Homework Assignment 4

Due: Monday, October 2, 2017

This assignment has two parts. The goal of the first part is to test your understanding of the concepts of information leakage and perfect security. The goal of the second part is to familiarize yourself with modes of operations for block ciphers.

Problem 1: Twister

Twister is a block cipher on 3-letter blocks. It uses both substitution and transposition. The message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ are triples of letters, encoded by numbers in the range $[0..25]$ as with the Caesar cipher. The key space $\mathcal{K} = \{0, \ldots, 77\}$.

Twister encryption is the composition of two ciphers E_k^1 and E_k^2, so $E_k = E_k^2 \circ E_k^1$. The first cipher,

$$E_k^1(m_1, m_2, m_3) = ((m_1 + k) \bmod 26, (m_2 + k) \bmod 26, (m_3 + k) \bmod 26),$$

is the shift substitution used by the Caesar cipher, applied separately to each letter of the message block (m_1, m_2, m_3). The second cipher,

$$E_k^2(m_1, m_2, m_3) = (m'_1, m'_2, m'_3),$$

is a transposition cipher, where the letter in position j is moved to position $t_k(j)$, where $t_k(j) = ((j + k - 1) \bmod 3) + 1$. Thus, $m'_{t_k(j)} = m_j$,

Questions:

1. How does one decrypt Twister?
2. Is Twister information-theoretically secure? Why or why not?
3. How much does increasing the key space to $\{0, \ldots, 155\}$ increase the difficulty of breaking Twister?
4. What is the effect on security of increasing the key space to $\{0, \ldots, 78\}$?

Please answer questions 3 and 4 with respect to both information leakage and to the difficulty of carrying out a brute-force attack. As usual, we assume keys are chosen uniformly at random from the key space.

Problem 2: Modes of operations

CBC (block chaining) and CTR (counter mode) are the two most commonly used modes of operations for block ciphers. Both modes are explained in detail in Chapter 5 of "Understanding Cryptography" by Paar and Pelzl.

Questions:

1. Draw diagrams to illustrate encryption and decryption in CBC and CTR modes using the following notation:
   - c_i - ciphertext block i,
   - p_i - plaintext block i,
   - k - key,
   - E - encryption function,
   - D - decryption function,
   - IV - initialization vector.
2. List and explain one advantage and one disadvantage of each mode of operation.
3. Suppose that one block of ciphertext was corrupted during transmission. For each mode of operation, explain the effect on the decrypted message.
4. Suppose that the encryption formula for CTR mode is replaced with $c_i = m_i \oplus E_k(IV)$. Does this change have any security implications? Explain your answer and clearly state your assumptions.