Foundations of Cryptography (CS60088)

Spring 2026

Tutorial 1: Perfect Secrecy

1. The shift (caesar) cipher works as follows. Identify the English alphabet $\{A, B, \ldots, Z\}$ with the set $\{0, 1, \ldots, 25\}$ in the natural order. Define the key space, message space, and ciphertext space as

$$\mathcal{K} = \{0, 1, \ldots, 25\}, \qquad \mathcal{M} = \mathcal{C} = \{0, 1, \ldots, 25\}^*.$$

The encryption scheme is defined by the following algorithms:

- $\mathsf{Gen}()$: choose a key $k \xleftarrow{U} \mathcal{K}$ uniformly at random.
- $\mathsf{Enc}(k, m = m_1 m_2 \cdots m_n)$: for each i, compute

$$c_i \leftarrow (m_i + k) \bmod 26.$$

  Output the ciphertext $c = c_1 c_2 \cdots c_n$.
- $\mathsf{Dec}(k, c = c_1 c_2 \cdots c_n)$: for each i, recover

$$m_i \leftarrow (c_i - k) \bmod 26.$$

(a) Is this encryption scheme perfectly secret?

(b) Can you modify the description of the scheme to make it perfectly secret?

2. Let ℓ be an even positive integer. Define

$$\mathcal{M} = \mathcal{C} = \{0, 1\}^\ell.$$

The key-generation algorithm works as follows: first choose

$$\tilde{k} \xleftarrow{U} \{0, 1\}^{\ell/2},$$

and then define the key

$$k = \tilde{k} \,\|\, \tilde{k},$$

where $\|$ denotes concatenation. Encryption and decryption are defined as

$$\mathsf{Enc}_k(m) = k \oplus m, \qquad \mathsf{Dec}_k(c) = k \oplus c.$$

Is this encryption scheme perfectly secret? Justify your answer.

3. Prove or refute the following statement:

An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$ and for every $c_0, c_1 \in \mathcal{C}$,

$$\Pr[C = c_0] = \Pr[C = c_1].$$

4. Consider the one-time pad over $\{0,1\}^\ell$, where encryption is defined as $\mathsf{Enc}_k(m) = k \oplus m$. Observe that when $k = 0^\ell$, encryption reveals the message in the clear. It is therefore suggested to modify the scheme by defining Gen to choose the key uniformly from the set

$$\mathcal{K} = \{0,1\}^\ell \setminus \{0^\ell\},$$

i.e.,

$$k \xleftarrow{U} \mathcal{K}.$$

Is the resulting encryption scheme perfectly secret? Explain your answer.

5. For each of the following encryption schemes, state whether the scheme is perfectly secret. Justify your answer in each case.

   (a) The message space is $\mathcal{M} = \{0,1,2,3,4\}$ and the key space is $\mathcal{K} = \{0,1,2,3,4,5\}$. The algorithms are defined as:

   $$\mathsf{Gen}() : k \xleftarrow{U} \mathcal{K}, \qquad \mathsf{Enc}_k(m) = (k+m) \bmod 5, \qquad \mathsf{Dec}_k(c) = (c-k) \bmod 5.$$

   (b) The message space is

   $$\mathcal{M} = \{m \in \{0,1\}^\ell \mid \text{the last bit of } m \text{ is } 0\}.$$

   The key space is $\mathcal{K} = \{0,1\}^{\ell-1}$. The encryption and decryption algorithms are defined as:

   $$\mathsf{Gen}() : k \xleftarrow{U} \mathcal{K}, \qquad \mathsf{Enc}_k(m) = m \oplus (k \,\|\, 0), \qquad \mathsf{Dec}_k(c) = c \oplus (k \,\|\, 0).$$