Vernam Cipher

Liljana Babinkostova
Department of Mathematics, Boise State University
A readable message is called plaintext (or cleartext). The process of transforming a message in such a way as to hide its content is called encryption.

An encrypted message is called a ciphertext. The process of transforming ciphertext back into plaintext is called decryption.

A cryptographic algorithm, called a cipher, is the mathematical function $e_k$ used for encryption and the mathematical function used for decryption $d_k$.

Encryption and decryption are controlled by cryptographic keys.

The set of all plain texts is denoted by $\mathcal{P}$, the set of all cipher texts with $\mathcal{C}$ and the set of all possible keys is denoted by $\mathcal{K}$.
Computational Security: A cryptosystem is \textit{computationally secure} if the best algorithm for breaking it requires at least \(N\) operations, where \(N\) is some fixed large number.
Security of a cryptosystem

- **Computational Security**: A cryptosystem is *computationally secure* if the best algorithm for breaking it requires at least $N$ operations, where $N$ is some fixed large number.

- **Unconditional Security**: A cryptosystem is *unconditionally secure* if it cannot be broken, even with infinite computational resources.
Perfect Secrecy

Let the set of all plaintexts $\mathcal{P}$, the set of all ciphertexts $\mathcal{C}$ and the set of all keys $\mathcal{K}$ are sets of equal size. We write $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

\[1\] C. Shannon, *Communication Theory of Secrecy Systems*, (1949)
Perfect Secrecy

Let the set of all plaintexts $\mathcal{P}$, the set of all ciphertexts $\mathcal{C}$ and the set of all keys $\mathcal{K}$ are sets of equal size. We write $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

**Theorem (Shannon, 1949)**

A cryptosystem is perfectly secure if and only if every key is used with equal probability $1/|\mathcal{K}|$, and for every plaintext $x$ and every ciphertext $y$, there is a unique key $k$ such that $e_k(x) = y$.

---

Vernam cipher (One-Time-Pad)

Vernam cipher is a substitution cipher with $P = C = K$ and their elements are strings of a fixed number of bits.

- The message $m$ is a string of $n$ binary bits,

\[ m = b_1 b_2 b_3 ... b_n, \quad b_i \in \{0, 1\} \]
Vernam cipher (One-Time-Pad)

Vernam cipher is a substitution cipher with $\mathcal{P} = \mathcal{C} = \mathcal{K}$ and their elements are strings of a fixed number of bits.

- The message $m$ is a string of $n$ binary bits,
  $$m = b_1 b_2 b_3 \ldots b_n, \ b_i \in \{0, 1\}$$

- The key is random or pseudorandom string of $n$ binary bits
  $$k = k_1 k_2 k_3 \ldots k_n, \ k_i \in \{0, 1\}$$
Vernam cipher (One-Time-Pad)

Vernam cipher is a substitution cipher with $\mathcal{P} = \mathcal{C} = \mathcal{K}$ and their elements are strings of a fixed number of bits.

- The message $m$ is a string of $n$ binary bits,
  \[ m = b_1 b_2 b_3 ... b_n, \quad b_i \in \{0, 1\} \]

- The key is random or pseudorandom string of $n$ binary bits
  \[ k = k_1 k_2 k_3 ... k_n, \quad k_i \in \{0, 1\} \]

- Uses the XOR operation (addition modulo 2)

Encryption: \[ c_i = b_i \oplus k_i \text{ for } 1 \leq i \leq n. \]
Decryption: \[ b_i = c_i \oplus k_i \text{ for } 1 \leq i \leq n. \]
Vernam cipher (One-Time-Pad)

Vernam cipher is a substitution cipher with $P = C = K$ and their elements are strings of a fixed number of bits.

- The message $m$ is a string of $n$ binary bits,
  \[ m = b_1 b_2 b_3 \ldots b_n, \quad b_i \in \{0, 1\} \]

- The key is random or pseudorandom string of $n$ binary bits
  \[ k = k_1 k_2 k_3 \ldots k_n, \quad k_i \in \{0, 1\} \]

- Uses the XOR operation (addition modulo 2)

  **Encryption:** $c_i = b_i \oplus k_i$ for $1 \leq i \leq n$.
  
  **Decryption:** $b_i = c_i \oplus k_i$ for $1 \leq i \leq n$.

  If the key is truly random and used only once, this is perfectly secure cryptosystem (one-time pad).