MAS433 Cryptography: Tutorial 2
Information Theory, Block Cipher (DES, AES)
22.09.2010

Problem 1. One-time Pad

1.1. For the bit-wise one-time pad, the encryption is performed as: $C_i = K_i \oplus P_i = (K_i + P_i) \bmod 2$. Now an encryption system operates as: $C_i = K_i + P_i$. How to attack this modified one-time pad?

Solution Outline. If $C_i = 0$, then $P_i = 0$. If $C_i = 2$, then $P_i = 1$.

1.2. Show that the above modified one-time pad encryption scheme is not perfectly secure.

Solution Outline. $\mathbf{Pr}[P|C = 0] = 1$, $\mathbf{Pr}[P|C = 2] = 1$. For perfect secrecy, we need to have $\mathbf{Pr}[P|C = c] = \mathbf{Pr}[P]$ for any ciphertext c.

Problem 2. Information Theory, Entropy

Let the plaintext space $\mathbf{P} = \{\beta_1, \beta_2\}$ with $\mathbf{Pr}[P = \beta_1] = 1/4$, $\mathbf{Pr}[P = \beta_2] = 3/4$. Let $\mathbf{K} = \{\gamma_1, \gamma_2, \gamma_3\}$ with $\mathbf{Pr}[K = \gamma_1] = 1/2$, $\mathbf{Pr}[K = \gamma_2] = \mathbf{Pr}[K = \gamma_3] = 1/4$. The encryption is performed as follows:

$$\begin{array}{l} E_{\gamma_1}(\beta_1) = \phi_1,\ E_{\gamma_1}(\beta_2) = \phi_2, \\ E_{\gamma_2}(\beta_1) = \phi_2,\ E_{\gamma_2}(\beta_2) = \phi_3, \\ E_{\gamma_3}(\beta_1) = \phi_3,\ E_{\gamma_3}(\beta_2) = \phi_4, \end{array}$$

2.1. Compute the probabilities $\mathbf{Pr}[C = \phi_i]$ for $i = 1, 2, 3, 4$.

Solution Outline.

$$\begin{aligned} \mathbf{Pr}[C = \phi_1] &= \mathbf{Pr}[\gamma_1] \times \mathbf{Pr}[\beta_1] \\ &= 1/2 \times 1/4 \\ &= 1/8 \end{aligned}$$

$$\begin{aligned} \mathbf{Pr}[C = \phi_2] &= \mathbf{Pr}[\gamma_2] \times \mathbf{Pr}[\beta_1] + \mathbf{Pr}[\gamma_1] \times \mathbf{Pr}[\beta_2] \\ &= 1/4 \times 1/4 + 1/2 \times 3/4 \\ &= 7/16 \end{aligned}$$

Similarly,

$\mathbf{Pr}[C = \phi_3] = 1/4$

$\mathbf{Pr}[C = \phi_4] = 3/16$

2.2. Compute the entropy of **P**, **K** and **C**.
Solution Outline.

$$\begin{aligned} H(\mathbf{P}) &= -\mathbf{Pr}[P = \beta_1]\log_2\mathbf{Pr}[P = \beta_1] - \mathbf{Pr}[P = \beta_2]\log_2\mathbf{Pr}[P = \beta_2] \\ &= -\frac{1}{4}\log_2(\frac{1}{4}) - \frac{3}{4}\log_2(\frac{3}{4}) \\ &\approx 0.81 \end{aligned}$$

Similarly,
$H(\mathbf{K}) = 1.5$
$H(\mathbf{C}) \approx 1.85$

2.3. Compute the conditional probabilities $\mathbf{Pr}[\beta_i|\phi_j]$ for $i = 1, 2$, $1 \leq j \leq 4$.
Solution Outline.

$$\mathbf{Pr}[\beta_1|\phi_1] = 1; \mathbf{Pr}[\beta_2|\phi_1] = 0$$

$$\begin{aligned} \mathbf{Pr}[\beta_1|\phi_2] &= \frac{\mathbf{Pr}[\gamma_2] \times \mathbf{Pr}[\beta_1]}{\mathbf{Pr}[\gamma_2] \times \mathbf{Pr}[\beta_1] + \mathbf{Pr}[\gamma_1] \times \mathbf{Pr}[\beta_2]} \\ &= \frac{1}{7} \end{aligned}$$

Similarly,
$\mathbf{Pr}[\beta_2|\phi_2] = \frac{6}{7}$;
$\mathbf{Pr}[\beta_1|\phi_3] = \frac{1}{4}$;
$\mathbf{Pr}[\beta_2|\phi_3] = \frac{3}{4}$;
$\mathbf{Pr}[\beta_1|\phi_4] = 0$;
$\mathbf{Pr}[\beta_2|\phi_4] = 1$;

2.4. Compute the entropy of **P** if the ciphertext is given as ϕ_i $(1 \leq i \leq 4)$. Are these results different from the entropy of **P**? Why?
Solution Outline.
For $C = \phi_1$, $H(P) = -0 \times \log_2 0 - 1 \times \log_2 1 = 0$;
For $C = \phi_2$, $H(P) = -1/7 \times \log_2 1/7 - 6/7 \times \log_2 6/7 = 0.59$;
For $C = \phi_3$, $H(P) = -1/4 \times \log_2 1/4 - 3/4 \times \log_2 3/4 = 0.81$;
For $C = \phi_4$, $H(P) = -0 \times \log_2 0 - 1 \times \log_2 1 = 0$;
For $C = \phi_3$, the value of $H(P)$ is the same as the value of $H(P)$ before C is given. It means that when an attacker receives ϕ_3, no information of the plaintext is leaked to the attacker. The reason is that for any given plaintext (β_1 or β_2), the probabilities that they will be encrypted to ϕ_3 are equal that they will be encrypted to ϕ_3 since $\mathbf{Pr}[K = \gamma_2] = \mathbf{Pr}[K = \gamma_3]$.
For $C = \phi_1, \phi_2, \phi_4$, the values of $H(P)$ are less than the value of $H(P)$ before C is given. It indicates that some information of the plaintext is leaked to the attacker.

Subject: Date:

3.1 Solution.

$$\log_2 |K| = \log_2 (n!)$$
$$\approx \log_2 \left(\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\right)$$
$$= \log_2 \sqrt{2\pi} + 0.5 \log_2 n + n \log_2 \left(\frac{n}{e}\right)$$
$$\approx (0.5+n)\log_2 n - 1.44 n + 1.33$$

$$\log_2 |P| = \log_2 n$$

$$n_0 \approx \frac{\log_2 |K|}{R_L \log_2 |P|}$$
$$\approx \frac{(0.5+n)\log_2 n - 1.44 n + 1.33}{R_L \log_2 n}$$
$$\approx \frac{1}{R_L}\left(n + 0.5 + \frac{1.33 - 1.44 n}{\log_2 n}\right)$$

3.2 Solution.

For m-gram substitution cipher, the plaintext space's size n is

$$n = 26^m$$

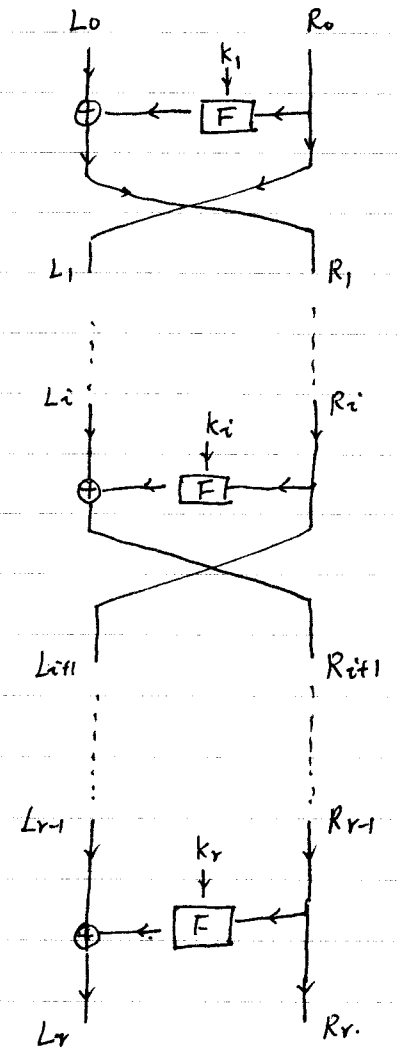
$$\therefore \quad n_0 \approx \frac{1}{R_L}\left(n + 0.5 + \frac{1.33 - 1.44 n}{\log_2 n}\right)$$
$$= \frac{1}{0.75}\left(26^m + 0.5 + \frac{1.33 - 1.44 \times 26^m}{m \log_2 26}\right)$$

For large value of m,

$$n_0 \approx \frac{1}{0.75} 26^m \approx 1.33 \times 26^m$$

Subject: Date:

4.1 Solution.



$P = (L_0, R_0)$

$C = (L_r, R_r)$

4.2 Solution. For Feistel network, for given (L_{i+1}, R_{i+1}), we can always ~~Compute~~ obtain (L_i, R_i) as follows:

$$R_i = L_{i+1}$$

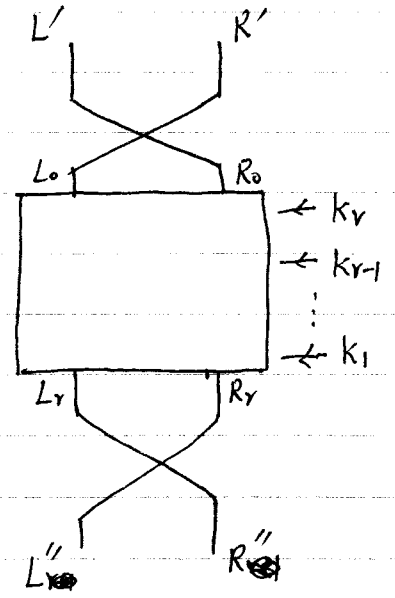
$$L_i = R_{i+1} \oplus F(k_i, R_i) = R_{i+1} \oplus F(k_i, L_{i+1})$$

Subject : Date

4.3 Solution.

To reuse the encryption algorithm for decryption, the following extra operations are needed:

1) Reverse the order of the round keys
2) Swap the left and right halves of the input
3) Swap the left and right halves of the output



$C = (L', R')$

$P = (L'', R'')$

Subject : Date :

5.1 Solution.

$$K_i = \overline{k_i'}$$

Reason: The DES key schedule does not modify the value of each key bit.

5.2 Solution. Let $C = E_K(P)$, $C' = E_{K'}(P')$, $K = \overline{K'}$, $P = \overline{P'}$

1) The initial permutation of DES does not affect the value of each plaintext bit. Let (L_0, R_0) represent the value after IP.
If $P = \overline{P'}$, then $L_0 = \overline{L_0'}$, $R_0 = \overline{R_0'}$

2) If $L_i = \overline{L_i'}$, $R_i = \overline{R_i'}$, $k_i = \overline{k_i'}$

Then $L_{i+1} = R_i$ ① and $L_{i+1}' = R_i'$ ② $\rightarrow L_{i+1} = \overline{L_{i+1}'}$ ③

$$R_{i+1} = L_i \oplus F(K_i, R_i) \quad ④$$

$$\begin{aligned} R_{i+1}' &= L_i' \oplus F(k_i', R_i') \\ &= L_i' \oplus \text{Permutation}(\text{Substitution}(\text{Expansion}(R_i') \oplus k_i')) \\ &= L_i' \oplus \text{Permutation}(\text{Substitution}(\text{Expansion}(R_i) \oplus k_i)) \\ &= L_i' \oplus F(k_i, R_i) \quad ⑤ \end{aligned}$$

From ④ & ⑤, $R_{i+1} = \overline{R_{i+1}'}$ ⑥

From ③ & ⑥, we know that $L_{16} = \overline{L_{16}'}$; $R_{16} = \overline{R_{16}'}$

3) The final permutation of DES does not affect the value of each bit of (L_{16}, R_{16}), thus $C = \overline{C'}$

Subject: Date:

5.3 Solution.

Suppose an attacker knows $E_k(P)$ & $E_k(\bar{P})$

Step 1. The attacker guess k_x

Step 2. The attacker computes $E_{k_x}(P)$

Step 3. The attacker compares $E_{k_x}(P)$ with $E_k(P)$. If they are equal, then likely $k_x = k$.

Step 4. The attacker compares ~~$E_{k_x}(P)$~~ $\overline{E_{k_x}(P)}$ with $E_k(\bar{P})$. If they are equal, then likely ~~k_x~~ $k = \bar{k}_x$. (Reason: $\overline{E_{k_x}(P)} = E_{\bar{k}_x}(\bar{P})$)

Step 5. If k_x is incorrect, go back to step 1 to try another key.

In the above attack, with only one DES computation, an attacker can test two keys: k_x & $\bar{k}_x$. The complexity of the brute force attack is reduced by half.

Remarks: ① ~~To search~~ Trying all the DES keys requires 2^{56} DES operations.

② In average, the brute force attack on DES requires 2^{55} DES operations (try 2^{55} keys) The reason is that a key would be found before the whole key space is tested.

③ With the ~~speed up~~ method in 5.3), the attack on DES requires 2^{54} DES operations on average.

5.4 Solution. We can apply some non-linear operations to the round keys. For example, applying 4x4-bit Sbox to the round keys.

Subject: Date:

6.1 Solution:

The MixColumns and ShiftRows operations in AES are linear, so they have the following properties:

$$\text{MixColumns}(a \oplus b) = \text{MixColumns}(a) \oplus \text{MixColumns}(b)$$
$$\text{ShiftRows}(a \oplus b) = \text{ShiftRows}(a) \oplus \text{ShiftRows}(b),$$

where a and b are 128-bit AES states.

Now, if SubByte operations are not implemented, the first Round is

$$\begin{aligned} & K_1 \oplus (\text{MixColumns}(\text{ShiftRows}(P \oplus K_0))) \\ = \; & \text{MixColumns}(\text{ShiftRows}(P)) \oplus (K_1 \oplus \text{MixColumns}(\text{ShiftRows}(K_0))) \\ = \; & f(P) \oplus f'(K_0, K_1) \end{aligned}$$

~~After 10 rounds (AES-128)~~.

The ciphertext can be expressed as:

$$C = g(P) \oplus h(K_0, K_1, \ldots)$$
$$C = g(P) \oplus K'$$

It is similar to one-time pad, but the key is repeatedly used. With one plaintext – ciphertext pair, K' can be determined, and the rest of the ciphertext can be recovered.

Subject: Date:

6.2 Solution.

If the ShiftRows operations are not implemented, each column of AES gets encrypted independently (Those four columns never affect each other). We obtain four small block ciphers with 32-bit block size. The block size is too small and it's vulnerable to dictionary attack (an attacker can collect enough plaintext-ciphertext pairs, then decrypt the rest of the ciphertext).

6.3 Solution.

If the MixColumns operations are not implemented, each byte in the state of AES gets encrypted independently. We obtain 16 small block ciphers with 8-bit block size.

Subject: Date:

7.1 Solution. $\{83\} = 1000011 = x^7+x+1$

Step 1. $x^8+x^4+x^3+x+1$ → a

Step 2. x^7+x+1 → b.

Step 3. $(x^8+x^4+x^3+x+1) \div (x^7+x+1) \Rightarrow$

$x^4+x^3+x^2+1 = (x^8+x^4+x^3+x+1) + (x^7+x+1)\,x$

d = a + b·c

Step 4. $(x^7+x+1) \div (x^4+x^3+x^2+1) \Rightarrow$

$x = (x^7+x+1) + (x^4+x^3+x^2+1)(x^3+x^2+1)$

e = b + d·f

Step 5. $(x^4+x^3+x^2+1) \div x \Rightarrow$

$1 = (x^4+x^3+x^2+1) + (x^3+x^2+x)\cdot x$

1 = d + h·e

Step 6. $1 = d+e\cdot h = d+(b+df)\cdot h$

$= d(1+fh)+bh$

$= (a+bc)(1+fh)+bh$

$= a(1+fh)+b(c+cfh+h)$

$\therefore b^{-1} = c+cfh+h = x+x(x^3+x^2+1)(x^3+x^2+x)+(x^3+x^2+x)$

$= x^7 = \{80\}$

Subject: Date:

7.2 Solution.

$$a(x) \bullet b(x) \bmod x^4+1$$
$$= (\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}) \bullet \{A5\}x \bmod x^4+1$$
$$= \{01\}\bullet\{A5\}x^3+\{01\}\bullet\{A5\}x^2+\{02\}\bullet\{A5\}x+\{03\}\bullet\{A5\}$$

$$\{01\}\bullet\{A5\} = \{A5\}$$
$$\{02\}\bullet\{A5\} = x(x^7+x^5+x^2+1) \bmod (x^8+x^4+x^3+x+1)$$
$$= x^6+x^4+1 = \{51\}$$
$$\{03\}\bullet\{A5\}$$
$$= \{01\}\bullet\{A5\} \oplus \{02\}\bullet\{A5\}$$
$$= \{A5\} \oplus \{51\}$$
$$= \{F4\}$$

$\{A5\}$: 10100101
$\{51\}$: 01010001
11110100