Chiffrements classiques

Rappelons la correspondence entre l'alphabet classique et les entiers $\{0, \dots, 25\}$:

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

Pour les exercises suivants, nous prenons le message $M =$ `LESMAISONSBLANCHES`.

1. Soit $K =$ `ULOIDTGKXYCRHBPMZJQVWNFSAE` une clé de substitution. En rappelant l'application induit par la clé :

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
  ↓          ···         ↓
ULOIDTGKXYCRHBPMZJQVWNFSAE
```

trouver le chiffrement de M. Quelles proprietés du texte clair et du texte chiffré restent inchangées par un chiffrement à substitution ?

2. Trouver le chiffrement de M par transposition avec la clé `[3,5,2,6,1,4]`. Quelles proprietés du texte clair et du texte chiffré restent inchangées par un chiffrement à substitution ?

3. Trouver le chiffrement de M par un chiffrement de Vigenère avec la clé `SECURITE`. Qu'est-ce se passe au fréquences des caractères dans un texte chiffré avec un chiffrement de Vigenère ?

Protocoles d'échange de message

Alice veut envoyer à Bob le message $M \in \mathbb{F}_2^n$.

4. Alice et Bob partagent une clé secrète $K \in \mathbb{F}_2^n$. Ils effectuent le protocole suivant :
— Alice envoie $C = M \oplus K$ à Bob.
— Bob calcule $M = C \oplus K$.
Montrer que $C \oplus K$ est bien le message M.

5. Alice possède une clé secrète $K \in \mathbb{F}_2^n$ et Bob une clé $L \in \mathbb{F}_2^n$.

Ils effectuent le protocole suivant :
— Alice envoie $C_1 = M \oplus K$ à Bob.
— Bob envoie $C_2 = C_1 \oplus L$ à Alice.
— Alice envoie $C_3 = C_2 \oplus K$ à Bob.
Montrer que Bob peut retrouver le message, mais en interceptant tous les échanges, un interlocuteur Oscar peut également retrouver M.

Probabilités

Nous allons étudier la sécurité de Shannon pour les cryptosystèmes symétriques. On suppose que les ensembles $\mathcal{K}$ et $\mathcal{M}$ sont donnés avec des fonctions de probabilité notées respectivement $p_{\mathcal{M}}$ et $p_{\mathcal{K}}$. On note alors $p_{\mathcal{K}\times\mathcal{M}}$ la fonction de probabilité produit :

$$p_{\mathcal{K}\times\mathcal{M}}((K,M)) = p_{\mathcal{K}}(K)\, p_{\mathcal{M}}(M)$$

sur $\mathcal{K}\times\mathcal{M}$. Pour un cryptosystème $\mathcal{E} : \mathcal{K}\times\mathcal{M} \to \mathcal{C}$ on définit une probabilité jointe sur $\mathcal{M}\times\mathbb{C}$ par :

$$p_{\mathcal{M}\times\mathbb{C}}(M,C) = \sum_{\substack{K\in\mathcal{K}\\ E_K(M)=C}} p(K)\, p(M),$$

et on en déduit une probabilité sur $\mathcal{C}$:

$$p_{\mathcal{C}}(C) = \sum_{M\in\mathcal{M}} p_{\mathcal{M}\times\mathcal{C}}(M,C).$$

Pour un espace de probabilité $\mathcal{X}$ on définit son *support* $\mathrm{supp}(p_{\mathcal{X}}) = \{x \in \mathcal{X} \mid p_{\mathcal{X}}(x) \neq 0\}$. Pour pour tout C dans $\mathrm{supp}(p_{\mathcal{C}})$, on en déduit également une probabilité relative

$$p(M|C) = \frac{p_{\mathcal{M}\times\mathbb{C}}(M,C)}{p_{\mathcal{C}}(C)}.$$

Pour simplifier les notations, on écrira simplement p pour ces probabilités si le domaine de la fonction est clair.

6. Si $\mathcal{M} = \mathrm{supp}(p_{\mathcal{M}})$ et $\mathcal{K} = \mathrm{supp}(p_{\mathcal{K}})$, et si le cryptosystème $\mathcal{E}$ est surjectif,[1] montrer que $\mathcal{C} = \mathrm{supp}(p_{\mathcal{C}})$.

7. On dit qu'un cryptosystème symétrique est *parfaitement sûr* si pour tout $C \in \mathrm{supp}(p_{\mathcal{C}})$ et $M \in \mathcal{M}$, $p(M|C) = p(M)$. Justifier la dénomination, et montrer l'equivalence des conditions :
- Le cryptosystème est parfaitement sûr.
- La probabilité $p_{\mathcal{M}\times\mathcal{C}}$ est la probabilité produit.
- L'information mutuelle[2] $I(\mathcal{M},\mathcal{C}) = 0$.

8. Si $\mathcal{C} = \mathrm{supp}(p_{\mathcal{C}})$ et le système est parfaitement sûr, montrer que $|\mathcal{K}| \geq |\mathcal{C}| \geq |\mathcal{M}|$.

9. On suppose maintenant que $\mathcal{M} = \mathrm{supp}(p_{\mathcal{M}})$, $\mathcal{C} = \mathrm{supp}(p_{\mathcal{C}})$ et $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{M}|$. Montrer que le cryptosystème est parfaitement sûr si et seulement si
- toutes les clés ont la même probabilité ; et
- pour tout $M \in \mathcal{M}$ et $C \in \mathcal{C}$ il existe une unique clé K satisfaisant $E_K(M) = C$.

10. On reprend le cryptosystème de l'exercise 4 en supposant que $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{F}_2^n$, $\mathcal{M} = \mathrm{supp}(p_{\mathcal{M}})$ et $p_{\mathcal{K}}(K) = 1/|\mathcal{K}|$ pour tout K (on tire aléatoirement les clés dans $\mathcal{K}$), et $E_K(M) = M \oplus K$. Montrer qu'un tel système est parfaitement sûr. Quels sont ses inconvénients ?

1. Un cryptosystème $\mathcal{E} = \{E_K \mid K \in \mathcal{K}\}$ est surjectif si et seulement si $\mathcal{C} = \bigcup_{K\in\mathcal{K}} E_K(\mathcal{M})$.

2. On rappelle que $I(\mathcal{X},\mathcal{Y}) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2\left(\frac{p(x,y)}{p(x)p(y)}\right) = H(\mathcal{X}) - H(\mathcal{X}|\mathcal{Y}) = H(\mathcal{Y}) - H(\mathcal{Y}|\mathcal{X})$.