Computer Science and Engineering, UCSD | Winter 09
CSE 107: Introduction to Modern Cryptography | **Instructor:** Mihir Bellare
Problem Set 3 Solutions | February 19, 2009

Problem Set 3 Solutions

Problem 1 [50 points] Let $\mathcal{K}$ be the key-generation algorithm that returns a random 128-bit string as the key K. Let $\mathcal{E}$ be the following encryption algorithm, based on the block cipher AES.

```
function $\mathcal{E}_K(M)$
    $R \xleftarrow{\$} \{0,1\}^{128}$
    $C[0] \leftarrow R$
    for $i = 1, \ldots, n$ do
        $W[i] \leftarrow (R + i) \bmod 2^{128}$
        $C[i] \leftarrow \mathsf{AES}_K(M[i] \oplus W[i])$
    $C \leftarrow C[0]C[1] \ldots C[n]$
    return $C$
```

Above $W[i] \leftarrow (R + i) \bmod 2^{128}$ means we regard R as an interger, add i to it, take the result modulo 2^{128}, view this as a 128-bit string, and assign it to $W[i]$. The message space is the set of all strings whose length is a positive multiple of 128, and, as usual $M[i]$ denotes the i-th (128-bit) block of a message M and n denotes the number of blocks.

1. **[10 points]** Specify a decryption algorithm $\mathcal{D}$ such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme.

```
Algorithm $\mathcal{D}_K(C)$
    $R \leftarrow C[0]$
    For $i = 1, \ldots, m$ do
        $W[i] \leftarrow (R + i) \bmod 2^{128}$
        $M[i] \leftarrow \mathsf{AES}_K^{-1}(C[i]) \oplus W[i]$
    Return $M$
```

2. Show that this scheme is insecure by presenting a practical adversary A such that $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A)$ is high. State the value of the advantage achieved by your adversary and the number of oracle queries it makes.

Let I_1 denote the 128-bit string representation of the integer 1.

```
adversary $A$
$C[0]C[1]C[2] \xleftarrow{\$} \mathrm{LR}(0^{128} \parallel 0^{128}, I_1 \parallel 0^{128})$
```

```
if $C[1] = C[2]$ then return 1 else return 0
```

Suppose we are playing game $\text{Left}_{\mathcal{SE}}$, so that $C[0]C[1]C[2] \xleftarrow{\$} \mathcal{E}_K(0^{128} \| 0^{128})$. Then

$$\begin{aligned} C[0] &= R \\ C[1] &= \mathsf{AES}_K(0^{128} \oplus (R+1)) = \mathsf{AES}_K(R+1) \\ C[2] &= \mathsf{AES}_K(0^{128} \oplus (R+2)) = \mathsf{AES}_K(R+2)\ . \end{aligned}$$

Since AES is a block cipher, $C[0], C[1]$ 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 $C[0]C[1]C[2] \xleftarrow{\$} \mathcal{E}_K(I_1 \| 0^{128})$. Then

$$\begin{aligned} C[0] &= R \\ C[1] &= \mathsf{AES}_K(I_1 \oplus (R+1)) \\ C[2] &= \mathsf{AES}_K(0^{128} \oplus (R+2))\ . \end{aligned}$$

Notice that if R ends in 01, then $R+1$ ends in 10 and $R+2$ ends in 11, and thus $(R+1) \oplus I_1$ ends in 11 and $(R+2) \oplus 0^{128}$ also ends in 11. In this case,

$$C[1] = C[2]$$

so the game returns 1. Since the probability that R ends with 01 is 1/4 we have

$$\Pr\left[\text{Right}_{\mathcal{SE}}^{A} \Rightarrow 1\right] \geq \frac{1}{4}\ .$$

So

$$\mathbf{Adv}_{\mathcal{SE},A}^{\text{ind-cpa}} \geq \frac{1}{4} - 0 = \frac{1}{4}\ .$$

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

Problem 2 [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 $M_1, \ldots, M_q$ denote the messages encrypted, and $C_1, \ldots, C_q$ the corresponding ciphertexts, where $q = 2^{35}$. The adversary A of coures knows $C_1, \ldots, C_q$ 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 $M_2, \ldots, M_q$ 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.