CS181A Notes #0

One-time pad Alice wants to send a one-bit message $b \in \{0, 1\}$ to Bob. They share a communication channel which is insecure due to the presence of an eavesdropper Eve. The goal is have Bob receive the bit b but without Eve having any knowledge of it.

Secret key Suppose that Alice and Bob *share* between them a secret uniform random bit $r \in \{0, 1\}$. Eve has no knowledge of this random bit.

Encryption Alice encrypts her plaintext bit b into a ciphertext bit

$$\hat{b} = b \oplus r \tag{1}$$

Alice then sends $\hat{b}$ to Bob over the insecure channel.

Decryption Bob decrypts by computing the ciphertext bit as follows:

$$b = \hat{b} \oplus r. \tag{2}$$

This holds since XOR (exclusive OR) is associative.

Security Eve cannot determine b from $\hat{b}$ since the latter is a uniform random bit. The one-time pad protocol is *unconditionally secure* (or information-theoretically secure).

Two-bit message Suppose Alice wants to send a two-bit message $b_1 b_2 \in \{0, 1\}^2$ but with only a one-bit random key $r \in \{0, 1\}$. Here, she sends $\hat{b}_1 = b_1 \oplus r$ and $\hat{b}_2 = b_2 \oplus r$ to Bob over the insecure channel. Then, Eve can find out if b_1 are b_2 are the same or not.