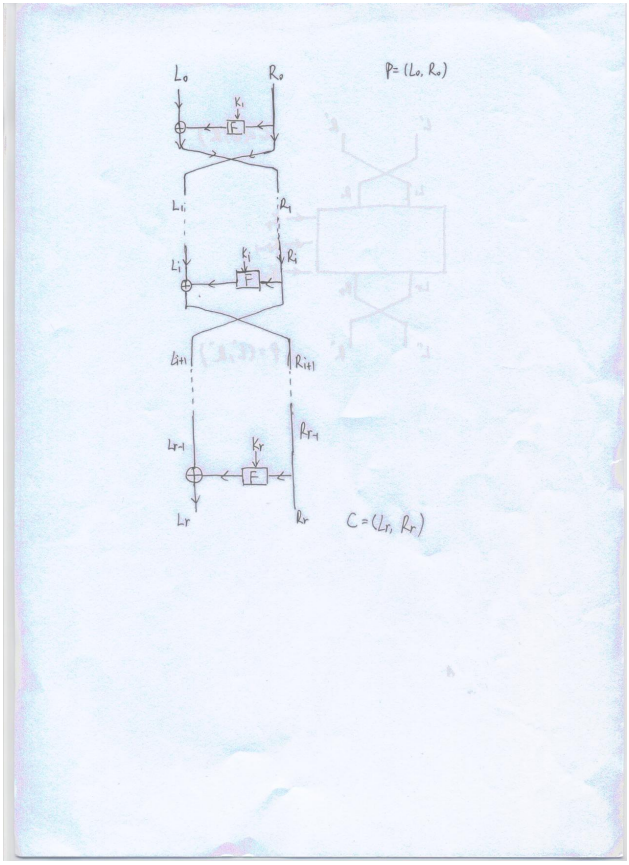
MAS 433 Tutorial 3

Wang Xueou (087199E16)

September 14, 2011

Question 1 Solution:
1.1.



1.2. For Feistel network, if we have known $L_i \& R_i$, we can always get $L_{i-1} \& R_{i-1}$ using the following way:

$$\begin{aligned} R_{i-1} &= L_i \\ L_{i-1} &= F(K_i, R_{i-1}) \oplus R_i = F(K_i, L_i) \oplus R_i \end{aligned}$$

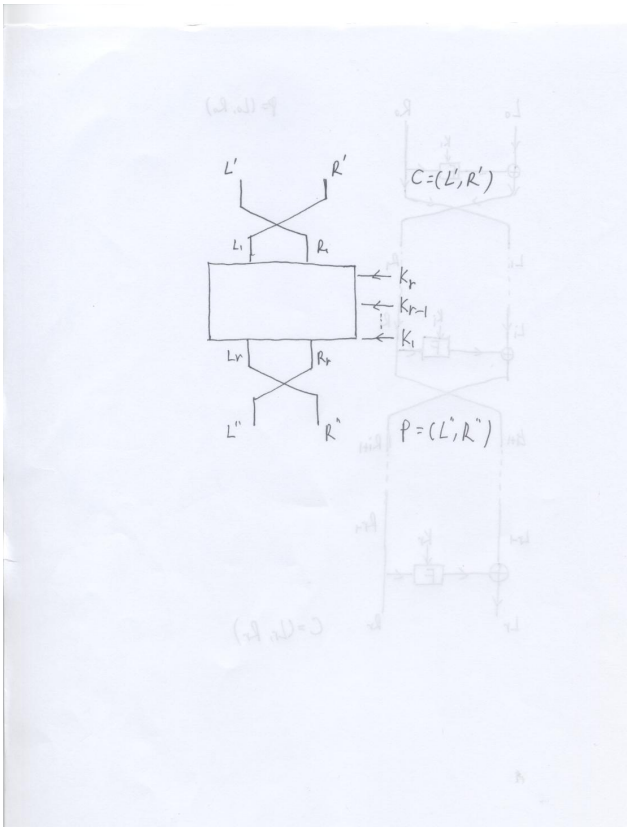
Thus, the Feistel network is always invertible.

1.3. We need 3 extra operations if we re-use the encryption algorithm:

(1). Reverse the order of input.

(2). Reverse the order of round key.

(3). Reverse the order of output



Question 2. Solution:

2.1. The relation between K_i and K_i' is

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

The reason is $K = \overline{K'}$, while DES doesn't modify the key bits of those K_i 's (K_i''s) generated from $K\,(K')$

2.2.

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

• The initial permutation doesn't change the bits of P. Let (L_0, R_0) & (L_0', R_0') denote the initial permutation. Since $P = \overline{P'}$, we have $L_0 = \overline{L_0'}, R_0 = \overline{R_0'}$

• If $L_i = \overline{L_i'}, R_i = \overline{R_i'}$

$$\begin{aligned}
L_{i+1} &= R_i && (1)\\
R_{i+1} &= L_i \oplus F(K_{i+1}, R_i) && (2)\\
L_{i+1}' &= R_i' && (3)\\
R_{i+1}' &= L_i' \oplus F\left(K_{i+1}', R_i'\right)\\
&= L_i' \oplus \text{Permutation}\left(\text{Substitution}\left(\text{Expansion}\left(R_i'\right) \oplus K_{i+1}'\right)\right)\\
&= L_i' \oplus \text{Permutation}\left(\text{Substitution}\left(\text{Expansion}\left(R_i\right) \oplus K_{i+1}\right)\right)\\
&= L_i' \oplus F(K_{i+1}, R_i) && (4)
\end{aligned}$$

$$\left.\begin{matrix}(1)\\(3)\end{matrix}\right\} \quad \Rightarrow \quad L_{i+1} = \overline{L_{i+1}'}$$

From (2) & (4), we have $R_{i+1}' = \overline{R_{i+1}'}$. Thus we have $L_{16} = \overline{L_{16}'}$ & $R_{16} = \overline{R_{16}'}$

• In the last permutation, we have $C = (R_{16}, L_{16})$, and $C' = (R_{16}', L_{16}')$. However, this permutation doestn't change the bits, then we have $C = \overline{C'}$.

2.3. Suppose the attacker knows C and C', where $C = E_K(P)$ & $C' = E_K(\overline{P})$. Then he can attack as follows:

Step1. Guess K_{x}.

Step2. Compute $E_{K_{\text{x}}}(P)$

Step3. Compare $E_{K_{\text{x}}}(P)$ with $E_K(P)$. If they are equal, then likely $K_{\text{x}} = K$.

Step4. Compare $\overline{E_{K_{\text{x}}}(P)}$ with $E_K(\overline{P})$. If they are equal, then likely $K = \overline{K_{\text{x}}}$ because $\overline{E_{K_{\text{x}}}(P)} = E_{\overline{K_{\text{x}}}}(\overline{P})$.

Step5. If K_{x} is incorrect, go back to step 1 to try another key.

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

Question 3 Solution: If there is an even number of 1's in K_b, the final cipher is just as the one without using K_b. If there is an odd number of 1's in K_b, the final cipher is then equivalent to the cipher without the second permutation after the last round. This can be risky.

Question 4 Solution:

4.1. In the first round, the MixColumn function makes each byte affect 4 outputs as a column. In the second round, ShiftRow function proceeds the MixColumn function and spreads the elements in one column over 4 columns. Then the again makes each byte affect 4 outputs in a column. So 2 rounds can make each byte affect all the 16 outputs.

4.2. Since the MixColumns and ShiftRows operations in AES are linear, they have the following properties:

$$\begin{aligned} \text{MixColumns}(a \oplus b) &= \text{MixColumns}(a) \oplus \text{MixColumns}(b) \\ \text{ShiftRows}(a \oplus b) &= \text{ShiftRows}(a) \oplus \text{ShiftRows}(b) \end{aligned}$$

where a and b are 128-bit AES states.

Now, if SubByte operations are not implemented, initially we apply AddRoundKey and get

$$C_0 = P \oplus K_0$$

Then the first round is

$$\begin{aligned} & \text{AddRoundKey}((\text{MixColumns}(\text{ShiftRows}(C_0)))) \\ = \; & K_1 \oplus (\text{MixColumns}(\text{ShiftRows}(P \oplus K_0))) \\ = \; & K_1 \oplus \text{MixColumns}(\text{ShiftRows}(P)) \oplus \text{MixColumns}(\text{ShiftRows}(K_0)) \\ = \; & \text{MixColumns}(\text{ShiftRows}(P)) \oplus (K_1 \oplus \text{MixColumns}(\text{ShiftRows}(K_0))) \\ = \; & f(p) + f'(K_0, K_1) \end{aligned}$$

After we perform all the rounds, we will get the ciphertext as

$$C = g(P) \oplus h(K_0, K_1, \cdots)$$

i.e.,

$$C = g(P) \oplus K', \text{ where } K' = h(K_0, K_1, \cdots)$$

Since h is the composite of linear functions, h is also a linear function. It is similar to the one-time pad, but the key is repeatedly used for different plaintext block. Thus, with one plaintext-ciphertext pair, K' can be determined, and the rest of the plaintext can be recovered.

4.3. If ShiftRows is not implemented, then the 4 elements in one column are not relocated to 4 different columns and encrypted independently during the subsequent enctryption. So we can obtain 4 block ciphers each of which is 32-bit size. Since the block size is too small, it is subject to dictionary attack. The attacker may collect many plaintext-ciphertext pair and build a dictionary between them and get the full plaintext.

4.4. If MixColumns is not implemented, the input byte will not affect all four outputs. This means each byte is encrypted independently so we get 16 block of 8-bit size cipher. This is vulnerable to dictionary attack.

Question 5 Solution:

5.1. $\{09\} = 00001001 = x^3 + 1, \{82\} = 10000010 = x^7 + x$, then

$$\begin{aligned} (x^3+1) \bullet (x^7+x) &= x^{10} + x^7 + x^4 + x \\ x^{10} + x^7 + x^4 + x \mod & x^8 + x^4 + x^3 + x + 1 \\ &= x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x \\ &= 11111110 \end{aligned}$$

$$\text{So} \qquad \{09\} \bullet \{82\} = \{fe\}$$

5.2. $\{09\} = 00001001 = x^3 + 1$. Use Extended Euclidean Algorithm, we have the following:

$$\begin{array}{lllll} \text{Step1.} & (x^8 + x^4 + x^3 + x + 1) \div (x^3 + 1): & x^2 & = & (x^8 + x^4 + x^3 + x + 1) + (x^3 + 1)(x^5 + x^2 + x + 1) \\ \text{Step2.} & x^3 \div x^2: & 1 & = & (x^3 + 1) + (x^2)(x) \end{array}$$

Thus we have:

$$\begin{array}{rcl} 1 & = & (x^3 + 1) + x[(x^8 + x^4 + x^3 + x + 1) + (x^3 + 1)(x^5 + x^2 + x + 1)] \\ & = & (x^3 + 1)(x^6 + x^3 + x^2 + x + 1) + (x^8 + x^4 + x^3 + x + 1)x \end{array}$$

Thus, $\{09\}^{-1} = 01001111 = \{4f\}$

5.3.

$$\begin{array}{rcl} a(x) \otimes b(x) & = & a(x) \bullet b(x) \bmod x^4 + 1 \\ & = & (\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}) \bullet \{A3\}x \bmod x^4 + 1 \\ & = & \{01\} \bullet \{A3\}x^3 + \{01\} \bullet \{A3\}x^2 + \{02\} \bullet \{A3\}x + \{03\} \bullet \{A3\} \end{array}$$

Further, we have

$$\begin{array}{rcl} \{01\} \bullet \{A3\} & = & \{A3\} \\ \{02\} \bullet \{A3\} & = & x(x^7 + x^5 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1) \\ & = & x^6 + x^4 + x^3 + x^2 + 1 \\ & = & 01011101 \\ & = & \{5d\} \\ \{03\} \bullet \{A3\} & = & \{01\} \bullet \{A3\} \oplus \{02\} \bullet \{A3\} \\ & = & 10100011 \oplus 01011101 \\ & = & 11111110 \\ & = & \{fe\} \end{array}$$

So $a(x) \otimes b(x) = \{A3\}x^3 + \{A3\}x^2 + \{5d\}x + \{fe\}$

5.4. Let

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0 = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

$$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0 = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$$

To prove $b(x) = a^{-1}(x)$, we need to show $a(x)b(x) + (x^4 + 1)c(x) = 1 \bmod x^4 + 1$. Now let

$$\begin{array}{rcl} d(x) & = & a(x)b(x) \bmod x^4 + 1 \\ & = & d_3x^3 + d_2x^2 + d_1x^1 + d_0 \end{array}$$

We have

$$
\begin{aligned}
d_0 &= (a_0 \bullet b_0) \oplus (a_3 \bullet b_1) \oplus (a_2 \bullet b_2) \oplus (a_1 \bullet b_3) \\
&= \{02\} \bullet \{0e\} \oplus \{03\} \bullet \{09\} \oplus \{01\} \bullet \{0d\} \oplus \{01\} \bullet \{0b\} \\
&= \{1c\} \oplus \{1b\} \oplus \{0d\} \oplus \{0b\} \\
&= \{00011100\} \oplus \{00011011\} \oplus \{00001101\} \oplus \{00001011\} \\
&= 1 \\
d_1 &= (a_1 \bullet b_0) \oplus (a_0 \bullet b_1) \oplus (a_3 \bullet b_2) \oplus (a_2 \bullet b_3) \\
&= \{01\} \bullet \{0e\} \oplus \{02\} \bullet \{09\} \oplus \{03\} \bullet \{0d\} \oplus \{01\} \bullet \{0b\} \\
&= \{0e\} \oplus \{12\} \oplus \{17\} \oplus \{0b\} \\
&= \{00001110\} \oplus \{00010010\} \oplus \{00010111\} \oplus \{00001011\} \\
&= 0 \\
d_2 &= (a_2 \bullet b_0) \oplus (a_1 \bullet b_1) \oplus (a_0 \bullet b_2) \oplus (a_3 \bullet b_3) \\
&= \{0e\} \oplus \{09\} \oplus \{1a\} \oplus \{1d\} \\
&= \{00001110\} \oplus \{00001001\} \oplus \{00011010\} \oplus \{00011101\} \\
&= 0 \\
d_3 &= (a_3 \bullet b_0) \oplus (a_2 \bullet b_1) \oplus (a_1 \bullet b_2) \oplus (a_0 \bullet b_3) \\
&= \{03\} \bullet \{0e\} \oplus \{01\} \bullet \{09\} \oplus \{01\} \bullet \{0d\} \oplus \{02\} \bullet \{0b\} \\
&= \{12\} \oplus \{09\} \oplus \{0d\} \oplus \{16\} \\
&= \{00010010\} \oplus \{00001001\} \oplus \{00001101\} \oplus \{00010110\} \\
&= 0
\end{aligned}
$$