Xueyuan Su *November 4, 2008*

Solution to Midterm Examination

Instructions:

This is a closed book examination. *Answer any 5 of the following 6 questions*. Write the numbers of the **five** questions that you want graded on the cover of your bluebook. All questions count equally. You have 75 minutes. Remember to write your name on your bluebook and to justify your answers. Good Luck!

Problem 1: Symmetric Cryptosystems and Information Security

Consider the encryption function for a symmetric cryptosystem described by the table below, where $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0, 1, 2, 3\}$:

$$\begin{array}{cc|cccc} & & & m & & \\ & & 0 & 1 & 2 & 3 \\ \hline & 0 & 3 & 0 & 2 & 1 \\ k & 1 & 1 & 3 & 0 & 2 \\ & 2 & 2 & 1 & 0 & 3 \\ & 3 & 0 & 2 & 3 & 1 \end{array}$$

(a) Give the corresponding decryption function.

(b) What does it mean for a cryptosystem to be information-theoretically secure?

(c) Is this cryptosystem information-theoretically secure? Why or why not?

Solution:

(a) From the original encryption function, we can easily derive the decryption function as:

$$\begin{array}{cc|cccc} & & & c & & \\ & & 0 & 1 & 2 & 3 \\ \hline & 0 & 1 & 3 & 2 & 0 \\ k & 1 & 2 & 0 & 3 & 1 \\ & 2 & 2 & 1 & 0 & 3 \\ & 3 & 0 & 3 & 1 & 2 \end{array}$$

(b) For the cryptosystem to have perfect secrecy (be information-theoretically secure), it means that the random variables c and m are statistically independent, that is,

$$\text{prob}[m = m_0 \wedge c = c_0] = \text{prob}[m = m_0] \times \text{prob}[c = c_0] \tag{1}$$

for all $m_0 \in \mathcal{M}$ and $c_0 \in \mathcal{C}$. An equivalent definition in terms of conditional probability is

$$\text{prob}[m = m_0 \mid c = c_0] = \text{prob}[m = m_0] \tag{2}$$

for all $m_0 \in \mathcal{M}$ and $c_0 \in \mathcal{C}$ such that $\text{prob}[c = c_0] \neq 0$. Hence, even after Eve receives the ciphertext c_0, her opinion of the likelihood of each message m_0 is the same as it was initially, so she has learned nothing about m_0.

(c) No, this cryptosystem is not information-theoretically secure. A simple observation is that $\text{prob}[m = 3] = 1/4$, but $\text{prob}[m = 3 \mid c = 0] = 0$. Similarly, $\text{prob}[m = 2] = 1/4$, but $\text{prob}[m = 2 \mid c = 1] = 0$. Therefore, after receiving $c = 0$ or $c = 1$, we have learned partial information about m.

Problem 2: Attacks

We have discussed a number of different possible attacks on a cryptosystem by a passive eavesdropper Eve, depending on what information is available to her.

(a) Describe the following three kinds of attack on a cryptosystem: ciphertext only, known plaintext, chosen plaintext. For each, give a scenario in which such an attack might be plausible for Eve to carry out.

(b) Consider the following simple cryptosystem: A message $m = m_1 m_2 \dots m_t$ is a t-bit string. A key is a single bit $k \in \{0, 1\}$. The encryption function is $E_k(m) = c$, where $c = c_1 c_2 \dots c_t$ and $c_i = m_i \oplus b$, for $i = 1, \dots, t$. Discuss the security of this system under each of the three kinds of attacks (from part (a) above). Where the system is insecure, describe carefully the sense in which it insecure. Be sure to say also how the security is affected by the choice of t.

Solution:

(a) **Ciphertext-only** Eve knows only c and tries to recover m. Eve is able to perform such attack if she has access to the communication channel between Alice and Bob, for example, if she controls the gateway through which Alice accesses the Internet.

Known plaintext Eve knows a sequence of plaintext-ciphertext pairs (m_1, c_1), …, (m_r, c_r). Now she obtains a new ciphertext $c \notin \{c_1, \dots, c_r\}$ and wants to recover the corresponding message m. Eve is able to perform such an attack if the previous plaintext-ciphertext pairs are revealed by Alice or Bob. Eve might also get information about the previous plaintext-ciphertext pairs by looking into Alice's swap files.

Chosen plaintext This is like a known plaintext attack, except that before getting c, Eve gets to choose messages m_1, …, m_r and somehow get Alice (or Bob) to encrypt them for her and supply her with the corresponding ciphertexts c_1, …, c_r. Eve is able to perform such attack if Alice is a server that provides encryption service. Eve can also perform such an attack on an asymmetric cryptosystem such as RSA where she has access to the public encryption key.

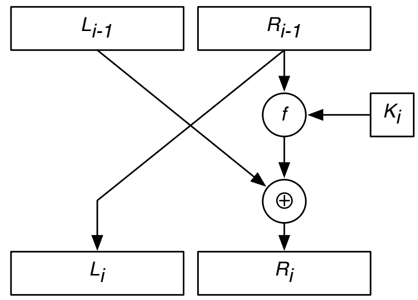
(b) **Ciphertext-only** When $t = 1$, this cryptosystem is information-theoretically secure. When $t > 1$, Eve is able to get partial information about the plaintext. In particular, if the ciphertext is $c = c_1 \dots c_t$, she knows that the plaintext is either c or $\bar{c}$ (the complement of c).

Known plaintext Whatever length the message is, one plaintext-ciphertext pair is sufficient to recover the key and break the cryptosystem.

Chosen plaintext A chosen plaintext attack is stronger than a known plaintext attack, so again, whatever length the message is, one plaintext-ciphertext pair is sufficient to recover the key and break the cryptosystem.

Problem 3: DES

Recall that the heart of DES is a round of the form:



Consider a simplified DES-like cryptosystem consisting of n such rounds, where the function f is defined by $f_K(X) = K \oplus X$. Here we assume that the key K is 32-bits long and that the same key is used at each round, that is, $K_i = K$ for each round i.

This system is used to encrypt a 64-bit message M as follows: L_0 is the leftmost 32-bits of M and R_0 is the rightmost 32-bits of M. The ciphertext $E_K(M)$ is $L_n \cdot R_n$.

(a) Describe how to decrypt messages encrypted with E_K.

(b) Express L_1, R_1, L_2, R_2 in terms of L_0, R_0, and K.

(c) Show why increasing the number of rounds n can actually decrease security.

Solution:

(a) This is a simplified DES-like cryptosystem. Like DES, decryption can be done by starting with the left and right halves of the ciphertext, L_n and R_n respectively, and working backwards round by round to the plaintext message $M = L_0 \cdot R_0$. In round i of encryption, the algorithm works as follows:

$$\begin{cases} L_{i+1} = R_i \\ R_{i+1} = L_i \oplus R_i \oplus K \end{cases} \tag{3}$$

To decrypt, we solve (3) to express L_i and R_i in terms of L_{i+1} and R_{i+1}. This yields

$$\begin{cases} L_i = L_{i+1} \oplus R_{i+1} \oplus K \\ R_i = L_{i+1} \end{cases} \tag{4}$$

Applying (4) for $i = n-1, n-2, \ldots, 0$ yields the desired plaintext.

We remark that, also like DES, the encryption and decryption functions for each round are almost the same. Let $E_K(L_i \cdot R_i) = L_{i+1} \cdot R_{i+1}$ be the encryption function defined by (3). Let $D_K(L_{i+1} \cdot R_{i+1}) = L_i \cdot R_i$ be the corresponding decryption function defined by (4). One can easily verify that

$$R_i \cdot L_i = E_K(R_{i+1} \cdot L_{i+1}). \tag{5}$$

Thus, if $S(L \cdot R) = R \cdot L$ is the function that swaps the left and right halves of its 64-bit argument, then it follows from (5) that

$$S(E_k(S(L_{i+1} \cdot R_{i+1}))) = L_i \cdot R_i = D_K(L_{i+1} \cdot R_{i+1}). \tag{6}$$

(b)

$$\begin{cases} L_1 = R_0 \\ R_1 = L_0 \oplus R_0 \oplus K \end{cases} \tag{7}$$

$$\begin{cases} L_2 = R_1 = L_0 \oplus R_0 \oplus K \\ R_2 = L_1 \oplus R_1 \oplus K = R_0 \oplus L_0 \oplus R_0 \oplus K \oplus K = L_0 \end{cases} \tag{8}$$

(c) If we continue the encryption to the third round, we will find that

$$\begin{cases} L_3 = R_2 = L_0 \\ R_3 = L_2 \oplus R_2 \oplus K = L_0 \oplus R_0 \oplus K \oplus L_0 \oplus K = R_0 \end{cases} \tag{9}$$

Therefore, increasing the number of rounds from 2 to 3 results in the ciphertext being identical to the plaintext, so there is no security at all.

Problem 4: Chaining Modes

Let (E, D) be a block cipher and let $m_1, m_2, \ldots, m_t$ be a sequence of t plaintext blocks. Happy Hacker was not happy with the chaining modes he learned about in CPSC 467, so he invented his own. He defines a sequence of $t + 2$ ciphertext blocks $c_0, c_1, c_2, \ldots, c_t, c_{t+1}$ which satisfies the equation

$$c_i = E_k(c_{i-1} \oplus m_i \oplus c_{i+1}), \text{ for } i = 1, \ldots, t.$$

(a) Describe how to reconstruct $m_1, \ldots, m_t$ given $c_0, \ldots, c_{t+1}$.

(b) Happy was having trouble figuring out how to compute the c_i's because of the cirular dependencies. Please help him by showing how to compute c_{i+1} from c_{i-1}, c_i, and m_i, where $1 \leq i \leq t$. How should he choose c_0 and c_1?

Solution:

(a) For $i = 1, \ldots, t$, we have the condition

$$c_i = E_k(c_{i-1} \oplus m_i \oplus c_{i+1}) \tag{10}$$

Applying decryption function to both sides of (10) gives

$$\begin{aligned} D_k(c_i) &= D_k(E_k(c_{i-1} \oplus m_i \oplus c_{i+1})) \\ &= c_{i-1} \oplus m_i \oplus c_{i+1} \end{aligned} \tag{11}$$

Adding (using $\oplus$) the expression $(\oplus c_{i-1} \oplus c_{i+1})$ to (11) and swapping the two sides gives

$$m_i = D_k(c_i) \oplus c_{i-1} \oplus c_{i+1} \tag{12}$$

(b) Adding (using $\oplus$) $(\oplus c_{i-1} \oplus m_i)$ to (11) and swapping the two sides gives

$$c_{i+1} = D_k(c_i) \oplus c_{i-1} \oplus m_i, \tag{13}$$

where $1 \leq i \leq t$. In order to get started, we set c_0 and c_1 to some fixed initialization vectors.

Problem 5: RSA

My toy RSA key is $N = 187, e = 107$. You observe a ciphertext $c = 2$. What is the plaintext? (Note: $187 = 11 * 17$.)

Solution:

Given $N = 187 = 11 \times 17$, it is easy to compute $\phi(N) = (11-1) \times (17-1) = 160$.

Next, given $e = 107$, which is relative prime to 160, we use extended Euclidean algorithm to compute d such that $ed \equiv 1 \pmod{107}$:

i	r_i	u_i	v_i	q_i
1	160	1	0	
2	107	0	1	1
3	53	1	-1	2
4	1	-2	3	

The result from the table is $d = v_4 = 3$.

Finally we apply the decryption function of RSA to get the plaintext

$$m = c^d \bmod N = 2^3 \bmod 187 = 8 \tag{14}$$

Problem 6: Euler's Theorem

(a) Define Euler's totient function $\phi(n)$, and state Euler's theorem.

(b) Calculate $2^{5^{49}} \bmod 29$.

(Hint: This problem is easily solved by hand using Euler's theorem to reduce the size of the exponents.)

Solution:

(a) Let $\mathbf{Z}_n^* = \{a \in \mathbf{Z}_n \mid \gcd(a, n) = 1\}$, then Euler's totient function $\phi(n)$ is the cardinality of $\mathbf{Z}_n^*$. If we represent an integer n by its prime factors as follows

$$n = \prod_i p_i^{e_i}, \tag{15}$$

then $\phi(n)$ can be calculated as

$$\phi(n) = \prod_i (p_i - 1) p_i^{e_i - 1}, \tag{16}$$

Euler's theorem says, for every x that is relative prime to n,

$$x^{\phi(n)} \equiv 1 \pmod{n} \tag{17}$$

(b) Given $n = 29$, it is easy to compute $\phi(29) = 29 - 1 = 28$, and $\phi(\phi(29)) = (2-1) \times 2^{2-1} \times (7-1) = 12$.

After verifying $\gcd(5, 28) = 1$, applying Euler's theorem gives

$$5^{49} = (5^{12})^4 \times 5^1 = (5^{\phi(28)})^4 \times 5^1 \equiv 5^1 \pmod{28} \tag{18}$$

Therefore after verifying $\gcd(2, 29) = 1$, we have

$$2^{5^{49}} \equiv 2^{5^1} \pmod{29}, \tag{19}$$

which implies $2^{5^{49}} \bmod 29 = 2^{5^1} \bmod 29 = 3$.