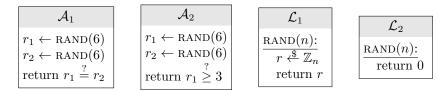
# TD 1 Crytography Engineering

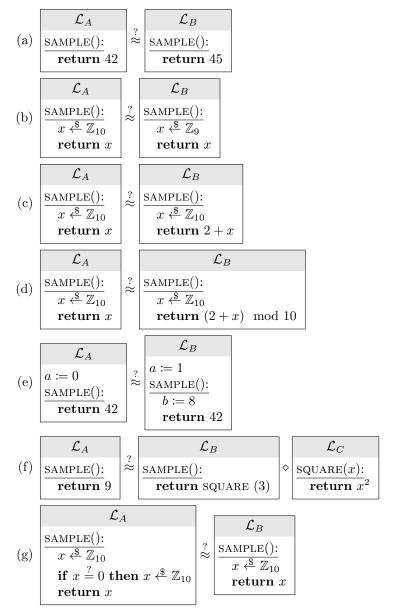
## Léo Colisson Palais

### Exercice 1:

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



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



(h) The libraries of the IND-CPA security definition with the encryption scheme  $\mathsf{Gen}(1^{\lambda})$  always returning 0, and  $\mathsf{Enc}_k(m) \coloneqq \bar{m}$ , 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

$$\frac{\mathcal{L}_{\text{ots\$-real}}}{\frac{\text{CTXT}(m):}{k \leftarrow \text{Gen}(1^{\lambda})}} = \frac{\mathcal{L}_{\text{ots\$-real}}}{\frac{\text{CTXT}(m):}{c \leftarrow \frac{\$}{\{0, 1\}^{\lambda}}}}$$

$$\frac{\text{return } c}{\text{return } c}$$
(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:

$$\begin{array}{|c|c|} & \mathcal{L}_{\text{cpa-L}}^{\Sigma} \\ \hline & \underbrace{\text{EAVESDROP}(m_L, m_R \in \mathcal{M}):}_{k \leftarrow \mathsf{Gen}(1^{\lambda})} \\ & \text{return } \mathsf{Enc}_k(m_{\boldsymbol{L}}) \end{array} \approx \begin{array}{|c|c|c|} & \mathcal{L}_{\text{cpa-R}}^{\Sigma} \\ \hline & \underbrace{\text{EAVESDROP}(m_L, m_R \in \mathcal{M}):}_{k \leftarrow \mathsf{Gen}(1^{\lambda})} \\ & \text{return } \mathsf{Enc}_k(m_{\boldsymbol{R}}) \end{array}$$

(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  $a^b = 2^{b \log a}$ )

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

- 2. Show that if f and g are negligible, so are f + g and fg.
- 3. Show that if  $f = poly(\lambda)$  and  $g = negl(\lambda)$ ,  $fg = negl(\lambda)$ .