Homework Assignment 5

Due on Tuesday, October 6, 2020

1 Goal

The goal of this assignment is to test your understanding of the concepts of block cipher, information leakage, and perfect security.

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 $\mathcal{K} = \{0, \ldots, 77\}$. Note that $|\mathcal{K}| = 78 = 26 \times 3$.

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

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

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,

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

is a transposition cipher. The letter m_j 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 on single blocks? Why or why not?
3. How much does increasing the key space to $\{0, \ldots, 155\}$ increase the difficulty of breaking Twister? Explain.
4. What is the effect on security of increasing the key space to $\{0, \ldots, 78\}$? Explain.

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.