MAS433 Cryptography: Tutorial 3
DES and AES
16.09.2011

Instructions.

1. Submission of tutorial solution is compulsory.
2. Submission deadline: 15 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. Feistel network

1.1 Draw the diagram of the Feistel network (you need to include the round function at the beginning, one round function in the middle, and the last round function).

1.2 Explain why the Feisel network is always invertible (i.e., you need to show that the round function in a Feistel network is always invertible)?

1.3 In the Feistel network, the outputs from the last round are swapped twice (no swapping). Suppose now that the output of the last round of the modified Feistel network is swapped only once, what extra operations are needed for decryption if we re-use the encryption algorithm in the decryption process?

Question 2. DES key schedule

Let $\bar{A}$ indicate the bitwise complement of A, i.e., each bit of $\bar{A}$ is the reverse of the relative bit of A. Let the encryption of DES be denoted as $C = E_K(P)$.

2.1 Let $K_1, K_2, \cdots, K_{16}$ denote the rounds keys of DES when the key K is used. Let $K'_1, K'_2, \cdots, K'_{16}$ denote the rounds keys of key $\overline{K}$. What is the relation between K_i and K'_i?

2.2 Show that $E_K(P) = \overline{E_{\overline{K}}(\overline{P})}$.

2.3 (Bonus Question) How to speed up the brute force attack on AES by using the property given in Question 2.2 ? (Hint: For an unknown key, an attacker has the ciphertexts of two plaintexts P and $\overline{P}$.)

2.4 How to improve DES against the attack given in Problem 3.3?

Question 3. A Weak DES Variant
In an DES-variant, an extra 16-bit key $K_b = b_{15}b_{14}b_{13}b_{12}\cdots b_2b_1b_0$ is used. During the computation of DES, each b_i is used to affect the swapping of L_{i+1} and R_{i+1} at the end of the $(i+1)$-th round: if $b_i = 1$, then L_{i+1} and R_{i+1} are swapped one more time; otherwise, no extra swapping is introduced. What is the security problem with this DES variant? (Hint: some values of K_b are extremely risky.)

Question 4. AES

4.1 In AES, for each plaintext byte to affect all the 16 bytes in the state, how many rounds are needed? Briefly explain why.

4.2 In the AES implementation, if the SubByte operations are not implemented, how to attack it?

4.3 In the AES implementation, if the ShiftRows operations are not implemented, how to attack it?

4.4 In the AES implementation, if the MixColumns operations are not implemented, how to attack it?

Question 5. $\mathbf{GF}(2^8)$
The finite field $\mathbf{GF}(2^8)$ in AES is defined by the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.

5.1 Compute $\{09\} \bullet \{82\}$ over $\mathbf{GF}(2^8)$, where $\{09\}$ and $\{82\}$ are in hexadecimal format.

5.2 Compute $\{09\}^{-1}$ over $\mathbf{GF}(2^8)$.

5.3 $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$, $b(x) = \{A3\}x$ and $x^4 + 1$ are polynomials with coefficients over $\mathbf{GF}(2^8)$. Compute $a(x) \otimes b(x) = a(x) \bullet b(x) \bmod x^4 + 1$.

5.4 For the $a(x)$ given in Question 5.3, verify that $a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$ modulo $x^4 + 1$.