Contents

Chapter 1

Introduction

Cryptography is the art and science of encrypting and decrypting a message.

1.1 Symmetric cipher

A symmetric cipher scheme Π can be viewed as a triplet $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ of algorithms. Suppose $\mathcal{M}$ be the set of all possible messages and $\mathcal{K}$ be the set of all keys. Gen chooses a key $k \in \mathcal{K}$ and then $\mathrm{Enc} : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ encrypts the message m with key k and returns the cipher c. Lastly, $\mathrm{Dec} : \mathcal{C} \times \mathcal{K} \to \mathcal{M} \cup \perp$ decrypts the cipher c with key k and returns either a message or an error, denoted as $\perp$. Without loss of generality we can assume that Gen picks k uniformly from $\mathcal{K}$. Futhermore, Enc can be randomized, however Dec is deterministic and for every message m and key k we must have

$$\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$$

1.2 Kerckhoff's principle

Kerckhoff's principle assumes the following for every encryption scheme

1. The encryption and decryption is known to everyone.
2. The security of the scheme is only dependent on the key.

1.3 Attacks

Some possible attacks include (in increasing power)

Cihpertext only Attacker only knows the ciphertexts.

Known-plaintext Attacker knows one or more plaintext/ciphertext generated by the key.

Chosen-plaintext Attacker can obtain encryption of plaintexts of his choice.

Chosen-ciphertext Attacker can obtain decryption of ciphertexts of his choise.

Chapter 2

Perfectly Secret Encryption

2.1 perfectly secure encryption

Let K and M be two random variables, where K is the result of Gen and M is the message. We can assume that they are independent. Furthermore, $C = \mathrm{Enc}_K(M)$ is also a random varible. By the Kerckhoff's principle, we assume that the distribution on M and Enc is known and only K is unknown.

Definition (Perfectly secure encrption): An encryption scheme is perfectly secure if for all $c \in \mathcal{C}$ with $\mathbb{P}(C = c) > 0$:

$$\forall m \in \mathcal{M}, \quad \mathbb{P}(M = m \mid C = c) = \mathbb{P}(M = m) \tag{2.1}$$

Proposition 2.1. *An encryption scheme* Π *is perfectly secure if and only if*

$$\forall m, m' \in \mathcal{M}, \quad \mathbb{P}(\mathrm{Enc}_K(m) = c) = \mathbb{P}(\mathrm{Enc}_K(m') = c) \tag{2.2}$$

Proof. Suppose Π is perfectly secure then (assuming that $\mathbb{P}(M = m) > 0$)

$$\begin{aligned}\mathbb{P}(\mathrm{Enc}_K(m) = c) = \mathbb{P}(C = c \mid M = m) &= \frac{\mathbb{P}(M = m \mid C = c)\mathbb{P}(C = c)}{\mathbb{P}(M = m)} \\ &= \frac{\mathbb{P}(M = m)\mathbb{P}(C = c)}{\mathbb{P}(M = m)} = \mathbb{P}(C = c)\end{aligned}$$

Now if the equation holds for Π then (again assuming that $\mathbb{P}(M = m) > 0$)

$$\begin{aligned}\mathbb{P}(M = m \mid C = c) &= \frac{\mathbb{P}(C = c \mid M = m)\mathbb{P}(M = m)}{\mathbb{P}(C = c)} \\ &= \frac{\mathrm{Enc}_K(m)\mathbb{P}(M = m)}{\sum_{m^*} \mathbb{P}(C = c \mid M = m^*)\mathbb{P}(M = m^*)} \\ &= \frac{\mathbb{P}(M = m)}{\sum_{m^*} \mathbb{P}(M = m^*)} = \mathbb{P}(M = m)\end{aligned}$$

2.2 Prefect adversarial indistinguishability

An encryption scheme is **perfectly indistinguishable** if no adversary $\mathcal{A}$ can succeed with probability better than $\frac{1}{2}$. Formally, we run the following experiment $\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}$

1. $\mathcal{A}$ outputs a pair $m, m_0 \in \mathcal{M}$.
2. $k = \mathrm{Gen}$ and b - chosen from $\{0,1\}$ uniformly - then the **challenge ciphertext** $c = \mathrm{Enc}_k(m_b)$ is given to $\mathcal{A}$.
3. $\mathcal{A}$ tries to determine the which message was encrypted and then outputs b'.
4. $$\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi} \begin{cases} 1 & b' = b \text{ then } \mathcal{A} \text{ succeeds} \\ 0 & b' \neq b \text{ then } \mathcal{A} \text{ fails} \end{cases}$$

Since $\mathcal{A}$ can guess randomly $\mathbb{P}\big(\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi} = 1\big) \geq \frac{1}{2}$ and thus a scheme is perfectly indistinguishable if

$$\mathbb{P}\big(\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi} = 1\big) = \frac{1}{2}, \quad \forall \mathcal{A}$$

Proposition 2.2. Π *is perfectly secret if and only if it is perfectly indistinguishable.*

Proof.

$$\mathbb{P}\big(\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi} = 1\big) = \mathbb{P}(M = m \mid C = c)$$

2.3 One-time pad

Let $l \in \mathbb{N}^*$ and $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^l$ then *one-time pad* scheme is describe as follows

- Gen is uniform.
- $\mathrm{Enc}_k(m) = k \oplus m$.
- $\mathrm{Dec}_k(c) = k \oplus c$.

Theorem 2.3. *One-time pad is perfectly secure.*

Proof.

$$\begin{aligned} \mathbb{P}(M = m \mid C = c) &= \frac{\mathbb{P}(C = c \mid M = m)\mathbb{P}(M = m)}{\sum_{m^*} \mathbb{P}(C = c \mid M = m^*)\mathbb{P}(M = m^*)} \\ &= \frac{\mathbb{P}(K = c \oplus m)}{\sum_{m^*} \mathbb{P}(K = c \oplus m^*)\mathbb{P}(M = m^*)}\mathbb{P}(M = m) \\ &= \mathbb{P}(M = m) \end{aligned}$$

Proposition 2.4. *If* Π *is perfectly secure then we must have* $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof. Suppose $|\mathcal{K}| < |\mathcal{M}|$ and let $c \in \mathcal{C}$ be a ciphertext and define $\mathcal{M}(c)$ to the

$$\mathcal{M}(c) = \{m \,|\, m = \mathrm{Dec}_k(c) \text{ for some } k \in \mathcal{K}\}$$

Then $|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}|$ and therefore there exists $m \in \mathcal{M}$ such that $m \notin \mathcal{M}(c)$ hence

$$\mathbb{P}(M = m \mid C = c) = 0 \neq \mathbb{P}(M = m)$$

Note that we assumed the distribution over $\mathcal{M}$ is uniform. ■

Theorem 2.5 (Shannon's Theorem). Π *with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ *is perfectly secure if and only if*

1. Gen *is uniform.*
2. $\forall m \in \mathcal{M}$ *and* $c \in \mathcal{C}$, $\exists! k \in \mathcal{K}$ *such that* $\mathrm{Enc}_k(m) = c$.

Proof.