Tutorial 4: PRP and block ciphers

Exercise 1. *A weak-PRP is a PRF*

Definition 1 (weak PRP). *A function $F : \{0,1\}^s \times \{0,1\}^n \to \{0,1\}^n$ is said to be a Pseudo-Random Permutation (PRP) if*

- *For any $k \in \{0,1\}^s$, the function $F_k : x \mapsto F(k,x)$ is a permutation (i.e., a bijection from $\{0,1\}^n$ to $\{0,1\}^n$).*
- *All PPT algorithms $\mathcal{A}$ have a negligible advantage in the following game*

$\mathcal{C}$		$\mathcal{A}$
$b \leftarrow U(\{0,1\})$		
$k \leftarrow U(\{0,1\}^s)$		
if $b = 0$, *then* $F = F(k,.)$		
else F *is a uniformly chosen permutation of* $\{0,1\}^n$		
	$\xleftarrow{x}$	*(polynomially many queries)*
	$\xrightarrow{F(x)}$	
		outputs $b' \in \{0,1\}$

where the advantage of $\mathcal{A}$ is defined by $\mathrm{Adv}(\mathcal{A}) = |\Pr(b' = 1 | b = 1) - \Pr(b' = 1 | b = 0)|$.

Remark. A PRP is very similar to a PRF, except that it is a bijection, and it should be indistinguishable from a uniform bijection (while a PRF should be indistinguishable from a uniform function).

The objective of this exercise is to show that a PRP is also a PRF. We will first show that a PPT algorithm cannot distinguish between a random function and a random permutation with non negligible advantage. Let $\mathcal{A}$ be a PPT algorithm with running time at most t. We want to show that $\mathcal{A}$ has negligible advantage in the following game

$\mathcal{C}$		$\mathcal{A}$
$b \leftarrow U(\{0,1\})$		
if $b = 0$, then F is a random permutation of $\{0,1\}^n$		
else, F is a random function from $\{0,1\}^n$ to $\{0,1\}^n$		
	$\xleftarrow{x}$	(polynomially many queries)
	$\xrightarrow{F(x)}$	
		outputs $b' \in \{0,1\}$

1. Give a pseudo-code algorithm for implementing $\mathcal{C}$ in the case where F is a random function and in the case where F is a random permutation.
2. Show that the advantage of $\mathcal{A}$ in distinguishing whether F is a random permutation or a random function is at most the probability that $\mathcal{A}$ finds a collision when F is a random function. In other words, show that

   $$|\Pr(\mathcal{A} \text{ outputs } 1 | F \text{ is a random function}) - \Pr(\mathcal{A} \text{ outputs } 1 | F \text{ is a random permutation})| \leq \delta,$$

   where δ is the probability to find a collision when sampling t independent uniform elements in $\{0,1\}^n$ (that is $\delta = \Pr_{y_1,\cdots,y_t \leftarrow U(\{0,1\}^n)}(\exists i \neq j \text{ s.t. } y_i = y_j)$).
3. Show that $\delta \leq \frac{t^2}{2^n}$.
4. Show that if $n \geq \lambda$ (the security parameter), then any pseudo-random permutation is also a pseudo-random function.

Exercise 2. *ECB*

We consider a block cipher $\mathcal{E}$ operating on blocks of n bits:

$$\begin{array}{rcl} \mathcal{E} : \mathcal{K} \times \mathcal{M} & \longrightarrow & \mathcal{C} \\ (k, m) & \longmapsto & \mathcal{E}_k(m) = \mathcal{E}(k, m) = c \end{array}$$

The ECB (Electronic Code Book) mode is recalled in Figure 1. The message is divided into blocks and each block is encrypted separately. Another mode, the CBC* mode, is described in Figure 2.

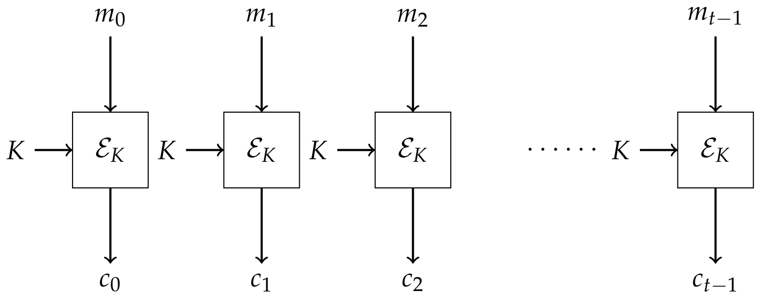

Figure 1: ECB mode

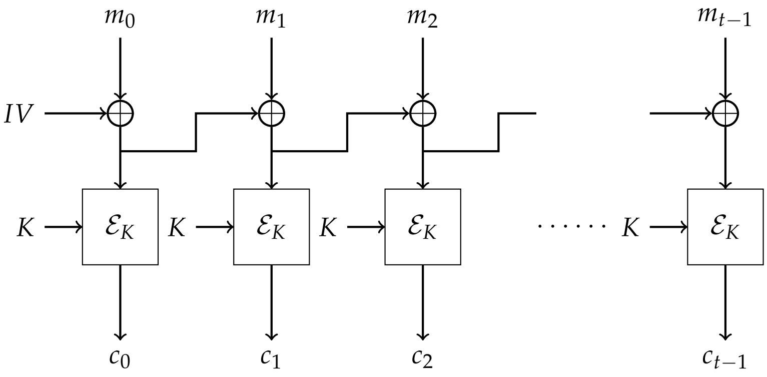

Figure 2: CBC* mode encryption

1. Show that the ECB mode is not secure under (one-time) chosen message attacks.

2. Give a decryption algorithm for the CBC* mode (the value IV is given as part of the ciphertext).

3. Show that the CBC* mode is not secure under (one-time) chosen message attacks, even if the underlying $\mathcal{E}$ is a secure block cipher.

Exercise 3. *3-DES*

A *double encryption scheme* consists in encrypting twice the plaintext $m \in \{0,1\}^n$ with two independent keys $k_1 \in \{0,1\}^\ell$ and $k_2 \in \{0,1\}^\ell$. We have $c = \mathcal{E}_{k_2}(\mathcal{E}_{k_1}(m))$.

1. Consider the following attacker $\mathcal{A}$: Assume that it knows some pairs plaintext/ciphertext (m, c), it computes $\mathcal{E}_k(m)$ and $\mathcal{D}_k(c)$ for all the keys k and memorizes all the results in a table. Analyse the complexity in memory and time of this attack and explain how the adversary can find the pair of keys used for the double encryption (compared to the exhaustive search).

This attack explains why we use the Triple-DES, which consists in a triple encryption with the DES encryption using three different keys $(K_1, K_2, K_3) \in \{0,1\}^{56} \times \{0,1\}^{56} \times \{0,1\}^{56}$:

$$\text{Triple-DES}_{K_1,K_2,K_3}(X) = \text{DES}_{K_3}(\text{DES}_{K_2}^{-1}(\text{DES}_{K_1}(X))).$$

2. Can the previous attack be adapted to Triple-DES? Is it practical?

3. Why do we use $\mathcal{E}_{K_2}^{-1}$ and not $\mathcal{E}_{K_2}$ for the second key in Triple-DES?

Exercise 4. *Security of the CTR encryption scheme*

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. To encrypt a message $M \in \{0,1\}^{d \cdot n}$, CTR proceeds as follows:

- Write $M = M_0 \| M_1 \| \ldots \| M_{d-1}$ with each $M_i \in \{0,1\}^n$.
- Sample IV uniformly in $\{0,1\}^n$.
- Return $IV \| C_0 \| C_1 \| \ldots \| C_{d-1}$ with $C_i = M_i \oplus F(k, IV + i \bmod 2^n)$ for all i.

The goal of this exercise is to prove the security of the CTR encryption mode against (many-time) chosen plaintext attacks, when the PRF F is secure.

1. Recall the definition of security of an encryption scheme against (many-time) chosen plaintext attacks.

2. Assume an attacker makes q encryption queries. Let $IV_1, \ldots, IV_q$ be the corresponding IV's. Let `Twice` denote the event "there exist $i \neq j \leq q$ and $k_i, k_j < d$ such that $IV_i + k_i = IV_j + k_j \bmod 2^n$." Show that the probability of `Twice` is bounded from above by $q^2 d / 2^n$.

3. Assume the PRF F is replaced by a uniformly chosen function $f : \{0,1\}^n \to \{0,1\}^n$. Bound the distinguishing advantage of an adversary $\mathcal{A}$ against this idealized version of CTR, as a function of d and the number of encryption queries q.

4. Show that if there exists a probabilistic polynomial-time adversary $\mathcal{A}$ against CTR based on PRF F, then there exists a probabilistic polynomial-time adversary $\mathcal{B}$ against the PRF F. Give a lower bound on the advantage degradation of the reduction.