TD 2 Cryptographie CSI 2024 – 2025

Léo Colisson Palais

Exercice 1: PRF pseudo-OTP est IND-CPA sécurisé (vu dans le cours)

Soit F une PRF sécurisée. On définit le chiffrement PRF pseudo-OTP comme $\mathcal{K} = \{0,1\}^\lambda$, $\mathcal{M} = \{0,1\}^{\text{out}}$, $\mathcal{C} = \{0,1\}^\lambda \times \{0,1\}^{\text{out}}$, et:

$\Sigma_{\text{prf-pseudo-OTP}}$

$\mathsf{Gen}()$:
  $k \xleftarrow{\$} \{0,1\}^\lambda$
  return k
$\mathsf{Enc}(k, m)$:
  $r \xleftarrow{\$} \{0,1\}^\lambda$
  $x := F(k,r) \oplus m$
  return (r, x)
$\mathsf{Dec}(k, c)$:
  $m := F(k,r) \oplus c$
  return m

(1)

Prouve que ce chiffrement est IND-CPA secure.

Indice: Vous devez utiliser (dans cet ordre): la définition (bien sûr), le fait que F est une PRF (définition encore) le théorème du paradoxe des anniversaires asymptotique, quelques simplifications, et reconnaître un chiffrement OTP.

Exercice 2: Modes block-cipher et attaque des anniversaires

1. Nous avons vu dans le cours que le mode CBC n'est pas parallelizable. Mais est-ce le cas pour le chiffrement ET le déchiffrement ?

2. Supposons qu'au lieu d'utiliser le mode CBC sur a block cipher, nous utilisons le one-time pad. Autrement dit, nous remplaçons chaque occurrence de $F(k,\cdot)$ avec $k \oplus \cdot$ dans le code du chiffrement CBC. Montrer que ce chiffrement n'est pas CPA sécurisé. Exhibe un distingueur et calcule son avantage.

3. (a) En mode CBC, si deux blocs de deux textes chiffrés (possiblement différents) sont égaux, c'est-à-dire $c_i = c'_j$, que pouvez-vous dire sur la relation entre les messages originaux ?
   (b) Quelle est la probabilité de trouver deux blocs identiques ? (Vous pouvez utiliser un raisonnement heuristique.)
   (c) Trouvez une attaque contre IND-CPA s'exécutant en temps $O(2^{\mathsf{blen}/2})$.

Exercice 3: Attaque du padding oracle

Implémenter (dans moodle) l'attaque du padding oracle.

Exercice 4: Essayer de protéger le IV : mauvaise idée

Les implémenteurs sont parfois prudents avec les IV dans les modes de chiffrement par bloc et peuvent essayer de les "protéger". Une idée pour protéger un IV est d'éviter qu'il apparaisse directement dans le texte chiffré. Le chiffrement CBC modifié ci-dessous passe le IV à travers le chiffrement par bloc avant de l'inclure dans le texte chiffré :

$$\begin{array}{l}\underline{\mathsf{Enc}(k, m_1\|\cdots\|m_\ell):}\\ \quad c_0 \leftarrow \{0,1\}^{\mathsf{blen}}\\ \quad c'_0 := F(k, c_0)\\ \quad \textbf{for } i \textbf{ in } [1,\ldots,\ell]:\\ \quad\quad c_i := F(k, m_i \oplus c_{i-1})\\ \quad \textbf{return } c'_0\|c_1\|\cdots\|c_\ell\end{array} \tag{2}$$

- Comment définir l'algorithme de déchiffrement (avec la clé) de ce chiffrement ?
- Montrez que ce chiffrement n'est pas sûr contre les attaques CPA.

Exercice 5: Insecure modes

Voici plusieurs modes de chiffrement par blocs, appliqués à une PRP F avec une taille de bloc $\mathsf{blen} = \lambda$. Pour chacun de ces modes :

- Décrivez la procédure de déchiffrement correspondante.
- Montrez que le mode ne possède **pas** la sécurité CPA. C'est-à-dire, décrivez un distingueur et calculez son avantage.

1.
$$\begin{array}{l}\underline{\mathsf{Enc}(k, m_1\|m_2\|\cdots\|m_\ell):}\\ \quad r_0 \leftarrow \{0,1\}^\lambda\\ \quad c_0 := r_0\\ \quad \textbf{for } i \textbf{ in } [1,\ldots,\ell]:\\ \quad\quad r_i := F(k, m_i)\\ \quad\quad c_i := r_i \oplus r_{i-1}\\ \quad \textbf{return } c_0\|\cdots\|c_\ell\end{array}$$

2.
$$\begin{array}{l}\underline{\mathsf{Enc}(k, m_1\|\cdots\|m_\ell):}\\ \quad c_0 \leftarrow \{0,1\}^\lambda\\ \quad \textbf{for } i \textbf{ in } [1,\ldots,\ell]:\\ \quad\quad c_i := F(k, m_i) \oplus c_{i-1}\\ \quad \textbf{return } c_0\|\cdots\|c_\ell\end{array}$$

3.
$$\begin{array}{l}\underline{\mathsf{Enc}(k, m_1\|\cdots\|m_\ell):}\\ \quad c_0 \leftarrow \{0,1\}^\lambda\\ \quad m_0 := c_0\\ \quad \textbf{for } i \textbf{ in } [1,\ldots,\ell]:\\ \quad\quad c_i := F(k, m_i) \oplus m_{i-1}\\ \quad \textbf{return } c_0\|\cdots\|c_\ell\end{array}$$

4.
$$\begin{array}{l}\underline{\mathsf{Enc}(k, m_1\|\cdots\|m_\ell):}\\ \quad c_0 \leftarrow \{0,1\}^\lambda\\ \quad r_0 := c_0\\ \quad \textbf{for } i \textbf{ in } [1,\ldots,\ell]:\\ \quad\quad r_i := r_{i-1} \oplus m_i\\ \quad\quad c_i := F(k, r_i)\\ \quad \textbf{return } c_0\|\cdots\|c_\ell\end{array}$$

Le mode (a) est similaire au mode CBC, sauf que le XOR a lieu après, plutôt qu'avant, l'application du chiffre par bloc. Le mode (c) est essentiellement équivalent au déchiffrement CBC.