TD 1 Crytography Engineering

Léo Colisson Palais

Exercice 1:

1. Compute $\Pr[\mathcal{A}_1 \diamond \mathcal{L}_1 = \mathsf{true}]$, $\Pr[\mathcal{A}_1 \diamond \mathcal{L}_2 = \mathsf{true}]$, $\Pr[\mathcal{A}_2 \diamond \mathcal{L}_1 = \mathsf{true}]$, $\Pr[\mathcal{A}_2 \diamond \mathcal{L}_2 = \mathsf{true}]$ with

$$\begin{array}{|l|}\hline \quad\mathcal{A}_1 \\ \hline r_1 \leftarrow \textsc{rand}(6) \\ r_2 \leftarrow \textsc{rand}(6) \\ \text{return } r_1 \stackrel{?}{=} r_2 \\ \hline \end{array} \quad \begin{array}{|l|}\hline \quad\mathcal{A}_2 \\ \hline r_1 \leftarrow \textsc{rand}(6) \\ r_2 \leftarrow \textsc{rand}(6) \\ \text{return } r_1 \stackrel{?}{\geq} 3 \\ \hline \end{array} \quad \begin{array}{|l|}\hline \quad\mathcal{L}_1 \\ \hline \underline{\textsc{rand}(n):} \\ \quad r \xleftarrow{\$} \mathbb{Z}_n \\ \quad \text{return } r \\ \hline \end{array} \quad \begin{array}{|l|}\hline \quad\mathcal{L}_2 \\ \hline \underline{\textsc{rand}(n):} \\ \quad \text{return } 0 \\ \hline \end{array}$$

2. Are the following libraries indistinguishable? (if so, describe the distinguisher (you can test it in Caseine) and **compute** its success probability:

(a) $$\begin{array}{|l|}\hline \quad\mathcal{L}_A \\ \hline \underline{\textsc{sample}():} \\ \quad \textbf{return } 42 \\ \hline \end{array} \stackrel{?}{\approx} \begin{array}{|l|}\hline \quad\mathcal{L}_B \\ \hline \underline{\textsc{sample}():} \\ \quad \textbf{return } 45 \\ \hline \end{array}$$

(b) $$\begin{array}{|l|}\hline \quad\mathcal{L}_A \\ \hline \underline{\textsc{sample}():} \\ \quad x \xleftarrow{\$} \mathbb{Z}_{10} \\ \quad \textbf{return } x \\ \hline \end{array} \stackrel{?}{\approx} \begin{array}{|l|}\hline \quad\mathcal{L}_B \\ \hline \underline{\textsc{sample}():} \\ \quad x \xleftarrow{\$} \mathbb{Z}_{9} \\ \quad \textbf{return } x \\ \hline \end{array}$$

(c) $$\begin{array}{|l|}\hline \quad\mathcal{L}_A \\ \hline \underline{\textsc{sample}():} \\ \quad x \xleftarrow{\$} \mathbb{Z}_{10} \\ \quad \textbf{return } x \\ \hline \end{array} \stackrel{?}{\approx} \begin{array}{|l|}\hline \quad\mathcal{L}_B \\ \hline \underline{\textsc{sample}():} \\ \quad x \xleftarrow{\$} \mathbb{Z}_{10} \\ \quad \textbf{return } 2 + x \\ \hline \end{array}$$

(d) $$\begin{array}{|l|}\hline \quad\mathcal{L}_A \\ \hline \underline{\textsc{sample}():} \\ \quad x \xleftarrow{\$} \mathbb{Z}_{10} \\ \quad \textbf{return } x \\ \hline \end{array} \stackrel{?}{\approx} \begin{array}{|l|}\hline \quad\mathcal{L}_B \\ \hline \underline{\textsc{sample}():} \\ \quad x \xleftarrow{\$} \mathbb{Z}_{10} \\ \quad \textbf{return } (2 + x) \mod 10 \\ \hline \end{array}$$

(e) $$\begin{array}{|l|}\hline \quad\mathcal{L}_A \\ \hline a := 0 \\ \underline{\textsc{sample}():} \\ \quad \textbf{return } 42 \\ \hline \end{array} \stackrel{?}{\approx} \begin{array}{|l|}\hline \quad\mathcal{L}_B \\ \hline a := 1 \\ \underline{\textsc{sample}():} \\ \quad b := 8 \\ \quad \textbf{return } 42 \\ \hline \end{array}$$

(f) $$\begin{array}{|l|}\hline \quad\mathcal{L}_A \\ \hline \underline{\textsc{sample}():} \\ \quad \textbf{return } 9 \\ \hline \end{array} \stackrel{?}{\approx} \begin{array}{|l|}\hline \quad\mathcal{L}_B \\ \hline \underline{\textsc{sample}():} \\ \quad \textbf{return } \textsc{square}\ (3) \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \quad\mathcal{L}_C \\ \hline \underline{\textsc{square}(x):} \\ \quad \textbf{return } x^2 \\ \hline \end{array}$$

(g) $$\begin{array}{|l|}\hline \quad\mathcal{L}_A \\ \hline \underline{\textsc{sample}():} \\ \quad x \xleftarrow{\$} \mathbb{Z}_{10} \\ \quad \textbf{if } x \stackrel{?}{=} 0 \textbf{ then } x \xleftarrow{\$} \mathbb{Z}_{10} \\ \quad \textbf{return } x \\ \hline \end{array} \stackrel{?}{\approx} \begin{array}{|l|}\hline \quad\mathcal{L}_B \\ \hline \underline{\textsc{sample}():} \\ \quad x \xleftarrow{\$} \mathbb{Z}_{10} \\ \quad \textbf{return } x \\ \hline \end{array}$$

(h) The libraries of the IND-CPA security definition with the encryption scheme $\mathsf{Gen}(1^\lambda)$ always returning 0, and $\mathsf{Enc}_k(m) := \bar{m}$, where $m \in \{0, 1\}^\lambda$, $\bar{m}$ is the bitwise flip of m (0 becomes 1 and 1 becomes 0).

(i) The libraries of the IND-CPA security definition with the One-Time Pad encryption scheme.

(j) The libraries of the IND-CPA security definition with any unknown deterministic encryption scheme.

Exercice 2: First security proof

We say that a scheme is *One-Time uniform ciphertexts* secure iff

$$\begin{array}{|l|}\hline \mathcal{L}_{\text{ots\$-real}} \\ \hline \underline{\textsc{ctxt}(m):} \\ \quad k \leftarrow \mathsf{Gen}(1^\lambda) \\ \quad c \leftarrow \mathsf{Enc}_k(m) \\ \quad \textbf{return } c \\ \hline \end{array} \equiv \begin{array}{|l|}\hline \mathcal{L}_{\text{ots\$-real}} \\ \hline \underline{\textsc{ctxt}(m):} \\ \quad c \xleftarrow{\$} \{0,1\}^\lambda \\ \quad \textbf{return } c \\ \hline \end{array} \tag{1}$$

1. Prove that the OTP is One-Time uniform ciphertexts secure by explicitly computing the probability.

2. We define the double-OTP construction by sampling two OTP keys k_1, k_2, and by encrypting the message twice as follows: $\mathsf{Enc}_{k_1,k_2}(m) \coloneqq k_2 \oplus (k_1 \oplus m)$.

   (a) Describe the decryption procedure.

   (b) Show that the double-OTP construction is One-Time uniform ciphertexts secure. (Your are not allowed to follow the same strategy as you did in the first question. See the exercice in Caseine to get advices and/or check your solution.)

   (c) If we reuse the key, i.e. $k_2 = k_1$, is the double-OTP construction One-Time uniform ciphertexts secure? Prove it by exhibiting a distinguisher or proving its security.

   (d) Prove that any One-Time uniform ciphertexts secure scheme satisfies One-Time secrecy:

$$\begin{array}{|l|}\hline \mathcal{L}^{\Sigma}_{\text{cpa-L}} \\ \hline \underline{\textsc{eavesdrop}(m_L, m_R \in \mathcal{M}):} \\ \quad k \leftarrow \mathsf{Gen}(1^\lambda) \\ \quad \text{return } \mathsf{Enc}_k(m_L) \\ \hline \end{array} \approx \begin{array}{|l|}\hline \mathcal{L}^{\Sigma}_{\text{cpa-R}} \\ \hline \underline{\textsc{eavesdrop}(m_L, m_R \in \mathcal{M}):} \\ \quad k \leftarrow \mathsf{Gen}(1^\lambda) \\ \quad \text{return } \mathsf{Enc}_k(m_R) \\ \hline \end{array}$$

   (e) How does One-Time secrecy compare with IND-CPA secure (is one implying the other?)?

Exercice 3: Negligible functions

1. Which of the following functions are negligible? (justify, you may use $a^b = 2^{b \log a}$)

$$\frac{1}{2^{\lambda/2}} \qquad \frac{1}{2^{\log(\lambda^2)}} \qquad \frac{1}{\lambda^{\log(\lambda)}} \qquad \frac{1}{\lambda^2} \qquad \frac{1}{2^{\log \lambda^2}} \qquad \frac{1}{\lambda^{1/\lambda}} \qquad \frac{1}{\sqrt{\lambda}} \qquad \frac{1}{2^{\sqrt{\lambda}}}$$

2. Show that if f and g are negligible, so are $f + g$ and fg.

3. Show that if $f = \mathsf{poly}(\lambda)$ and $g = \mathsf{negl}(\lambda)$, $fg = \mathsf{negl}(\lambda)$.