

Quiz 1 Solutions

Problem 1 [25 points] A nuclear plant transmits 2^{35} ciphertexts to a monitoring station. Each ciphertext encrypts, under a key shared between the parties, a voltage measurement that is either HIGH or LOW. (Each of these values is encoded in binary for the encryption.) Consider the following choices of encryption scheme:

1. [9 points] DES in CBC\$ mode
2. [8 points] 2DES in CBC\$ mode
3. [8 points] AES in ECB mode

For each choice, discuss possible threats and indicate to what extent they impact security. Highlight differences in the security provided by the schemes and what types of guarantees are available. Ultimately indicate for each choice whether it is secure or not. Strive to concisely provide only relevant information; you lose points otherwise.

Let M_1, \dots, M_q denote the messages encrypted, and C_1, \dots, C_q the corresponding ciphertexts, where $q = 2^{35}$. The adversary A of course knows C_1, \dots, C_q but it would be prudent to also assume it knows a few plaintexts. Specifically we assume it knows M_1 . This is realistic because A may be working at the plant or have a posteriori knowledge.

1. [9 points] DES in CBC\$ mode

The relevant attacks are exhaustive key search and the birthday attack. The value of q is too small for linear or differential cryptanalysis to be a threat.

A CBC\$ ciphertext where A knows the plaintext provides it with an input-output example of DES under the encryption key. This allows it to mount an exhaustive key-search attack, which finds the key in just a few hours using appropriate key-search machines. This is an important threat.

The birthday attack on CBC\$ mode becomes a threat once the number of messages encrypted reaches $2^{n/2}$ where n is the block length of the underlying block cipher. This is true here because $n = 64$ so $2^{n/2} = 2^{32}$ while $q = 2^{35} > 2^{32}$. Exploiting collisions in the initial vectors, this will be able to detect equality amongst some of the plaintexts, meaning partial information is lost. The attack is less damaging than key recovery, but it only requires $2^{64/2} = 2^{32}$ time compared to 2^{56} time for the key-recovery attack.

CBC\$ is IND-CPA, but only for $q < 2^{32}$.

In conclusion, the scheme is not secure.

2. [8 points] 2DES in CBC\$ mode

Since the key-length is 112, exhaustive key search is not a threat. The meet-in-the-middle attack takes only 2^{57} time but is impractical due to its space requirements and is not a serious threat. Linear and differential cryptanalysis fail. The real threat is the birthday attack on CBC\$ mode. The blocklength of 2DES is only 64, just as for DES, and $q = 2^{35} > 2^{64/2} = 2^{32}$, so this attack succeeds in detecting some equalities amongst plaintexts. This loss of partial information may be damaging.

In conclusion, the scheme is not secure.

3. [8 points] AES in ECB mode

The key length of AES is too large for exhaustive search. But ECB mode is totally insecure. Knowing just M_1 , the adversary can figure out M_2, \dots, M_q by the following simple procedure: For each i if $C_i = C_1$ then $M_i = M_1$ and else $M_i \neq M_1$.

In conclusion, the scheme is not secure.

Problem 2 [45 points] Define $F: \{0, 1\}^{256} \times \{0, 1\}^{256} \rightarrow \{0, 1\}^{128}$ as follows. A key $K = K_1 \| K_2$ is a pair of 128-bit strings and an input $x = x[1]x[2]$ is a pair of 128-bit blocks. Then

$$F_{K_1 \| K_2}(x) = \text{AES}_{K_1}(\text{AES}_{K_2}(x[1]) \oplus \text{AES}_{K_2}(x[2])).$$

1. [5 points] Is F a block cipher? Why or why not?

A block cipher is a map $E: \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ where E_K is a permutation for every $K \in \{0, 1\}^k$. Note the domain and range are the same set, namely $\{0, 1\}^\ell$. In our case the domain and range are different so F is not a block cipher.

2. [20 points] Give the best key recovery attack that you can on F . Say how many AES and AES^{-1} computations and input-output examples your attack uses. Your score depends on these quantities.

Let $(x[1]x[2], y)$ be an input-output example under $K = K_1 \| K_2$. Exhaustive key search takes 2^{256} time. But there is a meet-in-the-middle attack based on the fact that

$$\text{AES}_{K_1}^{-1}(y) = \text{AES}_{K_2}(x[1]) \oplus \text{AES}_{K_2}(x[2]).$$

Let T_1, \dots, T_N denote a listing of AES keys, where $N = 2^{128}$. Then the attack is as follows:

```

for  $i = 1, \dots, N$  do
   $L[i] \leftarrow \text{AES}_{T_i}(x[1]) \oplus \text{AES}_{T_i}(x[2])$ 
for  $j = 1, \dots, N$  do
   $R[j] \leftarrow \text{AES}_{T_j}^{-1}(y)$ 
 $S \leftarrow \{(i, j) : L[i] = R[j]\}$ 
Pick some  $(l, r) \in S$  and return  $T_l \| T_r$ 

```

The attack returns a key consistent with the input-output example. To increase the chance of getting the target key one could test the candidate pairs in S under a second input-output example.

The attack uses $3 \cdot 2^{128}$ AES or AES^{-1} applications.

- 3. [20 points]** Give the best PRF-attack you can on F . Say what is the advantage achieved by your adversary, what is its running time, and how many oracle queries it makes. The number of points you get depends on these quantities.

A weakness of the construct we can exploit is that

$$F_{K_1 \| K_2}(x[1]x[2]) = F_{K_1 \| K_2}(x[2]x[1]) .$$

This leads to the following.

adversary A

$Y_1 \leftarrow \mathbf{Fn}(0^{128}1^{128}) ; y_2 \leftarrow \mathbf{Fn}(1^{128}0^{128})$
if $y_1 = y_2$ then return 1 else return 0

In Game Real_F we will have $y_1 = F_{K_1 \| K_2}(0^{128}1^{128})$ and $y_2 = F_{K_1 \| K_2}(1^{128}0^{128})$ where $K_1 \| K_2$ is the target key chosen by the **Initialize** procedure. By the above observation we will have $y_1 = y_2$, so

$$\Pr [\text{Real}_F^A \Rightarrow 1] = 1 .$$

In Game Rand_F the responses y_1, y_2 will be independent random 128-bit strings so

$$\Pr [\text{Rand}_F^A \Rightarrow 1] = \Pr [y_1 = y_2] = 2^{-128} .$$

So

$$\mathbf{Adv}_F^{\text{prf}}(A) = 1 - 2^{-128} .$$

The number of oracle queries made by A is 2 and its running time is tiny.

Problem 3 [30 points] Let algorithm \mathcal{K} return a random 128-bit string. For $1 \leq i \leq 128$ let $I_i = 0^{128-i}1^i$ be the string consisting of $128 - i$ zeros followed by i ones. Let \mathcal{E} be the following encryption algorithm that takes input a message $M = M[1] \cdots M[m]$ consisting of at most 128 blocks, where each block is 128-bits long (that is, $1 \leq m \leq 128$ and $|M[i]| = 128$ for all $1 \leq i \leq m$):

Algorithm $\mathcal{E}_K(M)$

$R \xleftarrow{\$} \{0, 1\}^{128} ; C[0] \leftarrow \text{AES}_K(R)$

For $i = 1, \dots, m$ do

$C[i] \leftarrow \text{AES}_K(R \oplus I_i \oplus M[i])$

Return C

1. [5 points] Specify a decryption algorithm \mathcal{D} such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme with correct decryption.

Algorithm $\mathcal{D}_K(C)$
 $R \leftarrow \text{AES}_K^{-1}(C[0])$
 For $i = 1, \dots, m$ do
 $M[i] \leftarrow \text{AES}_K^{-1}(C[i]) \oplus R \oplus I_i$
 Return M

2. [25 points] Show that this scheme is insecure by presenting a practical adversary A such that $\text{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A)$ is high. Say what is the advantage achieved by your adversary, what is its running time, and how many oracle queries it makes. The number of points you get depends on these quantities.

adversary A
 $C[0]C[1] \xleftarrow{\$} \text{LR}(0^{128}, I_1)$
if $C[0] = C[1]$ **then return 1 else return 0**

Suppose we are playing game $\text{Left}_{\mathcal{SE}}$, so that $C[0]C[1] \xleftarrow{\$} \mathcal{E}_K(0^{128})$. Then

$$\begin{aligned} C[0] &= \text{AES}_K(R) \\ C[1] &= \text{AES}_K(R \oplus I_1 \oplus 0^{128}) = \text{AES}_K(R \oplus I_1) . \end{aligned}$$

Since AES is a block cipher, the two quantities above cannot be equal. So

$$\Pr \left[\text{Left}_{\mathcal{SE}}^A \Rightarrow 1 \right] = 0 .$$

Suppose we are playing game $\text{Right}_{\mathcal{SE}}$, so that $C[0]C[1] \xleftarrow{\$} \mathcal{E}_K(I_1)$. Then

$$\begin{aligned} C[0] &= \text{AES}_K(R) \\ C[1] &= \text{AES}_K(R \oplus I_1 \oplus I_1) = \text{AES}_K(R) . \end{aligned}$$

So $C[0] = C[1]$. So

$$\Pr \left[\text{Right}_{\mathcal{SE}}^A \Rightarrow 1 \right] = 1 .$$

So

$$\text{Adv}_{\mathcal{SE}, A}^{\text{ind-cpa}} = 1 - 0 = 1 .$$

A makes 1 oracle query and its running time is very small.
