Examen du 16 juin 2009

Durée 2h - documents autorisés

Exercice 1. *Chiffrement avec* OPENSSL

Voici un extrait des systèmes de chiffrement avec lesquels OPENSSL permet de chiffrer des fichiers : `bf-cbc, bf-cfb, bf-ecb, bf-ofb, des-cbc, des-cfb, des-ofb, des-ecb, rc4, aes-[128|192|256]-cbc, aes-[128|192|256]-cfb, aes-[128|192|256]-ecb, aes-[128|192|256]-ofb`.

Question 1. Que signifie `aes-[128|192|256]` ?

Question 2. On peut constater que certains systèmes apparaissent plusieurs fois avec des variantes CBC, ECB, CFB et OFB. De quoi s'agit-il ? Décrivez deux de ces variantes.

Question 3. Le système `rc4` fait exception. Il n'est pas décliné comme les autres en quatre variantes. Pourquoi ?

Exercice 2. *Un peu de tout*

Le but de cet exercice est de décrypter un message chiffré qu'Alice a envoyé à Bob et dont voici le début :

```
TWCZW SKMNV PEIUI TWDVD EOSMV FDVHA TALEW SKHAJ LRVKD ZXFZU
ICWPF MRHMI RKUZN IIWGL DIVJE DWNKD EJUOL JSVLL VKTUN OLKDV
NRZWZ UGNTL OLKLV JEJGU UJEAW VFMSJ GUYSI KWDVJ ELKSZ JCVLE
OSMVF EKLOL KLVKA LLRVK QLWVF MSRNE QUEJB OLJST ABFFN VUOEL
IEMAK AOEVA EKVFK EKMDV K....
```

Le texte clair est rédigé en français avec un alphabet limité aux 26 lettres non accentuées de l'alphabet latin.

Question 1. Donnez des arguments pour justifier le fait que ce message n'a pas été chiffré avec un système de transposition, ni avec un système de chiffrement pas substitution monoalphabétique.

On fait donc l'hypothèse que ce message a été chiffré par un système de chiffrement polyalphabétique du type Vigenère. On désigne dans la suite par C la clé utilisée pour chiffrer.

Question 2. Indiquez quelles techniques il est possible de mettre en œuvre pour déterminer la longueur de la clé C. En particulier, à quelle technique la figure 1 fait-elle référence, et quelle longueur de clé suggère-t-elle ?

Les questions qui suivent ont pour but de déterminer la clé C. Ces questions n'étant pas indépendantes, il vous faut pour répondre à l'une connaître la réponse à la précédente. Si vous êtes bloqués par l'une de ces réponses, appelez-moi et je vous la communiquerai. Bien entendu, cela sera pris en compte pour la correction.

Alice et Bob décident d'utiliser le protocole de Diffie-Hellman pour établir une clé k secrète. Ils appliquent le protocole dans le corps $\mathbb{F}_{167}$ à $p = 167$ éléments.

Question 3. L'un des deux nombres 2 ou 5 n'est pas un générateur du groupe multiplicatif de ce corps, et l'autre l'est. Lequel est générateur ?

Alice et Bob utilisent donc, le protocole de Diffie-Hellman avec le générateur trouvé dans la question qui précède.

Question 4. Sachant que de son côté Alice choisit au hasard le nombre $x_A = 12$ et Bob le nombre $x_B = 15$, calculez la clé k commune à laquelle ils parviennent à la fin du protocole. Déterminez le nombre de multiplications modulaire effectuées par Alice pour calculer k à partir de x_A.

La clé k établie après ce protocole va servir à initialiser un LFSR, qui produira une suite binaire avec laquelle la clé C sera masquée.

Question 5. En initialisant le LFSR de longueur 8 de polynôme et de rétroaction $P(X) = X^8 + X^4 + X^3 + X + 1$ avec la clé k trouvée dans la question précédente, calculez les quinze premiers bits produits par ce LFSR.

Les quinze bits trouvés dans la question précédente ont servi à masquer la clé C que l'on cherche. Cette clé a été codée en codant le rang de chaque lettre de l'alphabet latin en binaire sur cinq bits. Ainsi le `A` est codé `00000`, le `B` est codé `00001`, ..., et le `Z` est codé `11001`.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

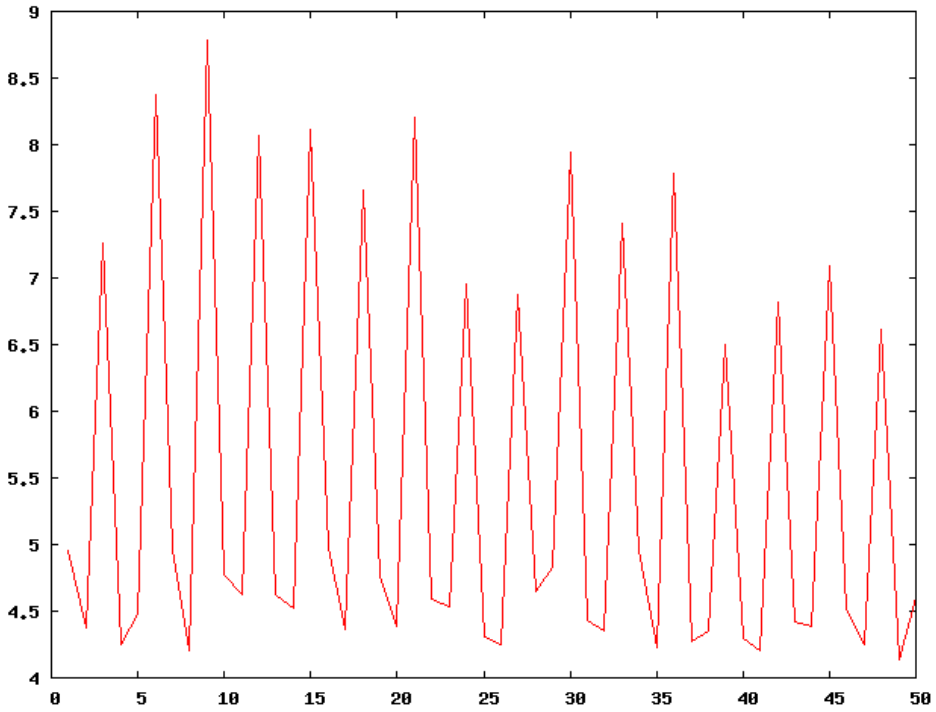

FIG. 1 – Une méthode pour déterminer la longueur de la clé

Question 6. Voici la clé C masquée avec la suite chiffrante produite dans la question précédente (par un ou-exclusif bit à bit) :

11110 01011 10011.

Déterminez la clé C.

Question 7. Décryptez maintenant la première ligne du message.

Exercice 3. *Sur les LFSR*

Dans les questions qui suivent, par l'expression « Donnez un LFSR », on entend « donnez sa longueur et donnez son polynôme de rétroaction ».

Question 1. Donnez un LFSR qui produit la suite binaire périodique de période `100110010`.

Question 2. Donnez le plus petit LFSR qui produit cette suite.

Question 3. Le polynôme de rétroaction du LFSR trouvé dans la question qui précède est-il primitif ? irréductible ?

Question 4. Donnez le plus petit LFSR qui produit la suite binaire ultimement périodique de prépériode `111` et de période `100110010`.