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

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:

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

2.1. Compute the probabilities $\mathbf{Pr}[C = \phi_i]$ for $i = 1, 2, 3, 4$.
2.2. Compute the entropy of $\mathbf{P}$, $\mathbf{K}$ and $\mathbf{C}$.
2.3. Compute the conditional probabilities $\mathbf{Pr}[\beta_i|\phi_j]$ for $i = 1, 2$, $1 \le j \le 4$.
2.4. Compute the entropy of $\mathbf{P}$ if the ciphertext is given as ϕ_i $(1 \le i \le 4)$. Are these results different from the entropy of $\mathbf{P}$? Why?

Problem 3. Information Theory, Unicity Distance
A substitution cipher over a plaintext space of size n has $|\mathbf{K}| = n!$ (i.e., the key space size is $n!$). Stirling's formula gives the following estimate for $n!$:

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

3.1. Using Stirling's formula, derive an estimate of the unicity distance of the substitution cipher.
3.2. Let $m \ge 1$ be an integer. The m-gram substitution cipher is the substitution cipher where the plaintext (and ciphertext) spaces consist of all 26^m m-grams. Estimate the unicity distance of the m-gram substitution cipher if $R_L = 0.75$.

Problem 4. Feistel network

4.1. 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).

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

4.3. In the Feistel network, the outputs from the last round are swapped twice (non-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 ?

Problem 5. 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 $C = E_K(P)$.

5.1. 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?

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

5.3. How to speed up the brute force attack on AES by using the property given in Problem 5.2 ? (Hint: For an unknown key, an attacker has the ciphertexts of two plaintexts P and $\overline{P}$.)

5.4. How to improve DES against the attack given in Problem 5.3?

Problem 6. AES

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

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

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

Problem 7. $\mathbf{GF}(2^8)$

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

7.1. Compute $\{83\}^{-1}$ over $\mathbf{GF}(2^8)$ ($\{83\}$ is in hexidecimal format).

7.2. $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$, $b(x) = \{A5\}x$ and $x^4 + 1$ are polynomials with coefficients over $\mathbf{GF}(2^8)$. Compute $a(x) \otimes b(x) = a(x) \bullet b(x) \bmod x^4 + 1$.