Principes et Algorithmes de Cryptographie

DS du 24 mars 2011

Durée 1h30 - documents de cours autorisés

Exercice 1. *Vider l'océan avec un dé à coudre*

La recherche d'une clé par force brute revient à « vider l'océan avec un dé à coudre ».

On considère qu'un dé à coudre est un cylindre de $1,5$ cm de hauteur pour $1,5$ cm de diamètre. Selon l'Institut Français des Mers, les océans couvrent 360 millions de km^2 avec une profondeur moyenne de 3800 m, et contiennent donc $360 \times 3,8 = 1368$ millions de km^3 d'eau.

Question 1. Encadrez entre deux puissances de 2 consécutives le nombre de dés à coudre d'eau que contiennent les océans [1].

Question 2. Qu'est-ce qui demande le plus de travail

1. vider l'océan avec un dé ?
2. ou bien rechercher exhaustivement une clé de 80 bits d'un système de chiffrement symétrique ?

Exercice 2. *Reconnaissance de systèmes de chiffrement*

Première partie

L'analyse des fréquences des caractères d'un cryptogramme intercepté de 1936 caractères donne le tableau suivant

A	3,36%	B	17,67%	C	1,50%	D	0,57%	E	0,52%	F	7,02%
G	0,31%	H	0,05%	I	6,25%	J	3,20%	K	6,87%	L	6,15%
M	3,46%	N	1,96%	0	6,66%	P	7,95%	Q	7,28%	R	6,30%
S	1,29%	T	0,05%	U	0,41%	V	0,15%	W	0,15%	X	7,08%
Y	0,98%	Z	2,79%								

Question 1. En supposant que le message clair est rédigé en français, quels sont les éléments de ce tableau de fréquences qui permettent de déterminer avec confiance le système de chiffrement utilisé, et quel est ce système ?

Question 2. Déchiffrez alors le message suivant

```
MBQBP XJMOX PXSXF QRKQB KKFPM OBSFP FYIB
```

Deuxième partie

Le tableau qui suit donne les indices de coïncidence (I) pour un second cryptogramme en fonction du décalage (d).

d	I	d	I	d	I	d	I	d	I
1	3.62%	21	8.77%	41	4.12%	61	3.25%	81	3.40%
2	4.24%	22	4.65%	42	8.03%	62	3.47%	82	3.61%
3	3.31%	23	2.40%	43	4.60%	63	7.74%	83	4.16%
4	3.93%	24	3.82%	44	2.80%	64	4.22%	84	7.61%
5	4.09%	25	4.13%	45	3.49%	65	3.79%	85	4.92%
6	3.94%	26	3.04%	46	3.86%	66	4.22%	86	3.08%
7	7.31%	27	4.19%	47	3.23%	67	4.55%	87	3.73%
8	3.68%	28	7.49%	48	3.65%	68	3.59%	88	3.41%
9	3.11%	29	4.30%	49	7.21%	69	3.96%	89	3.79%
10	4.15%	30	2.94%	50	3.92%	70	7.66%	90	4.33%
11	3.74%	31	4.62%	51	3.87%	71	4.40%	91	7.53%
12	3.69%	32	3.83%	52	3.82%	72	2.95%	92	4.01%
13	4.47%	33	3.36%	53	4.62%	73	4.35%	93	3.47%
14	8.64%	34	3.94%	54	4.20%	74	3.28%	94	4.02%
15	4.01%	35	8.57%	55	4.20%	75	3.39%	95	3.75%
16	3.39%	36	4.89%	56	6.49%	76	4.73%	96	4.18%
17	4.69%	37	4.00%	57	3.94%	77	6.83%	97	3.64%
18	5.32%	38	4.06%	58	3.35%	78	4.57%	98	7.78%
19	3.34%	39	4.27%	59	4.48%	79	2.96%	99	3.97%
20	4.07%	40	3.59%	60	4.21%	80	3.72%	100	3.92%

1. Je ne vous fairai pas l'affront de vous rappeler que le volume d'un cylindre se calcule selon la formule $V = \pi R^2 h$, où R est le rayon du disque de base, et h la hauteur du cylindre.

Question 3. En tenant compte du fait que le message clair correspondant est rédigé en français, comment ce tableau permet-il de déduire que le chiffrement utilisé n'est certainement pas une substitution monoalphabétique ?

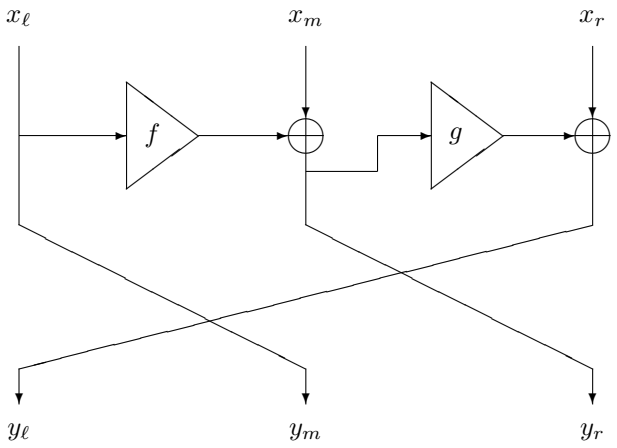
Question 4. On suppose que le système utilisé est celui de Vigenère. Quelle est la longueur de la clé utilisée ?

Question 5. Le mot clé utilisé est le nom (pas le prénom !) du personnage évoqué dans le message clair que vous avez déchiffré dans la première partie. Déchiffrez alors le cryptogramme suivant [2].

`UHMFLEKGIDARPWLIFTGOMDEBDEDSATCJVLIMEBPIT`.

Exercice 3. *Chiffrement par blocs*

On considère un système de chiffrement itératif par blocs. Un tour de chiffrement prend un bloc de 48 bits en entrée ; il est réalisé en partageant le bloc en 3 sous-blocs (x_ℓ, x_m, x_r) de 16 bits chacun selon le schéma ci-dessous :



que l'on peut également écrire

$$\begin{cases} y_\ell &= x_r \oplus g(x_m \oplus f(x_\ell)) \\ y_m &= x_\ell \\ y_r &= x_m \oplus f(x_\ell) \end{cases}$$

Question 1. Montrez que quelles que soient les fonctions f et g, ce schéma (correspondant à un tour) réalise une bijection. Faire un schéma et écrire l'équation de la fonction réciproque d'un tour.

Question 2. Expliquez comment on peut distinguer une fonction réalisée par deux tours de ce schéma d'une fonction aléatoire.

2. Si vous n'avez pas su déchiffrer le message précédent, vous pouvez me demander quel est ce nom.