Cryptology II
Homework 1

Ilya Kuzovkin

April 17, 2012

Exercise IV.5

If we want to talk about IND-CPA security of a symmetric cryptosystem we may want to introduce two security games:

```
$Q_0$
  sk ← Gen
  $(m_0, m_1) \leftarrow A^{\mathrm{Enc}}$
  return $A^{\mathrm{Enc}}(\mathrm{Enc}_{\mathrm{sk}}(m_0))$
```

```
$Q_1$
  sk ← Gen
  $(m_0, m_1) \leftarrow A^{\mathrm{Enc}}$
  return $A^{\mathrm{Enc}}(\mathrm{Enc}_{\mathrm{sk}}(m_1))$
```

and argue about success probability ε the t-time adversary A may achieve:

$$\mathrm{Adv}^{\text{IND-CPA}}(A) = |\Pr[Q_0^{\mathrm{A}} = 1] - \Pr[Q_1^{\mathrm{A}} = 1]| \leq \varepsilon$$

So we have symmetric cryptosystem scheme `Ctr-$`:

- Gen

```
  $\mathrm{k} \overset{u}{\leftarrow} \mathrm{K}$
  return k
```

- Enc$(m_1, \ldots, m_n)$

```
  $s_0 \overset{u}{\leftarrow} \mathrm{M}$
  for $(i = 1$ to $n)$
    $c_i \leftarrow m_i + f(s_0 + i, k)$
  end
  return $(s_0, c_1, \ldots, c_n)$
```

- Dec$(s_0, c_1, \ldots, c_n)$

```
  for $(i = 1$ to $n)$
    $m_i \leftarrow c_i - f(s_0 + i, k)$
  end
  return $(m_1, \ldots, m_n)$
```

and we want to argue that it is IND-CPA secure with some security parameters $t_\$$ and $\varepsilon_\$$. There is one assumption we will rely on: we say that function f is (t_f, ε_f)-secure pseudorandom permutation. This means that t_f-time adversary A^{PRP} will be able to distinguish if this function is taken from random permutation function family or from family of all functions with success probability ε_f.

Why do we care will he be able to do that or not? I presume because if he can, that he also can effectively try out all possible permutations and gain knowledge about our encrypted message (or even decrypt it).

Se let us setup two games and see how successful adversary B will be in distinguishing them (and how long it will take).

```
$G_0$
    sk ← Gen
    $(m_1^{\text{one}}, \ldots, m_n^{\text{one}}, m_1^{\text{two}}, \ldots, m_n^{\text{two}}) \leftarrow A^{\text{Enc}}$
    $(c_1, \ldots, c_n) \leftarrow \text{Enc}(m_1^{\text{one}}, \ldots, m_n^{\text{one}})$
    return $A^{\text{Enc}}(c_1, \ldots, c_n)$
```

```
$G_0$
    sk ← Gen
    $(m_1^{\text{one}}, \ldots, m_n^{\text{one}}, m_1^{\text{two}}, \ldots, m_n^{\text{two}}) \leftarrow A^{\text{Enc}}$
    $(c_1, \ldots, c_n) \leftarrow \text{Enc}(m_1^{\text{two}}, \ldots, m_n^{\text{two}})$
    return $A^{\text{Enc}}(c_1, \ldots, c_n)$
```

Here adversary generates message vectors in the way, which is best for him for later distinguishing. And since only thing he knows is how to distinguish PRF then best possible way for him to initialize message vectors is to generate one vector of messages using function from pseudorandom function family and second vector using function from family of all functions.

In such way each time we encrypt a message we introduce ε success probability for the adversary. Since we do it n times, the overall success probability of adversary can be $n \cdot \varepsilon$.

And here is adversary B, who can use adversary A. We can estimate advantage of B and therefore security parameters of the `Ctr-$` scheme.

```
$B$
    sk ← Gen
    $(m_1^{\text{one}}, \ldots, m_n^{\text{one}}, m_1^{\text{two}}, \ldots, m_n^{\text{two}}) \leftarrow A^{\text{Enc}}$
    return $(m_1^{\text{one}}, \ldots, m_n^{\text{one}}, m_1^{\text{two}}, \ldots, m_n^{\text{two}})$
```

```
$B(c_1, \ldots, c_n)$
    return $A^{\text{Enc}}(c_1, \ldots, c_n)$
```

$$\text{Adv}^{\text{IND-CPA}_{\texttt{Ctr-\$}}}(B) = |\Pr[G_0^{\text{A}} = 1] - \Pr[G_1^{\text{A}} = 1]| \leq \varepsilon_{\$}$$

Time analysis: B uses A to generate message and to work with ciphers. Aside from that B only generates sk once, which presumably takes $O(1)$ time. So the working time of B is equal to the working time of A: $t_f = t_{\$}$

Now we have both security parameters and can say that if f is (t_f, ε_f)-secure pseudorandom function, then `Ctr-$` is $(t_f, n\varepsilon_f)$-secure IND-CPA cryptosystem.