MAS433 Cryptography: Tutorial 4
Block Cipher; Stream Cipher
23.09.2011

Instructions.

1. Submission of tutorial solution is compulsory.
2. Submission deadline: 22 September 2011, 6PM
3. Please submit your solution by sending email to wuhj@ntu.edu.sg (If your solution is handwritten, you can scan and convert it into digital format, such as .pdf document.)
4. Tutorial solution will not be provided after the tutorial class.

Question 1. Modes of operation of block cipher

1.1 Consider those five modes of operation: ECB, CBC, CFB, OFB, CTR. If there is error in a ciphertext block (it is not the last ciphertext block), how many plaintext blocks would be decrypted wrongly?

1.2 A mode of operation operates as follows: $C_0 = IV$, $C_i = E_K(P_i) \oplus C_{i-1}$ for $i \geq 1$. Is this mode of operation better than ECB mode?

1.3 A mode of operation operates as follows: $P_0 = IV_1$, $C_0 = IV_2$, $C_i = E_K(P_i \oplus C_{i-1}) \oplus P_{i-1}$ for $i \geq 1$. How to decrypt the ciphertext? If there is error in a ciphertext block (it is not the last ciphertext block), how many plaintext blocks would be decrypted wrongly?

Question 2. The energy radiated by the sun in 1 year is about 1.21×10^{34} Joules. According to our current understanding of physics, the minimum amount of energy needed to flip a bit is roughly 5.8×10^{-23} Joules (at 4.2 Kelvin, the temperature of liquid helium). Assume we harness all the energy output by the sun to attack AES-256 by brute force (at 4.2 Kelvin), and assume that the energy required to test an AES-256 key is about the same as that required to perform 10000 bit-flips. How many years would it take to try all possible keys of AES-256? Note that the current estimated age of the universe is 2^{33} years. Do you expect brute-force search of 256-bit keys to be feasible any time soon?

Question 3. Meet-in-the-middle attack on block cipher

3.1 Apply the meet-in-the-middle attack to three-key Triple-DES. How to reduce the complexity of the attack to about 2^{112} DES operations, and about 2^{56} memory (we consider each unit of memory as 128 bits here) ?

3.2 (Optional) For the two-key Triple-DES (the first key and the third key are the same), how to find the keys with about 2^{56} chosen plaintexts and less than 2^{60} DES operations? (Chosen plaintext attack: an attacker can obtain the ciphertexts of some chosen plaintexts.) (Hint: This meet-in-the-middle attack starts from a position within the Triple-DES and meets at another position in the Triple-DES.)

Question 4. (Bonus Question) A user uses AES in the following way to encrypt message: $C = (E_a(P \oplus K)) \oplus K$, where K is a 128-bit secret key, a is a known constant, $E_a()$ indicates the encryption of AES using the constant a as key. Develop an efficient attack to recover K with computational complexity about 2^{64}. Suppose that an attacker can obtain about 2^{64} plaintext-ciphertext pairs.

Question 5. Solve over-defined algebraic equations

5.1 In a system of algebraic equations over GF(2), if there are n binary variables, and the highest degree of monomials is m, then what is the maximal number of different monomials in this system of equations? How many such equations are needed to solve this system of equations through linearization? (Hint: for a monomial over GF(2), $x^2y^3z^8 = xyz$, i.e., the degree is 3)

5.2 There are several nonlinear equations over GF(7),

$$\begin{aligned}
x_1 + x_2 + x_1x_2 + x_2x_3 &= 1 \\
x_1 + x_3 + x_1x_2 &= 0 \\
x_1 + x_2x_3 &= 6 \\
x_2 + x_3 + x_1x_2 &= 1 \\
x_2 + x_3 &= 3
\end{aligned}$$

Solve the above over-defined equations.

Question 6. (Optional) Differential Cryptanalysis
Describe how to attack a 5-round DES using differential cryptanalysis. (Hint: You can use the differential path given in Slide 18 of Lecture 8.)

Question 7. Stream cipher

7.1 The A5/1 stream cipher consists of 3 irregularly clocked LFSRs. To generate a 100-bit keystream, how many times would an LFSR be clocked on average?

7.2 For the RC4 stream cipher, will two elements in the table S become identical? Why? How many possible values are there in the RC4 table?