## Appendix: IND-CPA games

A scheme E is said to be IND-CPA secure if no attacker can win the following games with probability more than  $0.5 + \varepsilon(\lambda)$ , where  $\varepsilon(\lambda)$  is a negligible function of the security parameter  $\lambda$  (usually,  $\lambda$  is the size of the key).

## IND-CPA game without diversification

	Challenger		<u>Attacker</u>
1)			Choose messages $(m_1, \dots m_n)$
		$\xleftarrow{m_i}$	
2)	Compute $c_i = E_k(m_i)$	(m. a.)	
		$\xrightarrow{(m_i,c_i)}$	
3)			Analyses the data
4)			Choose two messages $m$ and $m'$
4)		$\overset{m,m'}{\longleftarrow}$	Choose two messages m and m
	Sample a random bit $b \stackrel{\$}{\leftarrow} \{0,1\}$ .	`	
5)	If $b = 0$ , compute $c = E_k(m)$ If $b = 1$ , compute $c = E_k(m')$		
	If $b=1$ , compute $c=E_k(m)$	$\overset{c}{\longrightarrow}$	
7)			Tries to guess the value of b

FIGURE 1 – The IND-CPA game without diversification

The attacker must respect some constraints when choosing their messages :

- 1. The number of queries must be of polynomial size (with regard to the security parameter  $\lambda$ ).
- 2. The messages m and m' cannot be among the queried messages.

## IND-CPA game with diversification

Now, our scheme E has three inputs: the key k, the message m and a diversifier d. The IND-CPA game becomes:

1)	Challenger	$(m_i,d_i)$	Attacker Choose messages $(m_1, \dots m_n)$ and diversifiers $(d_1, \dots, d_n)$
2)	Compute $c_i = E_k(m_i, d_i)$	$(m_i, d_i, c_i) $	
3)			$Analyses \ the \ data$
4)		$\overset{m,m'}{\longleftarrow},\!d$	Choose two messages $m$ and $m'$ and an unique diversier $d$
5)	Sample a random bit $b \stackrel{\$}{\leftarrow} \{0, 1\}$ . If $b = 0$ , compute $c = E_k(m, d)$ If $b = 1$ , compute $c = E_k(m', d)$	$\overset{c}{\longrightarrow}$	
7)			Tries to guess the value of b

Figure 2 – The IND-CPA game with diversification

The attacker must respect some constraints when choosing their messages and diversifiers :

- 1. The number of queries must be of polynomial size (with regard to the security parameter  $\lambda$ ).
- 2. The messages m and m' can be anything.
- 3. The diversifier d must be a nonce : it cannot be equal to any  $d_i$  chosen during the query phase.