Université de Yaoundé 2005–2006

Examen - Cryptographie & Securité Réseau

Sebastien.Varrette@imag.fr

(3 heures) Documents et calculatrices ***autorisés****. Les exercices sont indépendants et peuvent être traités dans n'importe quel ordre. On conseille de ne pas dépasser les indications horaires.*

Exercice 1. *Boites-S de DES (10 min)*

Le tableau 1 rappelle les boites-S de D.E.S. On suppose avoir en entrée de ces boîtes-S la chaine hexadécimale `5055 B1784DCE`. Quelle est la chaîne hexadécimale de sortie des boîtes S ?

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4															
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
S_5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Table 1 – Les boîtes S de DES

Exercice 2. *Chiffrement et signature RSA (30 min)*

1. Rappeler et démontrer le fonctionnement du chiffrement RSA.
2. On souhaite chiffrer le message $M = 14$. Vous avez généré les nombres premiers $p = 19$ et $q = 11$.
   a) Donnez en la justifiant une clef publique découlant de ces valeurs de p et q.
   b) Donnez la valeur du chiffré C de M à partir de votre clef publique.
3. Vous souhaitez maintenant signer numériquement un document M. L'application d'une fonction de hachage H sur ce document a permis d'obtenir le haché $H(M) = 10$. Donnez la valeur de votre signature RSA de $H(M)$. Quelle(s) démarche(s) dois-je effectuer pour vérifier cette signature ?

Exercice 3. *Tunnel SSH (10 min)*
On souhaite réaliser une connection distante sécurisée par un tunnel SSH et automatique (i.e qui ne nécessite pas d'entrer un mot de passe) entre deux machines Linux pour l'utilisateur `toto` (connu sur les deux machines). Expliquer votre démarche.

Exercice 4. *Entropie et chiffrement de Vernam (2h10)*
Le chiffrement de Vernam est très simple. Pour un message M de n bits et une clé K de même longueur, les fonctions de chiffrement et de déchiffrement s'écrivent :

$$\begin{aligned} C &= M \oplus K \\ M &= C \oplus M \end{aligned}$$

Cet exercice a pour objectif de prouver que ce chiffrement est parfait (ou inconditionnellement sûr) i.e que la connaissance du chiffré n'apporte aucune information sur le message émis ou sur la clé utilisée.

Préliminaires

On rappelle d'abord quelques notions sur les probabilités conditionnelles.
– deux évènements sont *indépendants* si $P(A \cap B) = P(A)P(B)$.
– On appelle *probabilité conditionnelle* de l'évènement A par rapport à l'évènement B, la probabilité que A se produise, sachant que B s'est déjà produit. Elle est notée $P(A|B)$ et définie par

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

– La formule dite de Bayes permet de calculer pour un ensemble d'évènements $A_1, \ldots, A_n, B$ les probabilités $P(A_k|B)$ en fonction des $P(B|A_k)$:

$$P(A_k|B) = \frac{P(A_k \cap B)}{P(B)} = \frac{P(B|A_k)P(A_k)}{\sum_i P(B|A_i)P(A_i)}$$

On donne maintenant le lemme de Gibbs qui nous sera utile dans la suite.

Lemme 1 (de Gibbs)**.** *Soient* $(p_1, \ldots, p_n)$, $(q_1, \ldots, q_n)$ *deux lois de probabilité discrètes* ($\sum_{i=1}^{n} p_i = \sum_{i=1}^{n} q_i = 1$)*. Alors :*

$$\sum_{i=1}^{n} p_i * \log \frac{q_i}{p_i} \leq 0 \ .$$

1. Prouver le lemme de Gibbs. On remarquera que $\forall x \in \mathbb{R}_*^+$, $\ln(x) \leq x - 1$
2. On propose le code secret suivant, permettant de chiffrer deux caractères a et b avec trois clefs différentes k_1, k_2 et k_3 :
   – si la clef est k_1 alors $a \to 1$ et $b \to 2$;
   – si la clef est k_2 alors $a \to 2$ et $b \to 3$;
   – sinon $a \to 3$ et $b \to 4$

   On suppose en outre que l'on a des connaissances *a priori* sur le message M envoyé et la clef K utilisée : $P(M = a) = 1/4$; $P(M = b) = 3/4$ et $P(K = k_1) = 1/2$; $P(K = k_2) = P(K = k_3) = 1/4$.
   a) Quelles sont les probabilités d'obtenir les chiffres 1, 2 ou 3 ?
   b) Quelles sont les probabilités conditionnelles que le message soit a ou b sachant la valeur du chiffre ?
   c) Peut-on dire intuitivement si ce code secret est un chiffrement parfait ?

Notion d'entropie

On appelle S l'alphabet du message source. Un message est alors un élément de S^+. Pour tout message, on peut calculer les fréquences d'apparition de chaque élément de l'alphabet, et construire ainsi une distribution de probabilités sur S. Une *source d'information* est constituée du couple $\mathcal{S} = (S, \mathcal{P})$ où $S = \{s_1, \ldots, s_n\}$ est l'alphabet source et $\mathcal{P} = (p_1, \ldots, p_n)$ est une distribution de probabilités sur S, c'est-à-dire que p_i est la probabilité d'occurrence de s_i dans une émission. On peut construire une source d'information à partir de n'importe quel message, en construisant la distribution de probabilités à partir de la fréquence des caractères dans le message. La source $\mathcal{S} = (S, \mathcal{P})$ est dite *sans mémoire* lorsque les événements (occurrences d'un symbole dans une émission) sont indépendants et que leur probabilité reste stable au cours de l'émission.
L'*entropie* d'une source $\mathcal{S} = (S, \mathcal{P})$, $S = (s_1, \ldots, s_n)$, $\mathcal{P} = (p_1, \ldots, p_n)$ est :

$$H(\mathcal{S}) = H(p_1, \ldots, p_n) = -\sum_{i=1}^{n} p_i \log_2(p_i) \ = \sum_{i=1}^{n} p_i \log_2(\frac{1}{p_i}) \ .$$

On désigne par extension l'entropie d'un message comme l'entropie de la source induite par ce message, la distribution de probabilités étant calculée à partir des fréquences d'apparition des caractères dans le message.

1. Soit $\mathcal{S} = (S, \mathcal{P})$ une source. Montrer que $0 \leq H(\mathcal{S}) \leq \log_2 n$ (on utilisera le lemme de Gibbs sur une distribution appropriée).
2. Pour quelle distribution de probabilité l'entropie est-elle maximale ? Justifier alors la désignation de l'entropie comme une “mesure du désordre”

(en supposant que le plus grand désordre est atteint par la distribution uniforme)

3. Quelle est l'entropie d'une source qui émet un caractère 1 avec une probabilité 0.1 et le caractère 0 avec une probabilité 0.9 ?

Entropies conjointe et conditionnelle

On étend facilement la définition de l'entropie à plusieurs sources. Soient $\mathcal{S}_1 = (S_1, P_1)$ et $\mathcal{S}_2 = (S_2, P_2)$ deux sources sans mémoire, dont les évènements ne sont pas forcément indépendants. On note $S_1 = (s_{11}, \ldots, s_{1n})$ et $S_2 = (s_{21}, \ldots, s_{2m})$, et $p_{i,j}$ la probabilité d'occurrence conjointe de s_{1i} et s_{2j}.
On appelle l'*entropie conjointe* de $\mathcal{S}_1$ et $\mathcal{S}_2$ la quantité

$$H(\mathcal{S}_1, \mathcal{S}_2) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p_{i,j} \log_2(p_{i,j})$$

si les évènements de $\mathcal{S}_1$ et $\mathcal{S}_2$ ne sont pas indépendant, on calcule alors l'*entropie conditionnelle* de $\mathcal{S}_1$ relativement à la valeur de $\mathcal{S}_2$ par

$$H(\mathcal{S}_1|\mathcal{S}_2 = s_{2j}) = -\sum_{i=1}^{n} p_{i,j} \log_2(p_{i,j})$$

Enfin, on étend cette notion à une entropie conditionnelle de $\mathcal{S}_1$ connaissant $\mathcal{S}_2$, qui est la quantité d'information restant dans $\mathcal{S}_1$ si la loi de $\mathcal{S}_2$ est connue :

$$H(\mathcal{S}_1|\mathcal{S}_2) = -\sum_{j=1}^{m} p_j H(\mathcal{S}_1|\mathcal{S}_2 = s_{2j})$$

1. Montrer que $H(\mathcal{S}_1) \geq H(\mathcal{S}_1|\mathcal{S}_2)$ avec égalité si et seulement si $\mathcal{S}_1$ et $\mathcal{S}_2$ sont indépendantes.
2. Montrer que $H(\mathcal{S}_1, \mathcal{S}_2) = H(\mathcal{S}_2) + H(\mathcal{S}_1|\mathcal{S}_2)$.

Cette notion est cruciale en cryptographie. En effet, il est très important que tous les messages cryptés aient une entropie forte, pour ne pas que les traces d'organisation dans un message donnent des informations sur la manière dont il a été crypté.

Chiffrement parfait et entropie

Un chiffrement est *parfait* si le message chiffré C ne fournit aucune information sur le message initial M ni sur la clef K : en terme d'entropie, on aura donc :

$$H(M|C) = H(M) \text{ et } H(K|C) = H(K)$$

.

1. Rappelez les conditions évoquées en cours permettant d'assurer que le chiffrement de Vernam est parfait (ou inconditionnellement sûr).
2. En utilisant uniquement les entropies conditionnelles et la définition du chiffrement de Vernam, démontrer que dans Vernam, H(M) = H(C).
3. En déduire que chiffrement à clef jetable de Vernam est un chiffrement parfait.