Introduction to Cryptology

Boise State University
Introduction

Cryptography

is the field concerned with techniques for securing information, particularly in communications. It focuses on the following paradigms:

- **Confidentiality** ensuring that no one can read the message except the intended receiver.
- **Authentication** the process of proving one's identity.
- **Integrity** assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation** a mechanism to prove that the sender really sent this message.
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 used for encryption and the mathematical function used for decryption.

Encryption and decryption are controlled by cryptographic keys.
Definition
A cryptosystem is a five-tuple \((\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})\) where the following conditions are satisfied:

1. \(\mathcal{P}\) is a finite set of possible plaintexts.
2. \(\mathcal{C}\) is a finite set of possible ciphertexts.
3. \(\mathcal{K}\), the keyspace, is a finite set of possible keys.
4. \(\mathcal{E}\) and \(\mathcal{D}\) are two sets of functions.
5. For each \(K \in \mathcal{K}\), there is an encryption function \(e_K \in \mathcal{E}\) and a corresponding decryption function \(d_K \in \mathcal{D}\). Each \(e_K : \mathcal{P} \rightarrow \mathcal{C}\) and \(d_K : \mathcal{C} \rightarrow \mathcal{P}\) are functions such that \(d_K(e_K(x)) = x\) for every plaintext \(x \in \mathcal{P}\).
Symmetric or private-key cryptosystems are characterized by the fact that the key is shared between the sender and the receiver and is kept secret.
Affine cipher is a substitution cipher with $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$ and

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n : \gcd(a, n) = 1\}$$

For $k = (a, b) \in \mathcal{K}$, define encryption/decryption mapping as follows

$$\begin{cases}
e_k(x) = ax + b \mod n \\
d_k(y) = a^{-1}(y - b) \mod n
\end{cases}$$

with $x, y \in \mathbb{Z}_n$. 
Asymmetric or public-key cryptosystems are characterized by the fact that the sender and the receiver get a pair of keys, one called the public key and the other called the private key.
PKE Example: Diffie-Hellman Encryption

Key Exchange Protocol:

- Alice and Bob publicly agree on a large prime number $P$ as the encryption modulus.
- Alice and Bob publicly agree on a number $Q < P$ for which the least $x$ such that $Q^x = 1 \mod P$ is large. One may assume that $Q$ is a primitive root of $P$.
- Alice secretly chooses a number, $A$, not revealed to Bob or anyone, and then publicly reveals $A^*(= Q^A \mod P)$ to Bob.
PKE Example: Diffie-Hellman Encryption

Key Exchange Protocol:

- Bob secretly chooses a number, $B$, not revealed to Alice or anyone, and then publicly reveals the value $B \ast (Q^B \mod P)$ to Alice.
- Alice and Bob each separately computes the common secret key, DHS.
  - Alice’s computation: $DHS = (B^*)^A \mod P$.
  - Bob’s computation: $DHS = (A^*)^B \mod P$. 
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.
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

**Definition**
A cryptosystem has perfect secrecy if $P_{\mathcal{P}}(x|y) = P_{\mathcal{P}}(x)$ for all $x \in \mathcal{P}, y \in \mathcal{C}$.

---

Perfect Secrecy

Definition
A cryptosystem has perfect secrecy if $P_{\mathcal{P}}(x|y) = P_{\mathcal{P}}(x)$ for all $x \in \mathcal{P}$, $y \in \mathcal{C}$.

Theorem (Shannon, 1949)
Suppose $\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$ is a cryptosystem where $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$. Then the cryptosystem has a perfect secrecy iff every key is used with equal probability $1/|\mathcal{K}|$, and for every $x \in \mathcal{P}$ and every $y \in \mathcal{C}$, there is a unique key $k$ such that $e_k(x) = y$.

---

Vernam cipher

Vernam cipher \(^2\) is a substitution cipher with \(\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0, 1\}^n\).

- The message \(m\) is a string of \(n\) binary bits,
  \[ m = b_1b_2b_3...b_n, \quad b_i \in \{0, 1\} \]

---

\(^2\)G. Vernam, US Patent 1310719 (1917)
Vernam cipher

Vernam cipher \(^2\) is a substitution cipher with \(\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0, 1\}^n\).

- 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

\[
k = k_1 k_2 k_3 ... k_n, \quad k_i \in \{0, 1\}
\]

\(^2\)G. Vernam, US Patent 1310719 (1917)
Vernam cipher is a substitution cipher with $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0, 1\}^n$.

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

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

- 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 $1 \leq i \leq n$

---

$^2$G. Vernam, **US Patent 1310719** (1917)
Vernam cipher

Vernam cipher \(^2\) is a substitution cipher with 
\(\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0, 1\}^n\).

- 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: \(c_i = b_i \oplus k_i\) 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).

\(^2\)G. Vernam, US Patent 1310719 (1917)