## Security models

1st Semester 2014/2015

F.Autreau
P.Lafourcade
M. Gagné
JL. Roch

P. Lafourcade
M. Gagné

# SET 1

Date: 20.10.2014

**Exercise 1**

Prove that under CDH assumption El-Gamal is OW-CPA.

**Exercise 2**

Prove that if there is an adversary which can break DDH then there is an adversary which can break the IND-CPA security of El-Gamal.

**Exercise 3**

Prove that under DDH assumption El-Gamal is IND-CPA.

**Exercise 4**

Define the $n$-DDH problem as follows: on input $(A = g^a, (B_1 = g^{b_1}, C_1 = g^{c_1}), \ldots, (B_n = g^{b_n}, C_n = g^{c_n}))$, determine if for all $i$, $c_i = ab_i$ or if for all $i$, $c_i$ is randomly distributed.

Show that the $n$-DDH problem is intractable if and only if the DDH problem is intractable.

**Exercise 5**

Show that the straightforward application of the RSA function is not an IND-CPA encryption scheme. That is, the encryption function $E_{(n,e)}(m) = m^e \pmod{n}$ is not an IND-CPA encryption scheme.

**Exercise 6**

We define the $n$-IND-CPA game as follows: Given an encryption scheme $\mathbf{S} = (\mathbf{K}, \mathbf{E}, \mathbf{D})$, an $n$-IND-CPA adversary is a tuple $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_{n+1})$ of probabilistic polynomial-time algorithms. For $b \in \{0, 1\}$, define the following game.

$n - \mathbf{IND}^b - CPA$**:**

- Generate $(pk, sk) \leftarrow \mathbf{K}(\eta)$
- $(s_1, m_{1,0}, m_{1,1}) \leftarrow \mathcal{A}_1(\eta, pk)$
- $(s_2, m_{2,0}, m_{2,1}) \leftarrow \mathcal{A}_1(\eta, pk, s_1, \mathbf{E}(pk, m_{1,b}))$
- $\ldots$
- $b' \leftarrow \mathcal{A}_{n+1}(\eta, pk, s_n, \mathbf{E}(pk, m_{n,b}))$
- return $b'$

Define $Adv^{n-\text{IND-CPA}}_{\mathbf{S},\mathcal{A}} = \Pr[b' \leftarrow \text{n-IND}^1\text{-CPA} : b' = 1] - \Pr[b' \leftarrow \text{n-IND}^0\text{-CPA} : b' = 1]$.

Show that an encryption scheme is $n$-IND-CPA secure if and only if it is IND-CPA secure.

**Exercise 7 (Midterm 2008)**

1. Give the definition of NM-CPA NM-CCA1 and NM-CCA2.

2. Justify informally the implication relations between these three notions.

**Exercise 8 (Midterm 2008)**
We propose a modified version of El-Gamal encryption scheme. Consider the following scheme, where $g_1$, $g_2$ are two randomly-chosen generators in $G$ a cyclic group:
**KeyGen**$(1^k)$**:**
$x, y \leftarrow Z_q$;
$h = g_1^x g_2^y$;
$PK =< g_1, g_2, h >$;
$SK =< x, y >$;
output $(PK, SK)$;

**E**$(PK, m)$**:**
$r \leftarrow Z_q$;
output $< g_1^r, g_2^r, h^r * m >$;

**D**$(SK, u, v, e)$**:**
output $\frac{e}{u^x v^y}$;

1. Correctness: Assuming an honest execution of the protocol, prove that $\frac{e}{u^x v^y} = m$

2. Prove that the modified scheme is semantically (IND-CPA) secure under the DDH assumption (Only the reduction as in exercises session).

   Recall: DDH is given $(g, g^u, g^v, \alpha)$ guess whether $\alpha$ is $g^{uv}$ or $g^r$ where $r$ is a random value.

   Hint: one can take $g_1 = g$ and $g_2 = g^u$.

**Exercise 9 (Midterm 2010)**
Let $\mathcal{E}$ be an NM-CCA2 secure encryption scheme. We modify this scheme into $\mathcal{E}'(m) = \mathcal{E}(m)||h(m)$, where $h$ is a public hash function. This should help the user to detect some errors in the transmission of the messages.

- Give the definition of NM-CCA2

- Prove that the new scheme $\mathcal{E}'$ is not IND-CPA. It means give an attack against IND-CPA for $\mathcal{E}'$.

**Exercise 10 (Final 2009)**
Let $\mathcal{E}$ be an IND-CCA2 secure encryption scheme. We modify this scheme into $\mathcal{E}'(m) = \mathcal{E}(m)||h(m)$, where $h$ is an hash function. This should help the user to detect some errors in the transmission of the messages. Prove that the new scheme $\mathcal{E}'$ is not IND-CPA. It means give an attack against IND-CPA for $\mathcal{E}'$.

**Exercise 11 (Final 2009)**
Zheng & Seberry in 1993 proposed the following encryption scheme:

$$f(r)||(G(r) \oplus (x||H(x)))$$

where $x$ is the plain text, $f$ is a one way trap-door function (like RSA), $G$ and $H$ are two public hash functions, $||$ denotes the concatenation of bitstrings and $\oplus$ is the exclusive-or operator.

- Give the associated decryption algorithm.
- Give an IND-CCA2 attack against this scheme.

  Hint: you cannot ask the cipher of $m_b$ to the decryption oracle, but a cipher of $m_{\bar{b}}$ is not forbidden...

**Exercise 12 (Final 2010)**
Consider a naïve modified version of RSA with public parameter $(e, n)$ defined by : $E(x) = (v, w)$ where $k$ is a random number $v = k^e \mod n$ and $w = x * k$.

1. Show that you can extract $x^e \mod n$ from $e$ and the encryption $(v, w)$ of an unkown message $x$.
2. Find an IND-CPA attack against this encryption scheme.

**Exercise 13 (Final 2010)**
We consider random version of RSA proposed by David Pointcheval. Encryption of the message $m$ is $D - RSA_{(n,e)}(m) = (a, b)$ where $a = k^e \mod n$, $b = (k+1)^e \times m \mod n$ and $k$ is a random number.

- Give the decryption algorithm
- We define the Computational D-RSA problem (CD-RSA) by :
  Given $(n, e)$, and $a^e \mod n$
  Find $(a+1)^e \mod n$

  Prove that under CD-RSA assumption then D-RSA is OW-CPA.
- We define the Decisional D-RSA problem (DD-RSA) by Given $(n, e)$, $r^e \mod n$ and $s^e \mod n$

  Decide if $s = r + 1 \mod n$

  Prove that under DD-RSA assumption then D-RSA is IND-CPA.

**Exercise 14**
Find an attack on CBC encryption with counter $IV$, (proving that this encryption mode is not IND-CPA secure). In this scheme the frist $IV$ used is 0 and for generating the next $IV$ we just increase by one the value of the previous $IV$.

**Exercise 15**
Prove that CTR is not IND-CCA2 secure.

**Exercise 16**
Prove that CFB is not IND-CCA2 secure.

**Exercise 17**
Prove that OFB is not IND-CCA2 secure.

**Exercise 18**
Prove that CBC with random $IV$ is not IND-CCA2 secure. This time $IV$ is a random number. But notice that this mode is IND-CPA secure.

**Exercise 19**
Suppose that $E_1$ and $E_2$ are symmetric encryption schemes on strings of arbitrary length. Show that the encryption scheme defined by $E'((k_1, k_2), m) = E_2(k_2, E_1(k_1, m))$ (for randomly sampled keys $k_1$ and $k_2$) is IND-CPA secure if *either* $E_1$ or $E_2$ is IND-CPA secure.

**Exercise 20 (Final 2012, Security Proof (15 points))**

- (3 points) Give the definition of the notion of OW-CPA security in the form of a security game.
- (12 points) We remind the definition of a one-way function: a function $f$ is a one-way function if, for a randomly chosen $x$ in the domain of $f$, no polynomial-time algorithm can compute $x$ when given only the description of $f$ and $f(x)$.

  We define the encryption algorithm $E$, which has a one-way function as its public key, as follows:

  - sample a random $x$ in the domain of $f$.
  - output $\langle f(x), x \oplus m \rangle$

  Prove that this is a OW-CPA secure encryption scheme if $f$ is a one-way function.

**Exercise 21**
Let BadMac, be the message authentication code defined as follows:

$$
\begin{array}{l}
\text{BadMac}((k_1, k_2), m_1 | \ldots | m_n) \\
\quad c_0 = 1; \\
\quad \text{for } i = 1 \text{ to } n, \text{ do:} \\
\quad\quad z_i = c_{i-1} \cdot m_i \pmod{2}^{128}; \\
\quad\quad c_i = z_i + k_1 \pmod{2}^{128}; \\
\quad out = \mathcal{E}_{k_2}(c_n); \\
\quad \text{Output } out;
\end{array}
$$

Show that BadMac is not a secure message authentication code.

**Exercise 22 (Midterm 2011, 8 points)**

- (3 points) Give the definition of the notion of IND-CCA2 in the form of a security game.
- (5 points) We say that a public key encryption scheme $E$ is additively homomorphic if for any key $k$ and any two messages $m_0, m_1$, $E_k(m_0) \cdot E_k(m_1) = E(m_0 + m_1)$.
  Show that an additively homomorphic encryption scheme cannot be IND-CCA2 secure.

**Exercise 23 (Midterm 2011, 10 points)**
Suppose that $E$ is a IND-CPA secure public key encryption scheme on strings of arbitrary length. Show that the encryption scheme defined by $E'(pk, m) = E\left(pk, E(pk, m)\right)$ for any message $m$ is also IND-CPA secure.

**Exercise 24 (Midterm 2011, 12 points)**
Let $\mathcal{E}$ be a (secret key) block cipher, and CBC-MAC be the message authentication code defined as follows:

CBC-MAC($k, m_1|\dots|m_n$)
  $c_1 = \mathcal{E}_k(m_1)$;
  for $i = 2$ to $n$, do:
    $c_i = \mathcal{E}_k(c_{i-1} \oplus m_i)$;
  Output $c_n$;

Show that CBC-MAC is not a secure message authentication code by finding a collision in the MAC. The attacking adversary can query an oracle that will compute the MAC of any message, but cannot compute the block cipher $\mathcal{E}_k$ on his own.

**Exercise 25 (Midterm 2008)**
Prove that any deterministic symmetric encryption scheme is IND-CPA insecure.

**Exercise 26 (Final 2008)**
Let $E : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ be a secure block cipher. Let $\mathcal{K}$ be the key-generation algorithm that returns a random $k$-bit string as the key $K$. Let $\mathcal{E}$ be the following encryption algorithm:

  Algorithm $\mathcal{E}_K(M)$
If $|M|$ is not a positive multiple of $l$ then return FALSE
Divide $M$ into $l$ bit blocks, $M = M[1]\dots M[n]$
$P[0] \leftarrow^R \{0,1\}^l$; $C[0] \leftarrow E_K(P[0])$ For $i = 1,\dots,n$ do
$P[i] \leftarrow P[i-1] \oplus M[i]$;
$C[i] \leftarrow E_K(P[i])$;
EndFor
$C \leftarrow C[0]C[1]\dots C[n]$;
Return $C$

1. Specify a decryption algorithm $\mathcal{D}$ such that $\mathcal{SE} = (\mathcal{K};\mathcal{E};\mathcal{D})$ is a symmetric encryption scheme with correct decryption. We are denoting the inverse of $E_K$ by $E_K^{-1}$
2. Show that this scheme is insecure by presenting a practical adversary IND-CPA. Say what is the advantage achieved by your adversary.

**Exercise 27 (Midterm 2010)**
Let $(E, D)$ be a block cipher using a symmetric encryption $E_k$ with a symmetric key $k$. Let $m_1, m_2, ..., m_t$ be a sequence of $t$ plaintext blocks. We consider the following block cipher mode which produce $t+2$ ciphertext blocks $c_0, c_1, c_2, ..., c_t, c_{t+1}$ which satisfies the equation, for $i = 1, ..., t$.

$$c_i = E_k(c_{i-1} \oplus m_i \oplus c_{i+1})$$

1. Describe how to reconstruct $m_1, ..., m_t$ given $c_0, ..., c_{t+1}$.
2. Find a way to compute effectively this encryption mode knowing that in order to get started, we set $c_0$ and $c_1$ to some fixed initialization vectors.

3. Assuming that decrypting or encrypting twice a message gives the message again ($D_k(D_k(x)) = x$, $E_k(E_k(x)) = x$) and that an intruder can fix $c_0$ and $c_1$ then find an IND-CPA attack against this scheme.

**Exercise 28 (Final 2012, IND-XXX Attack (21 points) ONLY M2R)**
We consider the following encryption function that uses the RSA function with public key $(N, e)$ and secret key $d$, and a public hash function $G$:

- sample a random $x \in \{0, \dots, N-1\}$
- output $\mathcal{E}_{(N,e)}(m) = \langle RSA_{(N,e)}(x),\ G(x) \oplus m \rangle$

1. (3 points) Recall the defintion of IND-CCA2 in the form of a security game.
2. (3 points) Give the decryption function corresponding to the encryption function above.
3. (5 points) Show that this scheme is not IND-CCA2 secure by giving an adversary that breaks the IND-CCA2 security of the scheme.

Consider now the following modification to to the encryption function above, which uses one more hash function ($H$):

- sample a random $x \in \{0, \dots, N-1\}$
- output $\mathcal{E}'_{(N,e)}(m) = \langle RSA_{(N,e)}(x),\ G(x) \oplus m,\ H(m) \oplus x \rangle$

in which decryption of $C = \langle a, b, c \rangle$ proceeds as for the preceeding scheme, except that after the message $m$ is computed, the decryption algorithm also verifies that $c = RSA_d^{-1}(a) \oplus H(m)$; if it is, it outputs $m$, otherwise it outputs $\perp$.

4. (10 points) Show that this new scheme is not even IND-CPA by giving an adversary that breaks the IND-CPA security of the scheme.