HAI709I — TDs

Ivan Lejeune

1er décembre 2025

Table des matières

TD1 — Introduction

Exercice 1.1. Répondez aux questions suivantes :

- Supposons qu'un adversaire sache qu'un message, chiffré avec le chiffrement par décalage, est soit **aaa**, **aab**, **aac**, **abc**, **acd** soit **abd**. En examinant le texte chiffré obtenu, est-il (toujours) en mesure de déterminer le message d'origine ? Expliquez votre réponse : fournissez une stratégie si la réponse est correcte ou un contre-exemple (une clé) si elle ne l'est pas.
- Considérez le point précédent, mais cette fois-ci, le message est chiffré avec le chiffrement de Vigenère. Supposons d'abord que la période soit 2, puis que la période soit 3. Est-il (toujours) en mesure de déterminer le message d'origine ?
- Cette fois-ci, les messages possibles, chiffrés avec le chiffrement de Vigenère de période 2, sont soit **abcd**, **aabc** soit **bccd**. L'adversaire est-il capable de déterminer le texte en clair à partir du texte chiffré ? Pourquoi ?

Solution.

- Oui, il est toujours en mesure de déterminer le message d'origine. En effet, il suffit de décaler toutes les lettres du texte chiffré jusqu'à obtenir un des messages possibles. Comme les messages possibles ne peuvent pas être obtenus par décalage les uns des autres, il y a une et une seule possibilité.
- Non, il n'est pas toujours en mesure de déterminer le message d'origine. Si 2 messages partagent les mêmes lettres aux positions 1 et 3 (pour la période 2) alors ce n'est pas possible.
- Oui, facile, regarder les écarts entre les paires.

Exercice 1.2. Nous chiffrons le message abacbc avec le chiffrement de Vigenère et une clé de période 2. Trouvez une clé telle que le texte chiffré contienne exactement 4 fois le caractère c. Existe-t-il une clé pour laquelle le caractère c apparaît plus de 4 fois dans le texte chiffré ? Et pour les autres caractères ?

Solution. Oui, pour obtenir exactement 4 fois un caractère donné, on peut utiliser le chiffrement suivant :

- Pour c : la clé est $(2, 0)$
- Pour toute autre lettre, la clé est celle du c décalée de la différence entre c et la lettre voulue.

Ce n'est pas possible d'avoir plus de 4 fois un caractère dans le texte chiffré.

Exercice 1.3. Montrer que les chiffrements par décalage et par substitution mono-alphabétique ne sont pas inconditionnellement sûrs.

Solution. Le mot *aaa* a une probabilité non nulle d'être encodée en *bbb* avec le chiffrement par décalage ou par substitution mono-alphabétique. Ce n'est en revanche pas le cas du mot *aab*. Donc les deux chiffrements ne sont pas inconditionnellement sûrs.

□

Exercice 1.4. A partir de la définition de la sécurité inconditionnelle que nous avons donnée, prouver la proposition vue pendant le cours :

Proposition. Un schéma de chiffrement $(\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ avec un espace de messages M est inconditionnellement sûr si et seulement si, pour chaque $m, m' \in M$ et chaque $c \in C$, on a

$$\mathbb{P}(\mathsf{enc}_K(m) = c) = \mathbb{P}(\mathsf{enc}_K(m') = c).$$

Solution. Exercice solution

Exercice 1.5.

Solution. Exercice solution

Exercice 1.6 Optional title 2. Exercise 2 content

Solution. Exercice solution

Exercice 1.7 Optional title 2. Exercise 2 content

Solution. Exercice solution

TD2

Exercice 2.1. Dire si les fonctions suivantes sont :

- bornées par un polynôme :

$$f_1(n) = n, \quad f_2(n) = n^3 - 4n^2 + 2n + 9, \quad f_3(n) = n\log_2(n),$$
$$f_4(n) = 1.1^n, \quad f_5(n) = 2^{\frac{1}{2}n}, \quad f_6(n) = 2^{\sqrt{n}}, \quad f_7(n) = n^{\log_2(n)}$$

- négligeables :

$$g_1(n) = \frac{1}{n^2+n+1}, \quad g_2(n) = \frac{3}{\log_2(n)}, \quad g_3(n) = 2^{-n},$$
$$g_4(n) = 2^{-\frac{1}{2}n}, \quad g_5(n) = \frac{n^2+n+1}{e^n}, \quad g_6(n) = 2^{-\sqrt{n}}, \quad g_7(n) = n^{-\log_2(n)}$$

Solution.

- On a
  - $f_1 = n$ est bornée par n^2,
  - $f_2 = n^3 - 4n^2 + 2n + 9$ est bornée par n^4,
  - $f_3 = n\log_2(n)$ est bornée par n^2,
  - $f_4 = 1.1^n$ n'est pas bornée par un polynôme,
  - $f_5 = 2^{\frac{1}{2}n}$ n'est pas bornée par un polynôme,
  - $f_6 = 2^{\sqrt{n}}$ n'est pas bornée par un polynôme,
  - $f_7 = n^{\log_2(n)}$ n'est pas bornée par un polynôme.
- On a
  - $g_1(n) = \frac{1}{n^2+n+1}$ n'est pas négligeable,
  - $g_2(n) = \frac{3}{\log_2(n)}$ n'est pas négligeable,
  - $g_3(n) = 2^{-n}$ est négligeable par rapport à $\frac{1}{n}$,
  - $g_4(n) = 2^{-\frac{1}{2}n}$ est négligeable par rapport à $\frac{1}{n}$,
  - $g_5(n) = \frac{n^2+n+1}{e^n}$ est négligeable par rapport à $\frac{1}{n}$,
  - $g_6(n) = 2^{-\sqrt{n}}$ est négligeable par rapport à $\frac{1}{n}$,
  - $g_7(n) = n^{-\log_2(n)}$ est négligeable par rapport à $\frac{1}{n}$,

Exercice 2.2. Considérons un chiffrement de Vigenère π où l'espace de messages est constitué de toutes les chaînes de 3 caractères et gen fonctionne de la manière suivante : d'abord, une période t est tirée uniformément au hasard dans $1, 2, 3$, puis une clé k est tirée uniformément au hasard dans $0, ..., 25^t$.

- Définissez un adversaire $\mathcal{A}$ tel que $\mathbb{P}(\text{PrivK}^{eav}_{\mathcal{A},\Pi} = 1) > \frac{1}{2}$.
- Définissez un adversaire $\mathcal{A}$ tel que $\mathbb{P}(\text{PrivK}^{eav}_{\mathcal{A},\Pi} = 1) \geq \frac{3}{4}$.

Solution. On a

$$\begin{aligned}
&\mathbb{P}(\text{PrivK}^{eav}_{\mathcal{A},\Pi} = 1) \\
=&\mathbb{P}(b' = b) \\
=&\sum_{i=1}^{3} \mathbb{P}(t = i) \cdot \mathbb{P}(b' = b \mid t = i) \\
=&\frac{1}{3}\sum_{i=1}^{3} \mathbb{P}(b' = b \mid t = i)
\end{aligned}$$

$\mathcal{A}$ recoit c_1, c_2, c_3, choisit $m_0 = (0,0,0)$ et $m_1 = (0,1,2)$ et produit $b' = 0$. Si $c_1 = c_2$ ou $c_2 = c_3$, alors, pour $t = 1$:

$$\begin{aligned}\mathbb{P}(b' = b \mid t = 1) &= \mathbb{P}(b = 0) \cdot \mathbb{P}(b' = 0 \mid t = 1 \wedge b = 0) \\ &+ \mathbb{P}(b = 1) \cdot \mathbb{P}(b' = 1 \mid t = 1 \wedge b = 1) \\ &= \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 \\ &= 1,\end{aligned}$$

pour $t = 2$:

$$\begin{aligned}\mathbb{P}(b' = b \mid t = 2) &= \mathbb{P}(b = 0) \cdot \mathbb{P}(b' = 0 \mid t = 2 \wedge b = 0) \\ &+ \mathbb{P}(b = 1) \cdot \mathbb{P}(b' = 1 \mid t = 2 \wedge b = 1) \\ &= \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \left(1 - \frac{1}{26}\right) \\ &= \frac{51}{52},\end{aligned}$$

pour $t = 3$:

$$\begin{aligned}\mathbb{P}(b' = b \mid t = 3) &= \mathbb{P}(b = 0) \cdot \mathbb{P}(b' = 0 \mid t = 3 \wedge b = 0) \\ &+ \mathbb{P}(b = 1) \cdot \mathbb{P}(b' = 1 \mid t = 3 \wedge b = 1) \\ &= \frac{1}{2} \cdot p + \frac{1}{2} \cdot (1 - p) \\ &= \frac{1}{2}.\end{aligned}$$

Ce qui donne

$$\begin{aligned}\mathbb{P}(\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi} = 1) &= \frac{1}{3} \sum_{i=1}^{3} \mathbb{P}(b' = b \mid t = i) \\ &= \frac{1}{3} \cdot 1 + \frac{1}{3} \cdot \frac{51}{52} + \frac{1}{3} \cdot \frac{1}{2} \\ &= \frac{1}{3} + \frac{1}{3} + \frac{1}{3} \cdot 12 = \frac{5}{6} > \frac{3}{4}\end{aligned}$$

Exercice 2.3. Soit G un PRG avec un facteur d'expansion $l(n) > 2n$. Dans chacun des cas suivants, prouver que G' est aussi un PRG, si tel est le cas. Sinon, trouver un contre-exemple.

- Définissez $G' \stackrel{\text{def}}{=} G(s_1, \ldots, s_{\lceil \frac{n}{4} \rceil})$, où $s = s_1, \ldots s_n$.
- Définissez $G' \stackrel{\text{def}}{=} G(s_1, \ldots, s_{\lceil \frac{n}{2} \rceil})$, où $s = s_1, \ldots s_n$.
- Définissez $G' \stackrel{\text{def}}{=} G(s \,\|\, 0^{|s|})$.

Exercice 2.4. TO FILL

Solution. TO FILL

Exercice 2.5. TO FILL

Solution. TO FILL

TD3

Exercice 3.1.

Solution.

- On a la chaine suivante :

$$\begin{array}{c} 1000 \\ 1100 \\ 0110 \\ 1011 \\ 1101 \\ 0110 \\ 1011 \\ 1101 \\ 0110 \end{array}$$

  Où on peut remarquer que la période est de 3. On ne parcourt pas les 15 combinaisons donc elle n'est pas de longueur maximale.
- La longueur est de 15 et elle est maximale.

Exercice 3.2.

Solution.

- Avec $g(S_{n-1}, \dots, S_0) = S_0 \wedge S_1$, on a

$$\mathbb{P}(g(\cdots) = 0) = \frac{3}{4}, \quad \mathbb{P}(g(\cdots) = 1) = \frac{1}{4}$$

  ce qui n'est pas uniforme donc ce g n'est pas un bon générateur pseudo-aléatoire.
- Avec $g(S_{n-1}, \dots, S_0) = (S_0 \wedge S_1) \oplus S_2$, on a

$$\mathbb{P}(g = 0) = \mathbb{P}(S_2 = 0) \cdot \frac{3}{4} + \mathbb{P}(S_2 = 1) \cdot \frac{1}{4} = \frac{1}{2}$$
$$\mathbb{P}(g = 1) = \frac{1}{2}$$

  ce qui n'est pas uniforme donc ce g n'est pas un bon générateur pseudo-aléatoire.

Exercice 3.3.

Solution.

- A l'etape 1, on a :

$$\begin{aligned} \mathbb{P}(S_0[2] = 0 \wedge S_0[1] \neq 2) &= \frac{1}{256} \cdot \left(1 - \frac{1}{255}\right) \\ &= \frac{254}{256 \cdot 255} \end{aligned}$$

- A l'étape 2, on a :

$$\begin{array}{l} S_0[2] = 0, S_0[1] \neq 2 \\ i = 1, J = S_0[1] = X \\ S_1[1] = S_0[J] = S_0[X] \\ S_1[X] = S_0[1] = X \end{array}$$

- A l'étape 3, on a :

$$\begin{aligned} i = 2, J &= X + S_1[2] \\ &= X + S_0[2] \\ &= X + 0 \\ &= X \end{aligned}$$

  et

$$\begin{aligned} S_2[2] &= S_1[X] = X \\ S_2[X] &= S_1[2] = 0 \\ t &= S_2[1] + S_2[J] = X + 0 = X \\ Y &= S_2[t] = S_2[X] = 0 \end{aligned}$$

- On en déduit que le 2e octet de la clé est 0. De plus, on a une probabilité uniforme sur cet octet.
- On en conclut que le 2e octet est biaisé avec probabilité $\frac{1}{128} > \frac{1}{256}$.

TD5

Exercice 5.1. Soit $k \in \{0,1\}^n$ la clé d'un MAC. Prouvez que, si la longueur de l'étiquette

$$t(n) = \mathsf{O}(\log n),$$

alors le MAC n'est pas sûr (c'est-à-dire, qu'un MAC sûr doit toujours avoir un $t(n)$ super-logarithmique).

Solution. On peut faire une attaque par force brute. On prend (m,t) au hasard et m admet au moins une étiquette.

$$\mathbb{P}(\mathsf{Vrfy}_k(m,t) = 1) \geq \frac{1}{2^{\mathsf{O}(\log n)}} = \frac{1}{\mathsf{poly}(n)}.$$

Exercice 5.2.

1. Ecrivez formellement l'expérience correspondant à l'infalsifiabilité forte d'un MAC à partir de celle de l'infalsifiabilité.
2. Prouvez la proposition vue en cours :

   Proposition. Un MAC déterministe sûr avec vérification canonique est fortement sûr.

Solution.

1.
2. Il y a 2 cas de réussite pour l'adversaire :
   (a) Il produit (m,t) tel que $\forall (m',t') \in Q$ avec $m' \neq m$,

   $$\mathbb{P}(\mathsf{Vrfy}_k(m,t) = 1) \leq \mathsf{negl}(n).$$

   car MAC est sûr.
   (b) Il produit (m,t) tel que $\exists (m,t') \in Q$ avec $t' \neq t$,

   $$\mathbb{P}(\mathsf{Vrfy}_k(m,t) = 1) = 0.$$

   Donc

   $$\mathbb{P}_{\text{tot}} = \mathbb{P}_1 + \mathbb{P}_2 \leq \mathsf{negl}(n).$$

   Donc le MAC est fortement sûr.

Exercice 5.3. Considérons le MAC suivant pour des messages de longueur $l(n) = 2n-2$ utilisant une PRF F.
En entrée, un message $m_0||m_1$ avec $|m_0| = |m_1| = n-1$ et une clé $k \in \{0,1\}^n$, le MAC produit

$$t = F_k(0||m_0)||F_k(1||m_1).$$

La vérification est canonique. Le MAC est-il sûr ?

Solution. On a

$$\mathsf{Mac}_k(m_0||m_1) = F_k(0||m_0)||F_k(1||m_1).$$

L'adversaire peut utiliser la stratégie suivante :

1. Il demande l'étiquette de $m_0||m_{i\neq 1}$ à l'oracle et reçoit $t_1||t_2$.
2. Il demande l'étiquette de $m_{j\neq 0}||m_1$ à l'oracle et reçoit $t_3||t_4$.
3. Il produit $(m_0||m_1, t_1||t_4)$.

Exercice 5.4. Montrez que les MAC suivants ne sont pas sûrs même s'ils sont utilisés pour authentifier des messages de longueur fixe. Dans chaque cas, F est une PRF, la clé $k \in \{0,1\}^n$ est choisie au hasard et $\langle i \rangle$ désigne l'entier i encodé sous forme de chaîne de $\frac{n}{2}$ bits.

1. L'étiquette de $m = m_1, \ldots, m_l$ avec $m_i \in \{0,1\}^n$ est $t \coloneqq F_k(m_1) \oplus \cdots \oplus F_k(m_l)$.
2. L'étiquette de $m = m_1, \ldots, m_l$ avec $m_i \in \{0,1\}^{\frac{n}{2}}$ est $t \coloneqq F_k(\langle 1 \rangle || m_1) \oplus \cdots \oplus F_k(\langle l \rangle || m_l)$.
3. L'étiquette de $m = m_1, \ldots, m_l$ avec $m_i \in \{0,1\}^{\frac{n}{2}}$ est r, t où r est choisi uniformément dans $\{0,1\}^n$ et
$$t \coloneqq F_k(r) \oplus F_k(\langle 1 \rangle || m_1) \oplus \cdots \oplus F_k(\langle l \rangle || m_l).$$

Solution.

1. Pour $m = m_1, \ldots, m_l$ on a
$$\mathsf{Mac}_k(m) = F_k(m_1) \oplus \cdots \oplus F_k(m_l).$$
où $|\mathsf{Mac}_k(m)| = n \neq |m|$. L'adversaire peut utiliser la stratégie suivante :
   (a) Il donne $m_1 || m_2$ à l'oracle et reçoit $t = F_k(m_1) \oplus F_k(m_2)$. avec $m_1 \neq m_2$.
   (b) Il produit $((m_2 || m_1), t)$

   Ainsi,
$$\mathbb{P}(\mathsf{Vrfy}_k(m_2 || m_1, t) = 1) = 1.$$
2. Pour $m = m_1, \ldots, m_l$ on a
$$\mathsf{Mac}_k(m) = \bigoplus_{i=1}^{l} F_k(\langle i \rangle || m_i).$$
où $|\mathsf{Mac}_k(m)| = n \neq |m|$. L'adversaire peut utiliser la stratégie suivante dans le cas $l = 2$:
   (a) Il donne $m_1 || m_2$ à l'oracle et reçoit $t_1 = F_k(\langle 1 \rangle || m_1) \oplus F_k(\langle 2 \rangle || m_2)$.
   (b) Il donne $m_3 || m_4$ à l'oracle et reçoit $t_2 = F_k(\langle 1 \rangle || m_3) \oplus F_k(\langle 2 \rangle || m_4)$.
   (c) Enfin, il donne $m_1 || m_4$ à l'oracle et reçoit $t_3 = F_k(\langle 1 \rangle || m_1) \oplus F_k(\langle 2 \rangle || m_4)$.
   (d) Alors, il obtient
$$t_1 \oplus t_2 \oplus t_3 = F_k(\langle 1 \rangle || m_3) \oplus F_k(\langle 2 \rangle || m_2).$$
   donc il peut identifier $m_3 || m_2$ avec cette étiquette.

   Donc
$$\mathbb{P}(\mathsf{Vrfy}_k(m_3 || m_2, t_1 \oplus t_2 \oplus t_3) = 1) = 1.$$

Exercice 5.5. Prouvez que les modifications suivantes du CBC-MAC ne permettent pas d'obtenir un MAC sûr (même pour des messages de longueur fixe) :

1. Mac produit tous les blocs $t_1, \ldots, t_l$ au lieu de seulement t_l. La vérification ne controle que t_l.
2. Au lieu de $t_0 = 0^n$, un bloc initial aléatoire t_0 est utilisé à chaque fois qu'un message est authentifié. Ainsi, pour le message $t_0, m_1, \ldots, m_l$, affichez (t_0, t_l) comme étiquette. La vérification est canonique.

Solution.