Lecture 05: Private-key Encryption
(Definition & Security of One-time Pad)
Three algorithms

- Key Generation: Generate the secret key $sk$
- Encryption: Given the secret key $sk$ and a message $m$, it outputs the cipher-text $c$ (Note that the encryption algorithm can be a randomized algorithm)
- Decryption: Given the secret key $sk$ and the cipher-text $c$, it outputs a message $m'$ (Note that the decryption algorithm can be a randomized algorithm)
Yesterday Alice and Bob met and generated a secret key 
\( sk \sim \text{Gen()} \)
- Read as: the secret key \( sk \) is sampled according to the 
distribution \( \text{Gen()} \)

Today Alice wants to encrypt a message \( m \) using the secret 
key \( sk \). Alice encrypts \( c \sim \text{Enc}_{sk}(m) \)
- Read as: the cipher-text \( c \) is sampled according to the 
distribution \( \text{Enc}_{sk}(m) \)

Then Alice sends the cipher-text \( c \) to Bob. An eavesdropper 
gets to see the cipher-text \( c \)

After receiving the cipher-text \( c \) Bob decrypts it using the 
secret key \( sk \). Bob decrypts \( m' \sim \text{Dec}_{sk}(c) \)
- Read as: the decoded message \( m' \) is sampled according to the 
distribution \( \text{Dec}_{sk}(c) \)
Correctness

- We want the decoded message obtained by Bob to be identical to the original message of Alice with high probability.
- We insist

\[ P[M = M'] = 1 \]

- Recall we use capital alphabets to represent the random variable corresponding to the variable (so, \( M \) is the random variable for the message encoded by Alice and \( M' \) is the random variable for the message recovered by Bob).
- We want to say that the cipher-text $c$ provides the adversary no additional information about the message.
- We insist that, for all message $m$, we have

$$P[M = m | C = c] = P[M = m]$$
Suppose we insist only on correctness and not on security

- The trivial scheme where $\text{Enc}_{sk}(m) = m$, i.e. the encryption of any message $m$ using any secret key $sk$ is the message itself, satisfies correctness. But is completely insecure!

Suppose we insist only on security and not on correctness

- The trivial scheme where $\text{Enc}_{sk}(m) = 0$, i.e. the encryption of any message $m$ using any secret key $sk$ is 0, satisfies this security. But Bob cannot correctly recover the original message $m$ with certainty!

So, the non-triviality is to simultaneously achieve correctness and security
One-time Pad

- Let \((G, \circ)\) be a group

- Secret-key Generation:
  
  \[
  \text{Gen()} : \\
  \quad \text{Return } sk \leftarrow G
  \]

- Encryption:
  
  \[
  \text{Enc}_{sk}(m) :
  \quad \text{Return } c := m \circ sk
  \]

- Decryption:
  
  \[
  \text{Dec}_{sk}(c) :
  \quad \text{Return } m' := c \circ \text{inv}(sk)
  \]

- Note that Encryption and Decryption is deterministic

- The only randomized step is the choice of \(sk\) during the secret-key generation algorithm
Correctness of One-time Pad

- It is trivial to see that

\[ P [M = M'] = 1 \]

- So, one-time pad is correct!
We want to simplify the probability\[ P[M = m | C = c] \]

Using Bayes’ Rule, we have\[ = \frac{P[M = m, C = c]}{P[C = c]} \]

Using the fact that \[ P[C = c] = \sum_{x \in G} P[M = x, C = c] \], we get\[ = \frac{P[M = m, C = c]}{\sum_{x \in G} P[M = x, C = c]} \]
We will prove the following claim later

**Claim**

For any $x, y \in G$, we have

$$P[M = x, C = y] = P[M = x] \cdot \frac{1}{|G|}$$

Using this claim, we can simplify the expression as

$$P[M = m] \cdot \frac{1}{|G|} = \frac{P[M = m]}{\sum_{x \in G} P[M = x] \cdot \frac{1}{|G|}}$$

$$= \frac{P[M = m]}{\sum_{x \in G} P[M = x]}$$
Using the fact that \( \sum_{x \in G} \Pr[M = x] = 1 \), we get that the previous expression is

\[
= \Pr[M = m]
\]

This proves that \( \Pr[M = m | C = c] = \Pr[M = m] \), for all \( m \) and \( c \). This proves that the one-time pad encryption scheme is secure!
Proof of Claim 1

- You will prove the following statement in the homework: If there exists $sk$ such that $x \circ sk = y$ then $sk$ is unique (i.e., there does not exist $sk' \neq sk$ such that $x \circ sk' = y$)
- Using this result, we get the following. Suppose $z \in G$ be the unique element such that $x \circ z = y$. Then we have:

$$P[M = x, C = y] = P[M = x, SK = z]$$

- Note that the secret-key is sample independent of the message $x$. So, we have

$$P[M = x, SK = z] = P[M = x] \cdot P[SK = z]$$

- Note that $sk$ is sampled uniformly at random from the set $G$. So, we have

$$P[M = x, SK = z] = P[M = x] \cdot \frac{1}{|G|}$$
Example I

- Encrypting bit messages
  - Consider \((G, \circ) = (\mathbb{Z}_2, + \ mod \ 2)\)
Encrypting $n$-bit strings

- Consider $G = \{0, 1\}^n$
- Define $(x_1, \ldots, x_n) \circ (y_1, \ldots, y_n) = (x_1 + y_1 \mod 2, \ldots, x_n + y_n \mod 2)$
Example III

- Encrypting an alphabet
  - Consider $G = \mathbb{Z}_{26}$
  - Define $\circ$ as $+ \mod 26$

- You will construct one more scheme in the homework by interpreting the set of alphabets as $\mathbb{Z}_{27}^{*}$
Example IV

- Encrypting $n$-alphabet words
  - Consider $G = \mathbb{Z}_{26}^n$
  - Define $\circ$ as the coordinate-wise $+ \mod 26$