MAS 433 Tutorial 4

Wang Xueou (087199E16)

September 22, 2011

Question 1 Solution:

1.1.

EBC: One block would be decrypted wrongly. Since each ciphertext block is decrypted independently, this ciphertext block doesnt't affect other ciphertext blocks decryption.

CBC: Two blocks would be decrypted wrongly. Since one ciphertext block is used in the next ciphertext block's decryption, both this ciphertext block and the next ciphertext block's decryption would be affected.

CFB: Two blocks would be decrypted wrongly. Since one ciphertext block is used in the next ciphertext block's decryption, both this ciphertext block and the next ciphertext block's decryption would be affected.

OFB: One block would be decrypted wrongly. Since each ciphertext block is decrypted independently, this ciphertext block doesnt't affect other ciphertext blocks decryption.

CTR: One block would be decrypted wrongly. Since each ciphertext block is decrypted independently, this ciphertext block doesnt't affect other ciphertext blocks decryption.

1.2.

From $C_i = E_K(P_i) \oplus C_{i-1}$, we can get

$$C_i \oplus C_{i-1} = E_K(P_i)$$

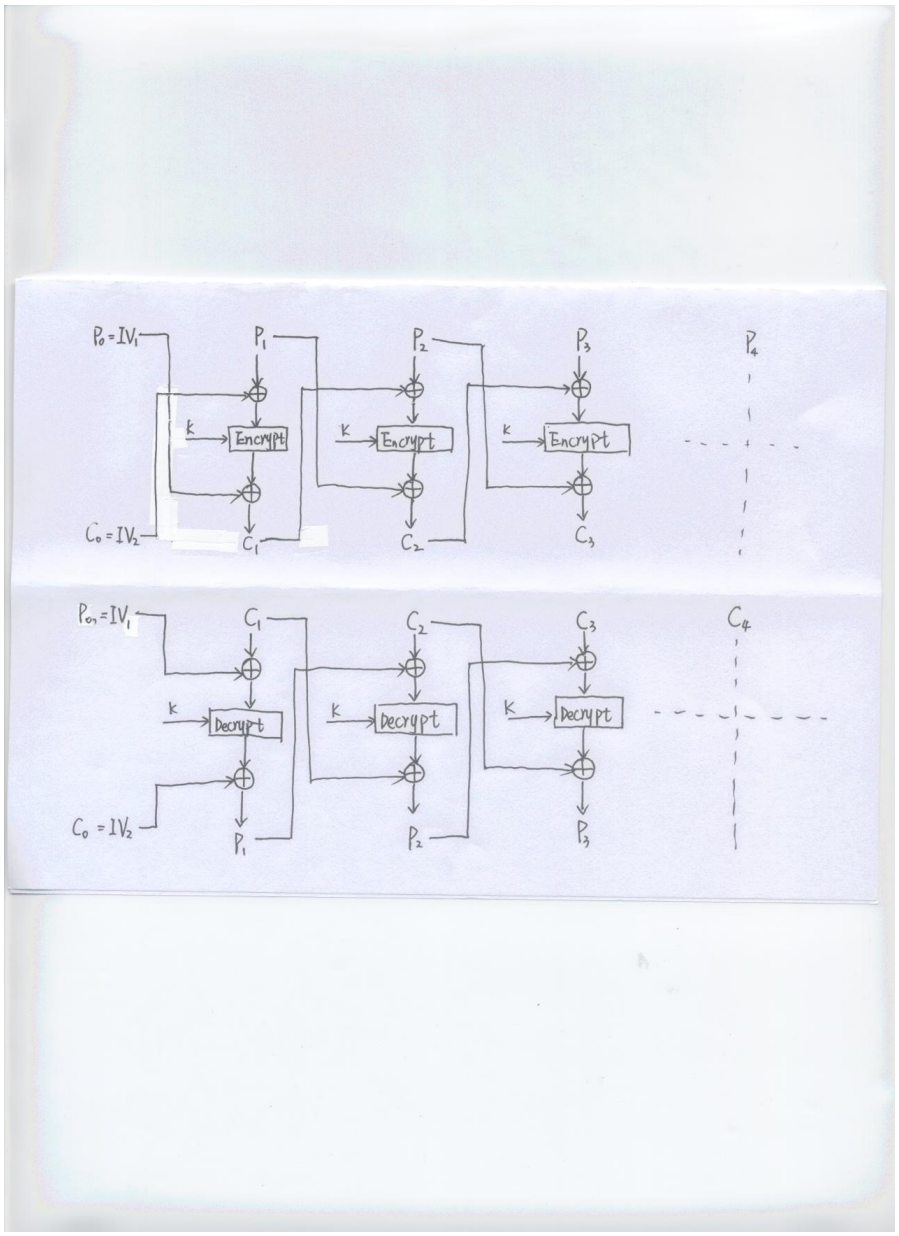
If we let $C'_i = C_i \oplus C_{i-1}$, then for $i \geq 1$, we get a cipher using the cipher we know, i.e.

$$C'_0 = IV_1, C'_i = E_K(P_i) \text{ for } i \geq 1$$

Now we can see this mode of operation is almost the same as ECB.

1.3.

The encryption and decryption diagram is as follows:


P0 = IV1
P1
P2
P3
P4
K
Encrypt
Encrypt
Encrypt
C0 = IV2
C1
C2
C3
P0 = IV1
C1
C2
C3
C4
K
Decrypt
Decrypt
Decrypt
C0 = IV2
P1
P2
P3

For decryption, we have:

$$P_0 = IV_1, P_i = E_K^{-1}(C_i \oplus P_{i-1}) \oplus C_{i-1} \text{ for } i \geq 1$$

Error propagation: If there is an error in C_i, then all the blocks $C_{i+j}, j \geq 1$ would be decrypted wrongly. Since there is an error in C_i, from the decryption diagram we can see that C_i will be decrypted wrongly, i.e., P_i is wrongly. However, P_i and C_i are both involved in the decryption of the next ciphertext block C_{i+1}. This means C_{i+1} would be decrypted wrongly, i.e., P_{i+1} is wrong. P_{i+1} is used in the decryption of C_{i+2}, thus the error would propagate. As the result, all the ciphertext blocks from C_i on (including C_i) would be decrypted wrongly.

Question 2. Soultion:
The key length is 256-bit, so there are totally 2^{256} keys. Thus the years needed to try all the keys is

$$\begin{aligned}
\frac{10000\times 2^{256}\times 5.8\times 10^{-23}}{1.21\times 10^{34}\times 10^{23}} &\approx 47933.8843 \times \frac{2^{256}}{10^{34}\times 10^{23}} \\
&= 47933.8843 \times \frac{2^{256}}{10^{57}} \\
&\approx 47933.8843 \times \frac{2^{256}}{(2^{10})^{19}} \qquad (\text{ by } 10^3 \approx 2^{10}) \\
&= 47933.8843 \times 2^{66}
\end{aligned}$$

This number is much larger than the estimated age of the universe. So we don't expect brute-force search of 256-bit keys to be feasible any time soon.

Question 3. Solution:
3.1. The three-key Triple-DES is performed as : $C = E_{K_3}(E_{K_2}^{-1}(E_{K_1}(P)))$, where K_1, K_2, K_3 are idependent 56-bit keys.
Step 1. From one pair of plaintext-ciphertext pair (P, C). We try all the possible keys of K_3 to decrypt C. For every guessed value of $K_{3,z} = z$, we can get $A_z = E_z^{-1}(C)$. After trying all the possible keys of K_3, we can get a table T_1 consisting of all the 2^{56} pairs (z, A_z).
Step 2. We sort the two tables first to get T_1' (The cost of sorting n elements is $O(nlogn)$).
Step 3. We try all the possible values of (K_1, K_2). For each guessed pair $(K_{1,x}, K_{2,y}) = (x, y)$, compute $B_{x,y} = E_{K_{2,y}}^{-1}(E_{K_{1,x}}(P))$, and then compare. If there is a $B_{x,y}$ also in T_1', i.e., $A_z = B_{x,y} = E_{K_{2,y}}^{-1}(E_{K_{1,x}}(P))$, for some x, y and z, then probably $(K_{1,x}, K_{2,y}, K_{3,z}) = (x, y, z)$ is the three keys used in Triple-DES. There are $2^{112} \times 2^{56} \times 2^{-64} = 2^{104}$ possible values of (K_1, K_2, K_3) to be examined at the end of this step.
Step 4. For each of the 2^{104} possible keys we found in Step 3, we test the keys with another plaintext-ciphertext pairs (P', C') and determine the correct key.
Computation complexity: In Step 1, the computation complexity is 2^{56} DES decryptions. In Step 3, the average numbers of trials we need to find a correct key (K_1, K_2) is 2^{111}, so the complexity of Step 3 is about $2 \times 2^{111} = 2^{112}$ DES encryptions. In Step 4, we expect to perform 2^{103} DES encryptions. Thus, the total complexity is about $2^{56} + 2^{112} + 2^{103} \approx 2^{112}$ DES encrytions. (The sorting complexity is neligible)
3.2. ??????????????

Question 4. Solution:

From $C = (E_a(P \oplus K)) \oplus K$, we get

$$C \oplus K = E_a(P \oplus K)$$

Now we have 2^64 pairs of $(P_i, C_i), 0 \leq i \leq 2^{64} - 1$, and a is known.
Step 1. We guess all possible values of K, and we get 2^{128} possible keys.
Step 2. For each guessed key $K_i, 0 \leq i \leq 2^{128} - 1$, perform one decryption as

$$A_i = C_i \oplus K_i, B_i = E_a(P \oplus K)$$

If $A_i = B_i$, then K_i is the possible key.
Step 3. Do Step 2 for each of 2^{64} pairs of (P_i, C_i), and determine the correct key.
The computational complexity for Step 2 is $1 \times 2^{128} \times \frac{1}{2^{128}}$?????????

Question 5. Solution:
5.1. Over GF(2), if there are n binary variables, and the highest degree of monomials is m, then the maximum number of different monomials is

$$\sum_{i=1}^{m} \left(\begin{array}{c} n \\ i \end{array} \right)$$

because at most there are monomials of degree 1 to m, and for a particular degree d, there are at most $\left(\begin{array}{c} n \\ d \end{array} \right)$ monomials.
Since the number of equations should be the same as the number of variables to solve the system, we need $\sum_{i=1}^{m} \left(\begin{array}{c} n \\ d \end{array} \right)$ equations.
5.2. Let $y_1 = x_1, y_2 = x_2, y_3 = x_3, y_4 = x_1x_2, y_5 = x_2x_3$, then the system becomes

$$\begin{aligned} y_1 + y_2 + y_4 + y_5 &= 1 \\ y_1 + y_3 + y_4 &= 0 \\ y_1 + y_5 &= 6 \\ y_2 + y_3 + y_4 &= 1 \\ y_2 + y_3 &= 3 \end{aligned}$$

Solve this system and we get $x_1 = y_1 = 3, x_2 = y_2 = 4, x_3 = y_3 = 6$.

Question 6. (Optional)
Question 7. Solution:
7.1. Every time the 3 irregularly clocked LFSRs generate one bit. Every time, for any of the three LFSRs, the probability of getting clocked is

$$2 \times \left[\frac{1}{2} \times \left(\begin{array}{c} 2 \\ 1 \end{array} \right) \times \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} \right] = \frac{3}{4}$$

Thus to generate a 100-bit keystream, an LFSR would be clocked about $100 \times \frac{3}{4} = 75$ times on average.
7.2. It is impossible that two elements in the table S are identical. The reason is that $S[i]$ is initialized to different values and the remaining steps only perform the swapping among $S[i], 0 \leq i \leq 255$.
There are totally 256! possible ways to initialize S table.