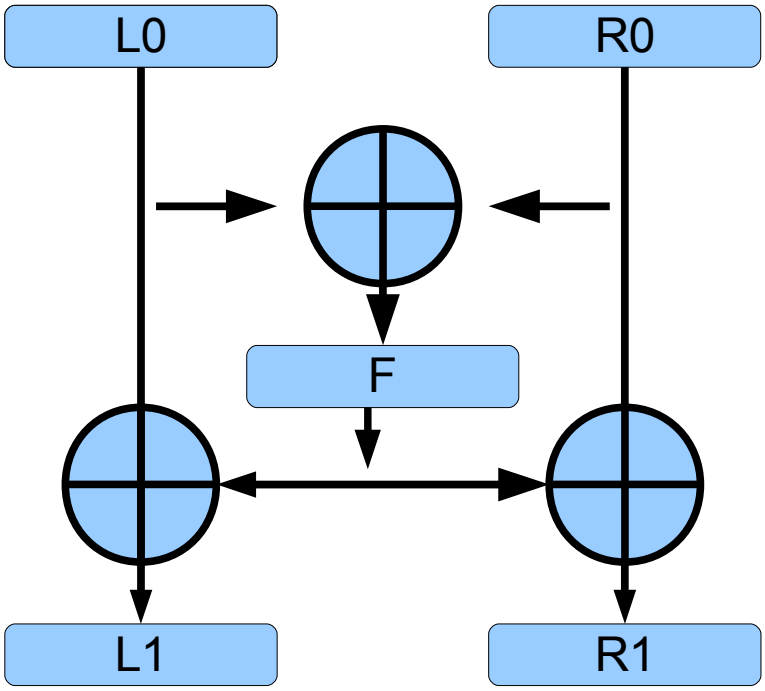
- **la taille du compte doit permettre d'avoir des valeurs différentes lors du chiffrement d'un fichier;**

- **2 fichiers chiffrés avec la même clef et commençant de la même façon auront une version chiffrée qui commence de la même façon**
    - **solution : choisir la valeur initiale du compteur au hasard et la transmettre en clair avant le fichier chiffré : IV**

A noter : seuls arguments concrets sont retenus. Dire « CBC est mieux car on combine avec le chiffré précédent ce qui semble plus sur que de combiner avec la version chiffrée d'un compte » n'est pas un raisonnement recevable.

Exercice 4 IDEA

IDEA est un algorithme de chiffrement par blocs. Il utilise des clefs de 128 bits et chiffre des blocs de 64 bits. Il utilise le schéma de Feistel modifié suivant :



question 1

Que pensez-vous de la taille des blocs et des clefs d'IDEA : comparés à DES et dans l'absolu du point de vue sécurité ?

- **Taille des clefs**
    - **IDEA: 128 bits (soit 2^128 clefs possibles) : mieux que DES et c'est suffisant actuellement**
    - **DES: 56 bits (trop faible actuellement)**
- **tailles des blocs :**
    - **DES : 64 bits**
    - **IDEA: 64 bits (idem DES, c'est trop peu : attaque des anniversaires. 128 est un minimum (d'après le cours)).**

question 2 chiffrement

Exprimez L1 et R1 en fonction de L0 et R0.

L1=L0 XOR f(L0 XOR R0)

R1=R0 XOR f(L0 XOR R0)

question 3 déchiffrement

Exprimez L0 et R0 en fonction de R1 et de L1.

On a vu en question 2 que : L1=L0 XOR f(L0 XOR R0) et R1=R0 XOR f(L0 XOR R0)

additionnons ces deux égalités et on obtient :

L1 XOR R1 =L0 XOR f(L0 XOR R0) XOR R0 XOR f(L0 XOR R0) = L0 XOR R0

des deux égalités de la question 2, on déduit le résultat cherché :

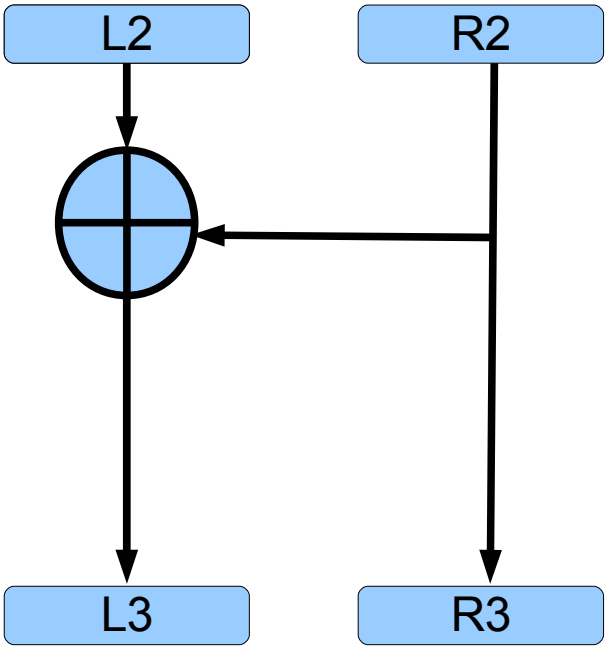
L0=L1 XOR f(L0 XOR R0) = L1 XOR f(R1+L1)

R0=R1 XOR f(L0 XOR R0) = R1 XOR f(R1+L1)

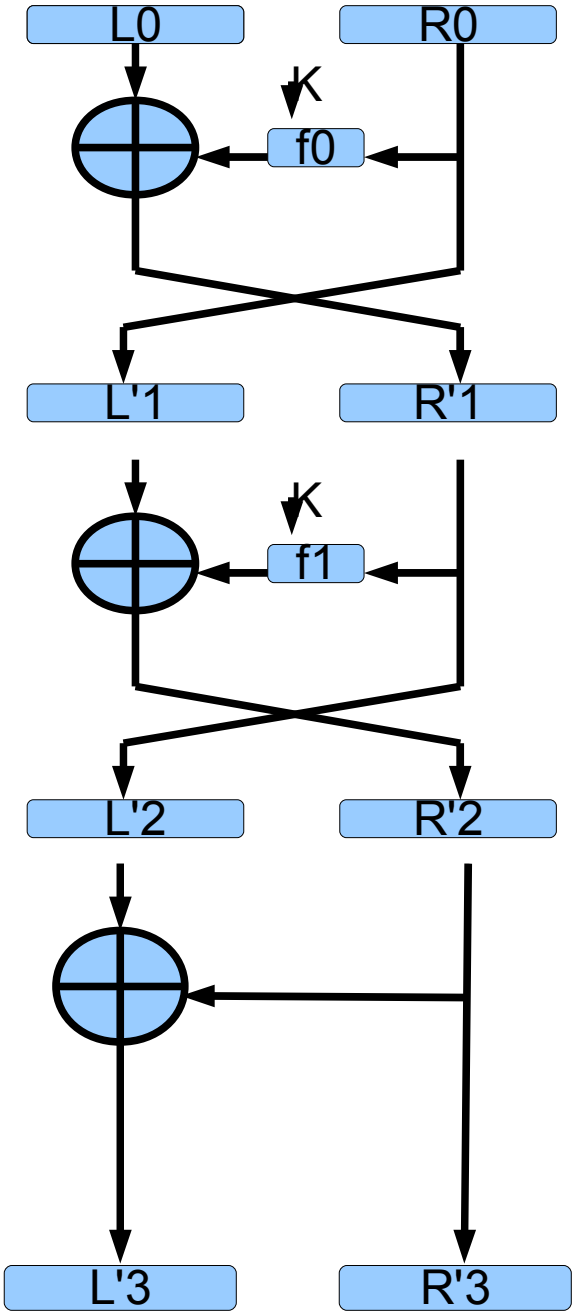
question 4 schéma de Feistel équivalent

Décrivez un schéma de Feistel 3 tours (avec, pour chaque tour une fonction f bien choisie) équivalent au schéma utilisé par IDEA. On prendra le schéma suivant pour le 3e tour (Feistel modifié). **Les schéma des 1er et 2e tour seront des schémas de Feistel non modifiés. Votre marge de manoeuvre consiste simplement à choisir habilement la fonction f de chaque tour.**

3e tour :



Votre travail consiste à fournir les tours 1 (calcul de L1, R1 en fonction de L0, R0) et 2 (calcul de L2, R2 en fonction de L1, R1 de façon à ce que L3,R3 soient égaux à ce que l'on obtiendrait en faisant passer R0, L0 à travers un tour d'IDEA.



Notre but est de choisir les deux fonctions f0 et f1 de façon à ce que L'3=L1=L0 XOR f(R0 XOR L0) et R'3=R1=R0 XOR f(R0 XOR L0).

R'2=R'3= R0 XOR f(R0 XOR L0) = L'1 XOR f1(R'1)

L'3=L'2 XOR R'2=R'1 XOR R0 XOR f(R0 XOR L0)

L'1= R0

R'1= L'0 XOR f0(R'0)

donc : R0 XOR f(R0 XOR L0) = R0 XOR f1(L'0 XOR f0(R'0))

on voit que deux fonctions conviennent pour réaliser cette égalité :

f0= Id soit f0(X)=X pour tout X

f1=f

Il reste ensuite à calculer L'3 et R'3 avec ces deux fonctions pour vérifier qu'elles conviennent bien.

Table :

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***
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	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	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