Introduction to Cryptosystems

Lesson 1

Introduction

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
code	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Doc: khoa cong nghe thong tin

Plaintext: 11081501 03151407 14070805 2008151407 200914

VD1: k = 3

Ciphertext:

VD2: k = 4018975632

Ciphertext:

VD2: k = 0185947263

Ciphertext:

Definition

E_k: $\mathcal{M} \rightarrow$ C "Invertible"

$\exists E_{k'}^{-1} \equiv D_{k'}$: C$\rightarrow \mathcal{M}$ such that

$\forall m \in \mathcal{M}, k, k' \in K, c = E_k(m) \leftrightarrow m = D_{k'}(c)$.

Types of cryptosystem

- k $\neq$ k': Asymmetric cryptosystem/Public key cryptosystem.
- k $\equiv$ k': Symmetric cryptosystem/Secrete key cryptosystem.

- $|\mathcal{M}| \geq |$C$|$: cryptographic hash function.

Example

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
code	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Doc: khoa cong nghe thong tin

Plaintext: 11081501 03151407 14070805 2008151407 200914

VD1: k = 3

Ciphertext:

VD2: k = 4018975632

Ciphertext:

VD2: k = 0185947263

Ciphertext:

Kerckhoff’s Principle for Cryptosystem

- The cryptosystem should be unbreakable practically, if not mathematically.
- Falling of the cryptosystem in the hands of an intruder should not lead to any compromise of the system, preventing any inconvenience to the user.
- The key should be easily communicable, memorable, and changeable.
- The ciphertext should be transmissible by telegraph, an unsecure channel.
- The encryption apparatus and documents should be portable and operable by a single person.
- Finally, it is necessary that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Attacks

- Attacks are typically categorized based on the action performed by the attacker. An attack, thus, can be **passive** or **active**
- Passive Attacks. The main goal of a passive attack is to obtain **unauthorized access to the information**.
- Active Attacks. An active attack involves changing the information in some way by conducting some process on the information.

Assumptions of Attacker

- Environment around Cryptosystem
- Details of the Encryption Scheme
- Availability of Ciphertext
- Availability of Plaintext and Ciphertext

Cryptographic Attacks

- **Ciphertext Only Attacks (COA)**
- **Known Plaintext Attack (KPA)**
- **Chosen Plaintext Attack (CPA)**
- **Dictionary Attack**
- **Brute Force Attack (BFA)**
- **Birthday Attack**
- **Man in Middle Attack (MIM)**
- **Side Channel Attack (SCA)**
- **Timing Attacks**
- **Power Analysis Attacks**
- **Fault analysis Attacks**

Practicality of Attacks

References

- https://www.tutorialspoint.com/cryptography/block_cipher.htm