Faculté des sciences exactes et naturelles
Licence Informatique / INFO0603 : Compression et cryptographie
Année universitaire 2017-2018
Pascal Mignot

Université de Reims Champagne-Ardenne

Examen terminal du 15 mai 2018
Première session

Instructions :

- Le polycopié de cours est autorisé. Tout autre document (TDs, notes personnelles, livres, ...) est interdit.
- L'usage de la calculatrice est autorisé. Néanmoins, celle-ci ne devra pas avoir de fonctions communicantes (*i.e.* l'utilisation d'un téléphone portable comme calculatrice est interdit).
- Un résultat donné sans justification sera compté faux (*i.e.* joindre vos brouillons si nécessaire).

Notation : A_x signifie que le nombre A est écrit en base x. Par exemple, 101_2 est 101 en binaire (soit 5 en décimal), 12_{16} est le nombre hexadécimal 12 (soit 18 en décimal). Néanmoins, la base n'est pas précisée lorsqu'elle est évidente dans le contexte.

Exercice 1: Chiffre par décalage

Le message `DLGZTCNPDEAZFGZTC` a été codé avec un chiffre mono-alphabétique par décalage. On rappelle les fréquences des lettres les plus fréquentes : e=17.5%, s=8,0%, a=7,6%, i=7,5%, t=7,2%, n=6,6%.

1. Donner deux méthodes permettant d'éviter de tester toutes les clefs.
2. Décoder avec la méthode de votre choix. Indice : la lettre la plus fréquente est une voyelle.
3. Quel est le principal inconvénient de ce cryptosystème ?

Exercice 2: Chiffre de Vigenère

On souhaite effectuer la cryptanalyse du message suivant "`TERTRE TRES TERRESTRE`" codé avec un chiffre de Vigenère qui utilise un alphabet de 4 symboles $\{E, R, S, T\}$.
Ce message est constitué d'une suite de mots français utilisant les mêmes lettres (*i.e.* pour le code et le texte clair : $E = 0$, $R = 1$, $S = 2$, $T = 3$).

1. Calculer le chiffre de Vigenère pour la clef STR.
2. On voudrait faire de la cryptanalyse. Expliquer pourquoi le calcul des fréquences de lettres n'est d'aucune aide dans ce cas.
3. Appliquer le test de Kasiski sur des motifs de taille au moins 3 afin de déterminer la taille de la clef.
4. En quoi la connaissance de la longueur de la clef va-t-elle nous aider dans la cryptanalyse ?

5 Calculer l'index de coïncidence pour le langage. On supposera que la fréquence des lettres dans le langage est identique à leur fréquence d'apparition dans le texte clair.

6 Calculer les fréquences des lettres pour le troisième symbole de la clef.

7 Calculer l'indice de coïncidence de Friedmann avec deux des possibilités de symboles pour le troisième symbole de clef, dont le bon (par exemple, on effectuera le calcul pour A et R).

8 Comment déduit-on alors le troisième symbole de la clef à partir des indices de coïncidences ?

Exercice 3: Cryptosystème produit

Soit l'alphabet $\mathcal{A} = \{a, b, c, d\}$. On considère l'ensemble des cryptosystèmes par substitution sur $\mathcal{A}$ (noté S) et par permutation (noté Π).

1 Expliquer pourquoi pris seuls, un cryptosystème par substitution ou par permutation n'est pas sûr.

2 Pourquoi un cryptosystème produit est-il potentiellement plus sûr ?

3 Expliquer pourquoi le cryptosystème produit de chiffres par substitution est idempotent. Même question avec les chiffres par permutation.

4 On regarde maintenant le cryptosystème produit d'un substitution et d'une permutation. Soit la substitution s et la permutation π suivantes définies sur un mot de 4 symboles :

x	a	b	c	d
$s(x)$	b	c	d	a

et

i	1	2	3	4
$\pi(i)$	2	3	4	1

Est-ce que le cryptosystème produit est commutatif ? On le vérifiera sur le mot de 4 lettres *bdac*.

5 Comment démontrer le résultat obtenu à la question précédente dans le cas général (i.e. pour toute substitution s et permutation π) ?

6 Soit maintenant le cryptosystème produit obtenu avec $P = \Pi \times S$. Ce cryptosystème produit est-il idempotent ? (dans ce but, prendre p_1 et p_2 dans P, et vérifier si le résultat est idempotent).

7 P est-il commutatif ? On pourra utiliser le fait que S et Π ne sont pas commutatifs.

8 Que peut-on déduire des questions précédentes sur l'intérêt du choix d'un cryptosystème dans P ?

On considère maintenant la transformation d'un paquet de 12 bits, considérés soit comme 6 paquets de 2 bits lors d'une substitution, soit comme 4 paquets de 3 bits lors d'une permutation. Les lettres seront codées sur 2 bits de manière standard avec $a = 00$, $b = 01$, $c = 10$, $d = 11$.

9 En réutilisant la substitution s et la permutation π données ci-dessus, et le texte clair $x = badaca$, calculer $(s \times \pi)(x)$ et $(\pi \times s)(x)$.

10 Ce type de cryptosystème produit présente-t-il un intérêt ?

Exercice 4: Chiffrement AES

On veut dans cet exercice effectuer le chiffrement d'une ronde AES. Le résultat des calculs intermédiaires effectués lors de la ronde est :

B_0^k				B_1^k				B_2^k				B_3^k				B_4^k			
$0a$	89	$c1$	85	67	$a7$	78	97	.	.	.	.	ec	$1a$	.	80	db	$a1$	.	77
$d9$	$f9$	$c5$	$e5$	35	99	$a6$	$d9$	.	.	.	.	$0c$	50	.	$c7$	18	$6d$	.	ba
$d8$	$f7$	$f7$	fb	.	.	.	.	.	.	.	.	$3b$	$d7$	.	ef	$a8$	30	.	$4e$
56	$7b$	11	14	$b1$	21	82	fa	.	.	.	.	$b7$	22	.	$e0$	ff	$d5$	.	aa

où B_0^k est le bloc à l'entrée de la ronde, B_4^k est le bloc obtenu à la sortie de la ronde, et les autres blocs sont ceux obtenus lors de tous les calculs intermédiaires de la ronde. Les points dans les blocs représentent les valeurs que vous devrez calculer lors de cet exercice.

La clef utilisée pour cette ronde est : $K^k = \begin{bmatrix} 37 & bb & 38 & f7 \\ 14 & 3d & d8 & 7d \\ 93 & e7 & 08 & a1 \\ 48 & f7 & a5 & 4a \end{bmatrix}$

1. Quelle est la taille du bloc AES dans ce cas ?
2. Quelle est la taille de la clef, sachant que cette ronde est l'une des 10 appliquées lors du chiffrement.
3. Rappeler les fonctions qui sont appliquées sur une ronde d'AES. On donnera leurs noms, et que, comment sont obtenus les blocs B_1^k, B_2^k, B_3^k et B_4^k à partir de ces fonctions.
4. Calculer les éléments manquants du bloc B_1^k.
5. Calculer les éléments manquants du bloc B_2^k.
6. Calculer les éléments manquants du bloc B_3^k.
7. Calculer les éléments manquants du bloc B_4^k.
8. Calculer la clef de ronde de l'étage suivant.

Exercice 5: RSA

On souhaite construire un cryptosystème RSA (n, p, q, a, b).

1. Quelles sont les propriétés que doivent respecter n dans ce cas ?
2. On choisit $p = 7$ et $q = 37$. Vérifier de manière certaine que ces deux nombres sont premiers.
3. Parmi les valeurs suivantes $\{15, 31, 123, 183, 217\}$, choisir l'unique valeur de la clef privée a compatible avec les conditions requises pour son choix. Pour les autres valeurs, on indiquera pourquoi ce choix est inadéquat.
4. En déduire la valeur de clef privée b.
5. Quelles sont les information minimales qui doivent être transmise à un correspondant afin de lui permettre d'effectuer un chiffrement RSA ?
6. Combien de bits peuvent être transmis par un bloc RSA défini ainsi ? Ce nombre de bits sera calculé comme le plus grand nombre de bits possible pouvant être porté par n.

7 Les messages à transmettre sont codés avec l'alphabet $(\mathrm{a}, \mathrm{e}, \mathrm{n}, \mathrm{t})$. De combien de blocs RSA ai-je besoin pour envoyer le message "attentat" ? Donner alors la valeur des blocs correspondant au texte clair en utilisant un codage à taille fixe pour chacune des lettres.

8 Chiffrer les deux premiers bloc du message. Si $b > 10$, on utilisera l'algorithme d'exponentiation modulaire.

9 Décoder le message $\{107, 66\}$ en utilisant la méthode de décodage rapide (= la méthode utilisant les restes chinois).

10 Quel est l'intérêt d'utiliser une hasardisation du message ?

11 Pour l'hasardisation, on veut utiliser les fonctions binaires d'expansion et de condensation suivantes :

- expansion $G : \mathbb{B}^3 \to \mathbb{B}^5$ définie comme $G(b_0b_1b_2) = b_0b_1b_2b_1b_0$.
- condensation $H : \mathbb{B}^5 \to \mathbb{B}^3$ définie comme $H(b_0b_1b_2b_3b_4) = b_0b_1b_2 \oplus b_2b_3b_4$.

En déduire combien de bits seront utilisés par bloc pour la clef aléatoire et le message.

12 Montrer, en hasardisant uniquement le premier bloc de message, qu'en changeant la clef aléatoire, on produit des messages hasardisés différents à partir du même premier bloc du message.

13 Déchiffrer les deux blocs du message hasardisés $\begin{bmatrix} 250 & 43 \end{bmatrix}$. Si $a > 10$, on utilisera l'algorithme d'exponentiation modulaire. On ne calculera à cette question que l'exponentiation modulaire.

14 A partir des résultats des blocs obtenus à la question précédente, déshasardisez chaque bloc.

15 En déduire le message codé transmis dans ces deux blocs.

Exercice 6: Tests de primalité

1 Soit un nombre entier stocké sur n bits. On suppose que le bit de poids le plus fort soit à 1. De combien de chiffres a-t-on besoin pour représenter ce nombre en base 10 ?

2 Appliquer la formule obtenue à la question précédente afin de déterminer le nombre p de chiffres a un nombre entier stocké sur 512 bits.

3 En déduire la borne inférieure du nombre de nombres premiers qui ont exactement 512 chiffres.

4 Tester la primalité de 2821 en effectuant deux fois le test de Fermat (*i.e.* $k = 2$).

5 Tester la primalité de 2821 avec le test de Miller-Rabin.

6 Pour les tests de primalité effectué aux deux questions précédentes, peut-on dire quelque chose sur la chance effective que 2821 soit effectivement premier dans chacun des cas ?

7 Ce résultat aurait-il pu être prévisible ?