Lecture 03: One-time Pad for Bit-strings

- We will see an encryption algorithm called "One-time Pad" for bit-strings
- In the future, we shall extend its domain to general abstract objects (for example, *groups*)

One-time Pad I

Yesterday.

- **Secret-key Generation**: Alice and Bob met and sampled a secret-key sk uniformly at random from the set $\{0,1\}^n$, mathematically represented by $\mathsf{sk} \sim \{0,1\}^n$

Today.

- **Goal**: Alice wants to send a message $m \in \{0,1\}^n$ to Bob over a public channel so that any eavesdropper cannot figure out the message m.
- **Encryption**: To achieve this goal, Alice computes a ciphertext c that encrypts the message m using the secret-key sk, mathematically represented by $c = \mathsf{Enc}_{\mathsf{sk}}(m) := m \oplus \mathsf{sk}$. Here $\oplus$ represents the bit-wise XOR of the bits of m and sk.
- **Communication**: Alice sends the cipher-text c to Bob over a public channel
- **Decryption**: Now, Bob wants to decrypt the cipher-text c to recover the message m. Mathematically, this step is represented by $m' = \mathsf{Dec}_{\mathsf{sk}}(c) := c \oplus \mathsf{sk}$

One-time Pad II

- **Correctness**: Note that we will always have $m = m'$, i.e., Bob always correctly recovers the message
  - Note that in our case we always have $m = m'$
  - There are encryption schemes where with a small probability $m \neq m'$ is possible, i.e., the encryption scheme is incorrect with a small probability
- **Security**: Later in the course we shall see how to mathematically prove the following statement.

  "An adversary who gets the ciphertext c obtains no *additional information* about the message m sent by Alice."

One-time Pad III

Alice	Bob

$$sk \sim \{0,1\}^n$$

$$c = \mathsf{Enc}_{\mathsf{sk}}(m) := m \oplus \mathsf{sk}$$

$$\xrightarrow{\quad c \quad}$$

$$m' = \mathsf{Dec}_{\mathsf{sk}}(c) := c \oplus \mathsf{sk}$$

Figure: Pictorial Summary of the One-time Pad Encryption Scheme.

Dropping one Restriction makes the task Trivial

- Suppose we insist only on correctness and not on security
  - The trivial scheme where $\mathsf{Enc}_{\mathsf{sk}}(m) = m$, i.e., the encryption of any message m using any secret key sk is the message itself, satisfies correctness. However, this scheme is completely insecure!
- Suppose we insist only on security and not on correctness
  - The trivial scheme where $\mathsf{Enc}_{\mathsf{sk}}(m) = 0$, i.e., the encryption of any message m using any secret key sk is 0, satisfies the security constraint. However, Bob cannot correctly recover the origianl message m with certainty!
- So, the non-triviality is to simultaneously achieve correctness and security

Important

- We are <u>not</u> trying to hide the fact that Alice sent a message to Bob
- We are trying to hide <u>only the message</u> that is being sent by Alice to Bob

Closing Remarks: Crucial Observation

- Fix a cipher-text c
- Consider any message m
- There exists a unique secret-key $\mathsf{sk}_{m,c}$ such that $\mathsf{Enc}_{\mathsf{sk}_{m,\mathsf{sk}}}(m) = c$
- This observation shall be crucial to prove the security of the one-time pad private-key encryption scheme