Faculté des Sciences et Techniques
Limoges

2004-2005

Master I

Initiation à la Cryptographie

Contrôle du 13 janvier 2005

durée : 2 h

Avec calculatrices

Exercice 1 : D.E.S

1. Déterminer les entrées possibles de la Sbox S_4 lorsque la sortie est 12, puis 5.
2. Quels sont les bits de R qui sont utilisés par S_4 ?
3. Si $R = AE34ED2A$, quels sont les valeurs des bits en sortie de l'expansion E ?
4. Soit K une sous-clé fixée. On suppose que si $R = AE34ED2A$ alors $S_4(R, K) = 12$ et que si $R = F1A3305B$ alors $S_4(R, K) = 5$.
   a) Quelles sont les valeurs possibles de la partie de clé K utilisant par S_4 dans le premier cas ?
   b) Quelle est la valeur de la partie de clé K (Cryptanalyse à un tour) ?

Exercice 2 : AGDVFX

Sachant qu'il a été chiffré avec le système AGDVFX et la clé LINE, déchiffrer le message suivant :

`VADDGDVDDADGGDDVXGDADDVXVVVDGDVVDXGADADX`

Exercice 3 : Chiffrement de HILL

On considère la matrice de chiffrement

$$K = \begin{pmatrix} 2 & 1 \\ 5 & 7 \end{pmatrix}.$$

On code les lettres majuscules avec le principe suivant : 'A' est noté 0 jusqu'à 'Z' noté 25.

1. La matrice K est-elle une matrice de chiffrement correcte ?
2. Chiffrer le mot `CRYPTO` à l'aide de cette matrice.
3. Déterminer la matrice inverse puis déchiffrer la séquence suivante : `YIDPZJ`

On ne connaît plus la matrice de Hill utilisée mais on sait qu'elle est de dimension 2. On suppose que le début du clair a été intercepté et commence par `MONGENERAL`.

4. De quel type d'attaque s'agit-il ? Rappeler les trois autres cas de classification des attaques.
5. Retrouver la clé utilisée pour obtenir le chiffré suivant : `YKTZZUDCLW`

Rappels

Table d'Expansion E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Table S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

	A	**D**	**F**	**G**	**V**	**X**
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q