TD 2 Crytography Engineering

Léo Colisson Palais

Exercice 1: PRF pseudo-OTP is IND-CPA secure (statement seen in the course)

Let F be a secure PRF. We define the PRF pseudo-OTP encryption scheme as $\mathcal{K} = \{0,1\}^\lambda$, $\mathcal{M} = \{0,1\}^{\text{out}}$, $\mathcal{C} = \{0,1\}^\lambda \times \{0,1\}^{\text{out}}$, and:

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

$\mathsf{Gen}()$:
  $k \xleftarrow{\$} \{0,1\}^\lambda$
  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)

Prove that the PRF pseudo-OTP is IND-CPA secure.

Hint: You should use, in order: (of course) the definitions, the fact that F is a PRF (cf definition), the asymptotic birthday paradox theorem, some simplifications, and realize that you recover, basically, an OTP encryption.

Exercice 2: Block-cipher modes and birthday attack

1. We said in the course that the CBC mode is not parallelizable. But are both encryption and decryption hard to parallelize?

2. Suppose that instead of applying CBC mode to a block cipher, we apply it to one-time pad. In other words, we replace every occurrence of $F(k,\cdot)$ with $k \oplus \cdot$ in the code for CBC encryption. Show that the result does not have CPA security. Describe a distinguisher and compute its advantage.

3. (a) In CBC mode, if two blocks of two (possibly different) ciphertexts are equal, i.e. $c_i = c'_j$, what can you state on the relation between the original messages?
   (b) What is the probability of finding two identical blocks? (You can use a heuristic argument.)
   (c) Find an attack against IND-CPA running in time $O(2^{\mathsf{blen}/2})$.

Exercice 3: Trying to protect the IV: bad idea

Implementers are sometimes cautious about IVs in block cipher modes and may attempt to "protect" them. One idea for protecting an IV is to prevent it from directly appearing in the ciphertext. The modified CBC encryption below sends the IV through the block cipher before including it in the ciphertext:

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

- How do you define the decryption in this scheme ?
- Show that this new scheme is not CPA-secure.

Exercice 4: Insecure modes

Below are several block cipher modes for encryption, applied to a PRP F with blocklength $\mathsf{blen} = \lambda$. For each of the modes:

- Describe the corresponding decryption procedure.
- Show that the mode does **not** have CPA-security. That means describe a distinguisher and compute its advantage.

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

Mode (a) is similar to CBC, except the XOR happens after, rather than before, the block cipher application. Mode (c) is essentially the same as CBC decryption.