Devoir surveillé

Crytologie

durée 1h30

aucun document autorisé

Exercice 1 chiffrement de végenère

question 1

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

question 2

Déchiffrez le texte suivant à l'aide de la méthode de Vigénère et de la clef « manger »:
«HIIKQVZTYKWMMCNTGVE»

Exercice 2 chiffrement par bloc

question 1

Décrivez les méthodes de chiffrement par bloc ECB et CBC.

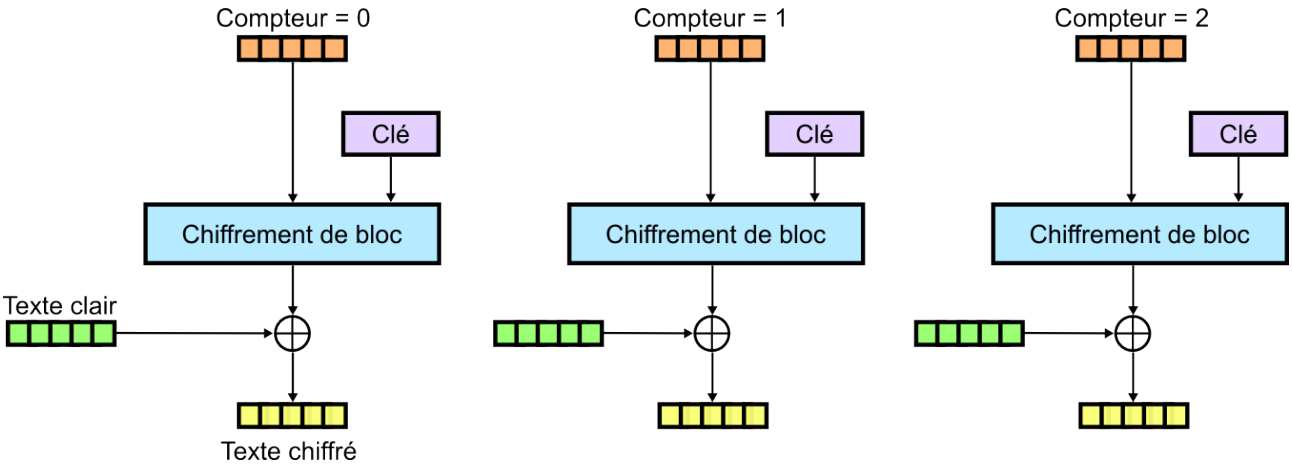
question 2

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

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.

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

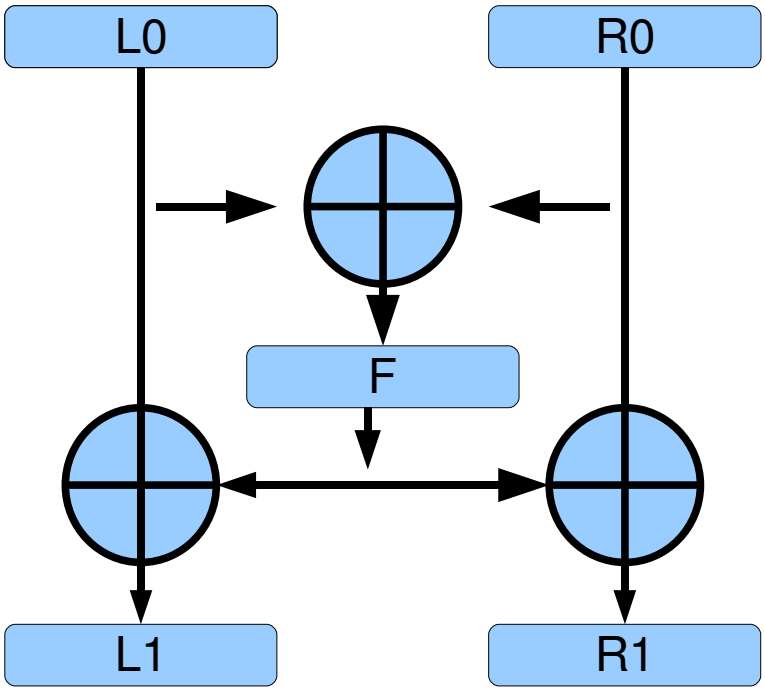
Donner la procédure de déchiffrement.

question 2

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

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 ?

question 2 chiffrement

Exprimez L1 et R1 en fonction de L0 et R0.

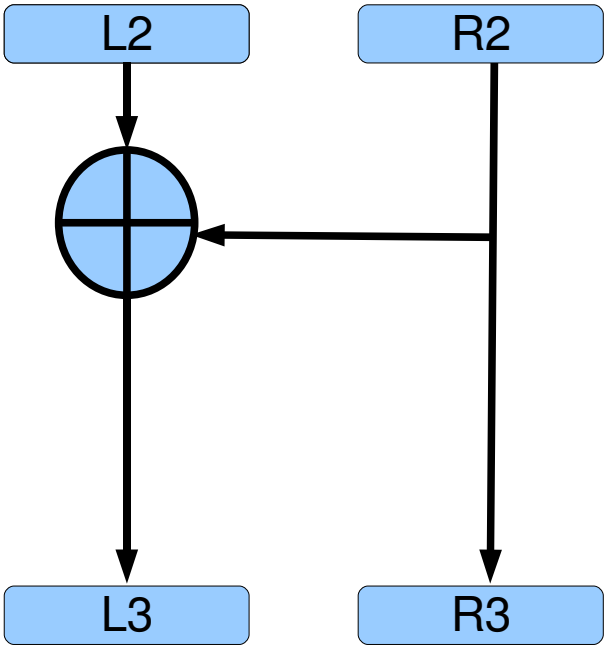
question 3 déchiffrement

Exprimez L0 et R0 en fonction de R1 et de 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 modifié. Votre marge de manoeuvre consiste simplement à choisir habilement la fonction f.**

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.

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