Symmetric Cryptosystems

Lesson 3

Initial examples

- Ex1: let p be a large prime, $2^{159} < p < 2^{160}$. $\mathrm{K} = \mathcal{M} = \mathrm{C} = Z_p^*$.

$$E_k(m) \equiv k * m \ (mod\ p)$$
$$D_k(c) \equiv k' * c \ (mod\ p)$$

- Ex2: let $\mathrm{K}, \mathcal{M}, \mathrm{C} = \{0, 1, \ldots, 2^B - 1\}$ be the sets of all binary strings of length B.

$$E_k(m) = k \oplus m$$
$$D_k(c) = k \oplus c$$

Analysis

If $(\mathrm{K}, \mathcal{M}, \mathrm{C}, E, D)$ is to be a successful cipher, it must have the following properties (Kerckhoff principal):

1. For any $\mathrm{k} \in \mathrm{K}$, $\mathrm{m} \in \mathcal{M}$, it must be easy to compute the cipher text $E_k(m)$.
2. For any $\mathrm{k} \in \mathrm{K}$, $\mathrm{c} \in \mathrm{C}$, it must be easy to compute the plaintext $D_k(c)$.
3. Given one or more $\mathrm{c}_1, \mathrm{c}_2, \dots, \mathrm{c}_\mathrm{n} \in \mathrm{C}$ are encrypted using $\mathrm{k} \in \mathrm{K}$, it must be difficult to compute any of the corresponding plaintexts $D_k(c_1), D_k(c_2), \dots, D_k(c_n)$ without knowing k.
4. Given one or more pairs $(m_1, c_1), \dots (m_n, c_n)$, it must be difficult to decrypt any cipher c that is not in the given list without knowing k (chosen plaintext attack).

Analysis…

- Ex1: $E_k(m) \equiv k * m \ (mod\ p).$ It doesn't have Property 4 (chosen cipher/plaintext attack).

- Ex2: $E_k(m) = k \oplus m$ (chosen plaintext attack)

Random bit sequences…

Suppose that we could construct a function $R: K \times \mathbb{Z} \to \{0,1\}$ with the following properties:

1. For all $\mathrm{k} \in K$, $\mathrm{j} \in \mathbb{Z}$, it is easy to compute R(k, j).
2. Given an arbitrarily long sequence of integer $j_1, \ldots, j_n$ and given all of values $R(k, j_1), \ldots, R(k, j_n)$, it is hard to determine k.
3. Given any list $j_1, \ldots, j_n$and given all of $R(k, j_1), \ldots, R(k, j_n)$, it is had to guess the value of $R(k, j)$ with better than 50% chance of success for any j not already in the list.

…and symmetric cipher

- There are two basic approaches to constructing candidates for R, and these two methods provide a good illustration of the fundamental conflict in cryptography between security and efficiency.
- The first approach is to repeatedly apply an ad hoc collection of mixing operations that are well suited to efficient computation and that appear to be very hard to untangle. This method is the basic of all most modern symmetric cryptosystems (DES, AES, …)
- The second approach is to construct R using a function whose efficient inversion is a well-known mathematical problem that is believed to be difficult. This method is less attractive for real-world ciphers.

Modern symmetric cryptosystems

- DES – Data Encryption Standard (IBM,1970).
- DES uses a 56-bit key and encrypts blocks of 64 bits at a time.
- DES mixing operations are linear, with the only nonlinear component being the use of eight S-box (Substitution box).
- Each S-box is a look-up table in which six input bits are replaced by four output bit.

DES S-Box

- Here is how an S-box is used. The input is a list of 6 bit Input = $\beta_1\beta_2\beta_3\beta_4\beta_5\beta_{6.}$
- First use the 2-bit binary number $\beta_1\beta_6$ to choose the row of the S-box, then use the 4-bit binary number $\beta_2\beta_3\beta_4\beta_5$ to choose the column of the S-box.
- The output is the entry of the S-box for the chosen row and column, and converted into a 4-bit binary number.

S-box and Example

- Suppose that Input = ‘110010’. ‘10’ = 2 → use row 2, and ‘1001’ = 9, use column 9. Output will be 12 = 1100.
- S-box(x) = F(A(x)) where A: affine, F(x):non-linear function.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	**12**	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Advanced Encryption Standard

- AES (J. Daemen and V. Rijmen, 2000). A block cipher in which the plaintext-cipher text blocks are 128 bits in length and the key size may be 128, 192, 256 bits.
- AES is similar to DES in hat it encrypts/decrypts by repeating a basic operation several times (10, 12, or 14 rounds depending on the size key).
- AES S-box is constructed using the operation of taking multiplication inverses in the field $F_2{}^8$.

block cipher mode of operation

Mode		Formulas	Ciphertext
Electronic codebook	(ECB)	Y_i = F(PlainText$_i$, Key)	Y_i
Cipher block chaining	(CBC)	Y_i = PlainText$_i$ XOR Ciphertext$_{i-1}$	F(Y, Key); Ciphertext$_0$ = IV
Propagating CBC	(PCBC)	Y_i = PlainText$_i$ XOR (Ciphertext$_{i-1}$ XOR PlainText$_{i-1}$)	F(Y, Key); Ciphertext$_0$ = IV
Cipher feedback	(CFB)	Y_i = Ciphertext$_{i-1}$	Plaintext XOR F(Y, Key); Ciphertext$_0$ = IV
Output feedback	(OFB)	Y_i = F(Y_{i-1}, Key); Y_0 = F(IV, Key)	Plaintext XOR Y_i
Counter	(CTR)	Y_i = F(IV + $g(i)$, Key); IV = token()	Plaintext XOR Y_i