Notice: the number of points corresponds approximatively to the number of minutes needed for solving an exercise.

Exercise 1
(10 points)
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.

- (5 points) Give the definition of NM-CCA2
- (5 points) Prove that the new scheme \( \mathcal{E}' \) is not IND-CPA. It means give an attack against IND-CPA for \( \mathcal{E}' \).

Solution:

- Game Adversary: \( A = (A_1, A_2) \)
  
  1. The adversary \( A_1 \) is given the public key \( pk \).
  2. The adversary \( A_1 \) chooses a message space \( M \).
  3. Two messages \( m \) and \( m^* \) are chosen at random in \( M \) and \( c = E(m;r) \) is given to the adversary.
  4. The adversary \( A_2 \) outputs a binary relation \( R \) and a cipher-text \( c' \).

Probability \( Pr[R(m,m')] - Pr[R(m,m^*)] \) is negligible,
where \( m' = D(c') \)

- Consider the following adversary:
  
  Notice that \( \mathcal{E}'(m_b) = \mathcal{E}||h(m_b) \)
  
  \( A_1(n,pk) : m_1, m_0, s \)
  
  \( A_2(n,pk,s,m_1,m_0,\mathcal{E}'(m_b)) : \text{if } h(m_0) = h(m_b) \text{ then return 0 else 1} \)
Exercise 2
(20 points) 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. (5 points) Describe how to reconstruct \(m_1, ..., m_t\) given \(c_0, ..., c_{t+1}\).
2. (5 points) 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. (10 points) 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.

Solution :

1. For \(i = 1, ..., t\), we have the condition

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

Hence

\[ D_k(c_i) = D_k(E_k(c_{i-1} \oplus m_i \oplus c_{i+1})) \]

\[ D_k(c_i) = c_{i-1} \oplus m_i \oplus c_{i+1} \]

\[ m_i = D_k(c_i) \oplus c_{i-1} \oplus c_{i+1} \]

2. We showing how to compute \(c_{i+1}\) from \(c_{i-1}, c_i, m_i\), where \(1 \leq i \leq t\).

Starting from

\[ D_k(c_i) = c_{i-1} \oplus m_i \oplus c_{i+1} \]

we get

\[ c_{i+1} = D_k(c_i) \oplus c_{i-1} \oplus m_i \]

for \(1 \leq i \leq t\).

3. *PASCAL ATTACK* with only \(IV_0\) fixed. Assuming \(IV_0 = c_0\) is fixed for each encryption. If we consider the two messages :

- \(DVD^1 = m_1^1||m_2^1 = IV_0||0\)
$DV D^2 = m_1^2||m_2^2 = IV_0||1$

Where $m_1^1 = IV_0$, $m_2^1 = 0$, $m_1^2 = IV_0$ and $m_2^2 = 1$

We have

$$E(DVD^1, c_0^1, c_1^1) = c_0^1||c_1^1||c_2^1||c_3^1$$

$$E(DVD^2, c_0^2, c_1^2) = c_0^2||c_1^2||c_2^2||c_3^2$$

By hypothesis $c_0^1 = c_0^2 = IV_0$ and we do not know any information about $c_1^1$ and $c_1^2$.

Using the definition of the cipher mode

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

and the fact that the encryption is symmetric we have:

$$c_2^1 = D_k(c_1^1) \oplus c_0^1 \oplus m_1^1$$

$$= D_k(c_1^1) \oplus IV_0 \oplus IV_0$$

$$= D_k(c_1^1)$$

$$c_3^1 = D_k(c_2^1) \oplus c_1^1 \oplus m_2^1$$

$$= D_k(d_k(c_1^1)) \oplus c_1^1 \oplus 0$$

$$= c_1^1 \oplus c_1^1$$

$$= 0$$

$$c_2^2 = D_k(c_1^2) \oplus c_0^2 \oplus m_1^2$$

$$= D_k(c_1^2) \oplus IV_0 \oplus IV_0$$

$$= D_k(c_1^2)$$

$$c_3^2 = D_k(c_2^2) \oplus c_1^2 \oplus m_2^2$$

$$= D_k(d_k(c_1^2)) \oplus c_1^2 \oplus 1$$

$$= c_1^2 \oplus c_1^2 \oplus 1$$

$$= 1$$

if $c_3^2 = 1$ then it is $DV D^2$ else it is $DV D^1$

- **MARTIN ATTACK** fixing $IV_0$ and $IV_1$.

Give $m_0 = 0^n$ to encryption oracle it means encrypting $E(m_0) = A, B, C$ where $A = IV_0$ and $B = IV_1$.

Fix $m_1 = 1^n$ and use the left right algorithm obtain the challenge with $IV_0 = A$ and $IV_1 = B$, it means encrypting $c = E(m_0) = A, B, C^*$.

if $C = C^*$ then output 0 else output 1