

Assignment #1

Due: Tuesday, September 14, 2004.

Problem 1 (20 pts) This problem asks you to formally define the Spartan Scytale Cipher.

Let $\Sigma = \{A, B, C, \dots, Z\}$; let $\ell < h < n$ be three positive integers. The plaintext space and the ciphertext space are $\bigcup_{i=1}^n \Sigma^i$, i.e., the set of all strings over Σ that have length between 1 and n . The keyspace is $[\ell..h]$. A key value k denotes the perimeter of the scytale in terms on how many rows can be written on the scytale.

Give the pseudo-code for the encryption procedure “encrypt($P[], C[], m, k$)”, where $m \leq n$ is the length of the plaintext, $k \in [\ell..h]$ is the value of the key, and both $P[]$ and $C[]$ are arrays of length m . $P[]$ initially stores the plaintext, and $C[]$ initially stores m spaces. When the procedure ends, $C[]$ stores the ciphertext, such that when they are printed on a belt and the belt is wrapped around a scytale of perimeter k , one can read the plaintext from left to right row by row.

Problem 2 (15 pts) Exercise 1.29 (a) on Page 43 of the textbook.

Hint: You may need to read Section 1.2.3 on how to use the concept of index of coincidence to find the key length used in the Vigenere Cipher as well as what is the key.

Problem 3 Recall that in class we proved that for any cipher that has perfect secrecy, the size of the key space is at least as large as the size of the plaintext space.

- a. (10 pts) Prove that for any cipher that has perfect secrecy, the size of the key space is at least as large as the size of the ciphertext space.
- a. (5 pts) Prove that for any cipher, the size of the ciphertext space is at least as large as the size of the plaintext space.

Problem 4 (15 pts) Consider a crypto system in which the plaintext space $\mathcal{M} = \{a, b, c\}$, the key space $\mathcal{K} = \{K_1, K_2, K_3\}$ and the ciphertext space $\mathcal{C} = \{1, 2, 3, 4\}$. Suppose that the encryption matrix is as follows:

| | | | |
|-------|-----|-----|-----|
| | a | b | c |
| K_1 | 1 | 2 | 3 |
| K_2 | 2 | 3 | 4 |
| K_3 | 3 | 4 | 1 |

Assume that the keys are chosen uniformly randomly; in other words, $\Pr[\text{Key} = K_1] = \Pr[\text{Key} = K_2] = \Pr[\text{Key} = K_3] = 1/3$. Further assume that the plaintext PT is drawn from the following probability distribution: $\{a \mapsto 1/2, b \mapsto 1/3, c \mapsto 1/6\}$; in other words,

$$\Pr[\text{PT} = a] = 1/2, \quad \Pr[\text{PT} = b] = 1/3, \quad \Pr[\text{PT} = c] = 1/6.$$

Show that this crypto system *does not* have perfect secrecy.

Problem 5 Let p be a 128-bit prime and let \mathbb{Z}_p be the set of integers $\{0, \dots, p-1\}$. Consider the following encryption scheme. The secret key is a pair of integers $a, b \in \mathbb{Z}_p$ where $a \neq 0$. An encryption of a message $M \in \mathbb{Z}_p$ is defined as:

$$E_{a,b}[M] = aM + b \pmod{p}$$

- a. (20 pts) Show that when E is used to encrypt a message $M \in \mathbb{Z}_p$ the system has perfect secrecy in the sense of Shannon.
- b. (15 pts) Show that if the system is used to encrypt a plaintext (M_1, M_2) , where $M_1, M_2 \in \mathbb{Z}_p$, then the system does not have perfect secrecy.
Hint: consider the case $M_1 = M_2$.

Note: Perfect Secrecy of The One-Time Pad encryption, Binary Edition The Cipher is defined as follows:

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^n$, where \mathcal{M} is the plaintext (message) space, \mathcal{C} is the ciphertext space, \mathcal{K} is the key space. The key K is drawn uniformly random from \mathcal{K} , in other words, each key in \mathcal{K} is drawn with equal probability.
- $\mathbb{E}_K[M] = \mathbb{E}[K, M] = K \oplus M$.
- $\mathbb{D}_K[C] = \mathbb{D}[K, C] = K \oplus C$.

One-Time Pad has Perfect Secrecy

Proof. Given any probability distribution from which the plaintext is drawn. For any plaintext-ciphertext pair (M_0, C_0) , we need to show that $\Pr[\text{PT} = M_0 \mid \text{CT} = C_0] = \Pr[\text{PT} = M_0]$.

$$\Pr[\text{PT} = M_0 \mid \text{CT} = C_0] = \frac{\Pr[\text{PT} = M_0, \text{CT} = C_0]}{\Pr[\text{CT} = C_0]} = \frac{\Pr[\text{PT} = M_0] \Pr[\text{CT} = C_0 \mid \text{PT} = M_0]}{\sum_{M \in \mathcal{M}} (\Pr[\text{PT} = M] \Pr[\text{CT} = C_0 \mid \text{PT} = M])}$$

Since that the encryption key is drawn uniformly random from the key space, and there is only one key that encrypts a given plaintext into a given cipher text (the key is given by the XOR of the plaintext and the ciphertext),

$$\Pr[\text{CT} = C_0 \mid \text{PT} = M_0] = \frac{\# \text{ of keys in } \mathcal{K} \text{ that encrypts } M_0 \text{ into } C_0}{\# \text{ of total keys in } \mathcal{K}} = \frac{1}{2^n}$$

Similarly, for every $M \in \mathcal{M}$, $\Pr[\text{CT} = C_0 \mid \text{PT} = M] = \frac{1}{2^n}$.

Therefore, continuing the first equation, we have

$$\Pr[\text{PT} = M_0 \mid \text{CT} = C_0] = \frac{\Pr[\text{PT} = M_0] \frac{1}{2^n}}{\sum_{M \in \mathcal{M}} (\Pr[\text{PT} = M] \frac{1}{2^n})} = \frac{\Pr[\text{PT} = M_0]}{\sum_{M \in \mathcal{M}} (\Pr[\text{PT} = M])} = \frac{\Pr[\text{PT} = M_0]}{1}$$

■