01. Introduction to Information Security and Cryptography

Hyung Tae Lee

Spring 2025

Introduction to Information Security

Computer Security

Computer Security [NIST95]

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity, availability, and confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommuncations)

- **CIA triad**
  1. **Confidentiality**: Data confidentiality, privacy
  2. **Integrity**: Data integrity, system integrity
  3. **Availability**
- Additional requirements: Authenticity, Accountability

Image from https://medium.com/@mohanathasholins17/cia-triad-in-cyber-security-d71e1dc45e1c

Security Terminology (from RFC 2828)

- **Adversary (threat agent)**: An entity that attacks a system
- **Attack**: An assault on system security that derives from an intelligent threat
- **Countermeasure**: An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack
- **Risk**: An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result
- **Security Policy**: A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical assets
- **System Resource (Asset)**: Data contained in an information system; or a service provided by a system; or a system capability; or a facility that houses system operations and equipment
- **Threat**: A potential violation of security, which exists when there is a circumstance, capability, action, or event, that could breach security and cause harm
- **Vulnerability**: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

Security Concept and Relations

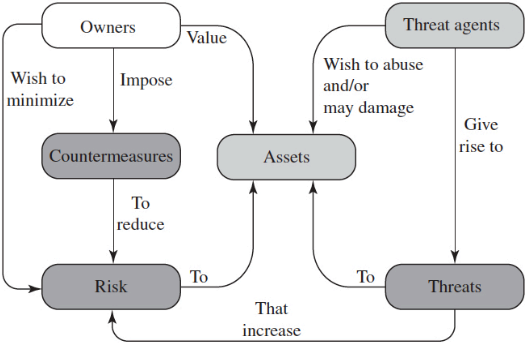


Figure 1.1 Security Concepts and Relationships

Types of Vulnerability, Attacks and Countermeasure

- Vulnerability
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)
- Attacks
  - Passive vs. Active
  - Insider vs. Outsider
- Countermeasure
  - Prevent
  - Detect
  - Recover

Scope of Computer Security

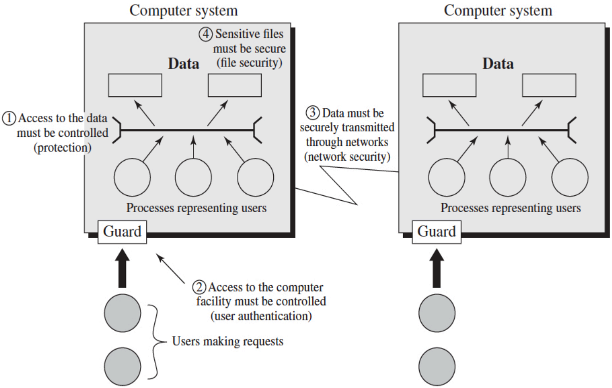


Figure 1.2 **Scope of Computer Security**

Fundamental Security Design Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

Attack Surfaces

- Attack surface: consists of the reachable and exploitable vulnerabilities in a system
  - **Network**: vulnerabilities over an enterprises, wide-area network, or the Internet, particularly, included in this category are network protocol vulnerabilities, e.g., a denial-of-service attack, disruption of communications links
  - **Software**: vulnerabilities in application, utility, or operating system code
  - **Human**: vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Computer Security Strategy

- **Security policy**: a formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
- **Security implementation**: involves prevention, detection, response, and recovery
- **Security assurance**: the degree of confidence one has that the security measures work as intended to protect the system and the information it processes
- **Security evaluation**: the process of examining a computer product or system with respect to certain creteria

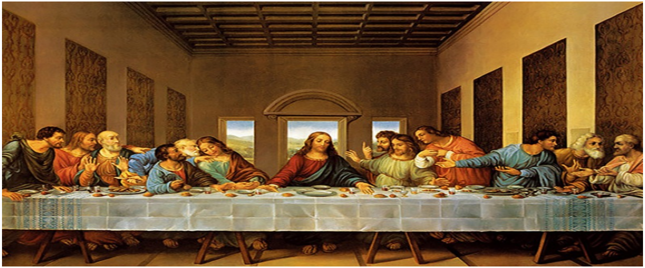
Introduction to Cryptography

Classical Cryptography

Concise Oxford Dictionary (2006) [KL08]

The art of writing or solving codes

- Consider secure communication
- Codes? Is Robert Langdon a cryptographer?



- Code, decode, encipher, decipher...
  - Unused terminology in "modern" cryptography

Modern Cryptography

Modern Cryptography [KL08, Chapter 1]

The scientific study of techniques for securing digital information, transactions, and distributed computations

- Range of modern cryptography
  - Primitives: Hash function (for data integrity), random number generator
  - Schemes: Encryption (for confidentiality), Signature (for data integrity)
  - Protocols: Identification (for authenticity), Key establishment, Secret sharing
  - Cryptographic applications: secure internet protocols, electronic cash

Encryption

- A technique to provide data confidentiality
- Symmetric (key) encryption (a.k.a, Secret key/Private key encryption)
  - Block cipher
  - Stream cipher
- Asymmetric (key) encryption (a.k.a, Public key encryption)
  - Factoring-based
  - Discrete Logarithm-based
  - Post-quantum secure encryption: Lattice-based, Code-based, $\cdots$
- Consist of the following three algorithms:
  - Setup algorithm: Setup(λ)$\rightarrow$ (K_{Enc}, K_{Dec})
  - Encryption algorithm: Enc(K_{Enc}, M)$\rightarrow$ CT
  - Decryption algorithm: Dec(K_{Dec}, CT)$\rightarrow$ M

Symmetric Encryption

- Assume that a sender and a receiver have the same key
  $\Rightarrow$ Symmetric/Private key

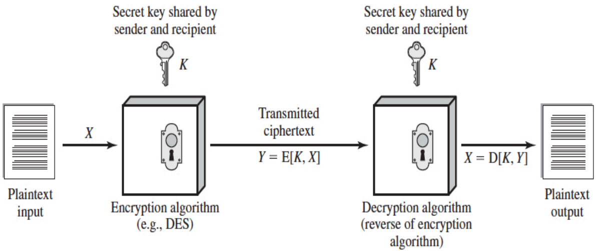


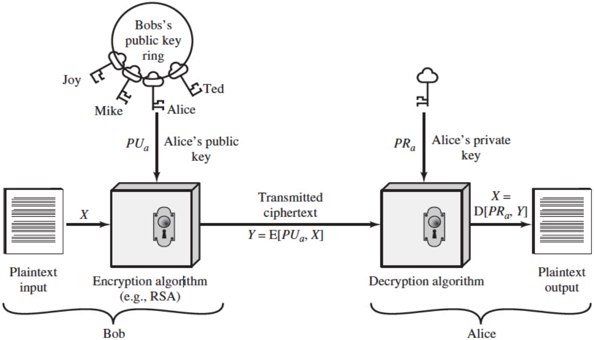
Figure 2.1 **Simplified Model of Symmetric Encryption**

- Classical encryption, block cipher (DES, AES, ARIA, SEED), stream cipher (RC4, ChaCha)
- Pros: Faster than asymmetric (public key) encryption
- Cons: Key share problem, large number of keys

Picture from [SB15]

Asymmetric Encryption

- A key for encryption is different from a key for decryption



(a) Encryption with public key

- RSA, ElGamal, NTRU
- Pros: Easy for key sharing, small number of keys
- Cons: Slower than symmetric (private key) encryption

Picture from [SB15]

Terminology for Encryption

- **Plaintext**: The original message or data that is fed into the algorithm as input
- **Ciphertext**: An output of an encryption algorithm
- **Encryption (algorithm)**: An algorithm that takes a plaintext and a key as inputs, and returns a ciphertext
- **Decryption (algorithm)**: An algorithm that takes a ciphertext and a key as inputs, and returns a plaintext
- **Private key** (for symmetric encryption): An input of encryption and decryption algorithms, those algorithms depend on a private key
- **Public key and private key** (for public key encryption): A pair of keys that have been selected for encryption and decryption, respectively

Kerckhoff's Principle

- Stated by Dutch cryptographer Auguste Kerckhoffs in the late 19th century
- Recall **Open Design** in fundamental security design principles

Kerckhoff's principle [KL08]

The cipher method (= encryption and decryption algorithms) must not be required to be secret, and it must be able to fall into the hands of the enemy (=adversary) without inconvenience.

- Primary arguments in favor of Kerckhoff's principle
  - Easier for parties to maintain a secrecy of a short key than an algorithm
  - Easier to maintain a system once a key is exposed
  - Easier for parties to communicate with others by using different keys, not algorithms

Basic Types of Attacks against Encryption

1. Brute-force attack: An attack that tries all possible keys on a target ciphertext until intelligible translation into plaintext is obtained

2. Cryptanalysis

Types of attacks	Information given to an adversary
Ciphertext only	ciphertexts
Known plaintext	pairs of plaintexts and ciphertexts
Chosen plaintext	ciphertexts of plaintexts chosen by an adversary
Chosen ciphertext	plaintexts of ciphertexts chosen by an adversary

Classical Encryption

Notations

- $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$
- g mod p: the remainder when g is divided by p

$$\begin{aligned} 10 \bmod 3 &= 1 \\ 729 \bmod 31 &= 16 \ (\because 729 = 23 \cdot 31 + 16) \\ -7 \bmod 26 &= 19 \ (\because -7 = 26 \cdot (-1) + 19) \end{aligned}$$

- Plaintext space = Ciphertext space = {Alphabet characters} = $\mathbb{Z}_{26}$

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Shift Cipher

Shift Cipher

For $0 \leq K \leq 25$,

- $\mathrm{Enc}(K, x) = (x + K) \bmod 26$ (cf. $K = 3$: Caesar Cipher)
- $\mathrm{Dec}(K, Y) = (Y - K) \bmod 26$

Example: $K = 9$

- shift (18 7 8 5 19) $\xrightarrow{+9 \bmod 26}$ (1 16 17 14 2) BQROC
- BQROC (1 16 17 14 2) $\xrightarrow{-9 \bmod 26}$ (18 7 8 5 19) shift

Attacks

- Brute-force attack: There are only 26 candidates for private key.
- Known plaintext attack: Given (shift, BQROC),

$$K = \mathrm{B} - \mathrm{s} = (1 - 18) \bmod 26 = 9$$

Affine Cipher

Affine Cipher

For $K = (\alpha, \beta)$ where $\alpha, \beta \in \mathbb{Z}_{26}$ and $\gcd(\alpha, 26) = 1$,

- $\mathrm{Enc}(K, x) = \alpha x + \beta \bmod 26$
- $\mathrm{Dec}(K, Y) = \alpha^{-1}(Y - \beta) \bmod 26$

Example: $K = (\alpha, \beta) = (7, 3)$

hot (7 14 19) $\xrightarrow{(\alpha,\beta)=(7,3)}$ (52 101 136) mod26 = (0 23 6) AXG

Attacks

- Brute-force attack: There are only $12 \times 26 = 312$ candidates for private key. (α such that $\gcd(\alpha, 26) = 1$: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25)
- Known plaintext attack: Given (hot, AXG),

$$\begin{cases} 7\alpha + \beta = 0 \bmod 26 \\ 14\alpha + \beta = 23 \bmod 26 \end{cases} \Rightarrow \alpha = 7, \beta = 3$$

$$(\text{cf. } 7^{-1} = 15 \bmod 26 \ (\because 15 \cdot 7 = 105 = 1 \bmod 26)$$

Substitution Cipher

Substitution Cipher

For K $= \pi$ where π is a permutation on $\mathbb{Z}_{26}$,

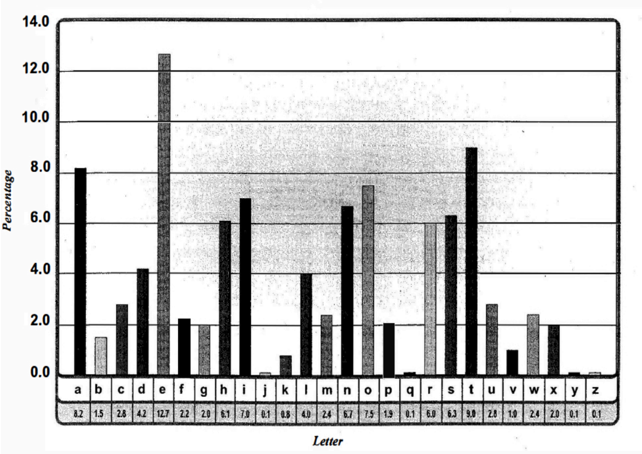
- $\mathrm{Enc}(K, x) = \pi(x)$
- $\mathrm{Dec}(K, Y) = \pi^{-1}(Y)$

Attacks

- Brute-force attack: There are 26! candidates for private keys.
  $\Rightarrow 26! \approx 4 \times 10^{26} \approx 2^{88.3}$
- Chosen-plaintext attack? If n pairs are given, the number of candidates is reduced to $(26 - n)!$.

Statistical Test

- Use average letter frequencies for English-language text



Picture from [KL08]

Example: Statistical Test

Ciphertext [Sti06, Section 1.2.2]

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

Letter	Frequency	Letter	Frequency	Letter	Frequency	Letter	Frequency
A	0	H	4	O	0	V	5
B	1	I	5	P	1	W	8
C	15	J	11	Q	4	X	6
D	13	K	1	R	10	Y	10
E	7	L	0	S	3	Z	20
F	11	M	16	T	2		
G	1	N	9	U	5		

- $\mathrm{Dec}(K, Z) = e \Rightarrow \ldots$

Example: Solution

Solution

Our friend from Paris examined his empty glass with surprise, as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sum.

Vigenère Cipher

- Named after Blaise de Vigenère who lived in the 16th century
- Monoalphabetic $\Rightarrow$ Polyalphabetic

Vigenère Cipher

For $K = (k_1, k_2, \ldots, k_m) \in (\mathbb{Z}_{26})^m$,

- $\mathrm{Enc}(K, x_1, \ldots, x_m) = (x_1 + k_1, \ldots, x_m + k_m)$
- $\mathrm{Dec}(K, Y_1, \ldots, Y_m) = (Y_1 - k_1, \ldots, Y_m - k_m)$

Attacks

- Brute-force attack: There are 26^m candidates for private keys.
  $\Rightarrow m = 18 : 26^{18} \approx 2^{84.6}$
- Ciphertext only attack: Statistical test such as Kasiski test
- Known plaintext attack: Easy (if m is known)

Permutation Cipher

Permutation Cipher

For a key $K = \pi$ where π is a permutation of $\{1, \ldots m\}$,

- $\mathrm{Enc}(K, x_1, \ldots, x_m) = (x_{\pi(1)}, \ldots, x_{\pi(m)})$
- $\mathrm{Dec}(K, Y_1, \ldots, Y_m) = (Y_{\pi^{-1}(1)}, \ldots, Y_{\pi^{-1}(m)})$

- We can interpret the above encryption algorithm as

$$(x_1 \ \ldots x_m)P = (Y_1 \ \ldots Y_m)$$

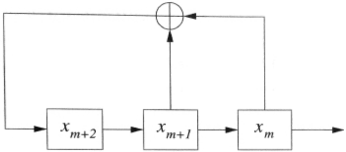
  where P is a permutation matrix.
- If P is an inverse matrix, it is Hill cipher.

Attacks

- Brute-force attack: There are $m!$ candidates for private keys.
  $\Rightarrow 25! \approx 2^{83.68}$
- Known plaintext/Chosen plaintext attacks: Need m "independent" ciphertexts to obtain P^{-1}

Linear Feedback Shift Register (LFSR)

- A shift register whose input bit is a linear function of its previous state
- Example I: a shift register satisfying $\underbrace{x_{m+3} = x_{m+1} + x_m}_{\text{linear relation}}$



- Example II: The sequence

$$0100001001011001111100011$$

is generated by giving initial values $x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0$, and $x_5 = 0$, and the linear relation

$$x_{n+5} = x_n + x_{n+2} \bmod 2.$$

Picture and example from [TW06]

LFSR Cipher

LFSR Cipher

For a linear function $f(z_1, \ldots z_\ell) = \sum_{i=1}^{\ell} c_i z_i$ with constant c_i's and a key $K = (k_1, \ldots, k_\ell) \in (\mathbb{Z}_2)^\ell$

- $\mathrm{Enc}(K, (x_1, \ldots, x_m)) = (x_1 \oplus k_1, \ldots, x_m \oplus k_m)$
- $\mathrm{Dec}(K, (y_1, \ldots, y_m)) = (y_1 \oplus k_1, \ldots, y_m \oplus k_m)$

where $k_j = f(k_{j-\ell}, k_{j-\ell+1}, \ldots k_{j-1})$ for $\ell + 1 \leq j \leq m$

Known Plaintext Attack

1. Find $k_1, \ldots, k_\ell$ from $((x_1, \ldots, x_m), (y_1, \ldots, y_m))$.
2. Build

$$\underbrace{\begin{pmatrix} k_1 & k_2 & \cdots & k_\ell \\ k_2 & k_3 & \cdots & k_{\ell+1} \\ \vdots & \vdots & \ddots & \vdots \\ k_\ell & k_{\ell+1} & \cdots & k_{2\ell-1} \end{pmatrix}}_{:=\mathbf{K}} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_\ell \end{pmatrix} = \begin{pmatrix} k_{\ell+1} \\ k_{\ell+2} \\ \vdots \\ k_{2\ell} \end{pmatrix}.$$

3. Obtain $(k_1, \ldots, k_m)$ if the matrix $\mathbf{K}$ is invertible.

One-Time Pads

- Developed by Gilbert Vernam and Joseph Mauborgne in 1918

One-Time Pads

- Plaintext space = Ciphertext space = Key space = $(\mathbb{Z}_2)^m$
- For a key $K = (k_1, \ldots, k_m) \in (\mathbb{Z}_2)^m$,
  - $\mathrm{Enc}(K, x_1, \ldots, x_m) = K \oplus (x_1, \ldots, x_m)$
  - $\mathrm{Dec}(K, Y_1, \ldots, Y_m) = K \oplus (Y_1, \ldots, Y_m)$

- Use a key K only once and throw it away
- Pros: Perfect secrecy - unbreakable cryptosystem
- Cons: Efficiency - Need a different key at each time

References

KL08 J. Katz and Y. Lindell, Introduction to Modern Cryptography, Chapman & Hall/CRC, 2008 (Chapter 1).

SB15 W. Stallings and L. Brown, Computer Security: Principles and Practice, 3rd edition, Pearson Prentice Hall, 2015 (Chapters 2, 20, & 21)

Sti06 D. R. Stinson, Cryptography: Theory and Practice, 3rd edition, Chapman & Hall/CRC, 2006 (Chapter 1).

TW06 W. Trappe and L. C. Washington, Introduction to Cryptography with Coding Theory, 2nd edition, Pearson Prentice Hall, 2006 (Chapters 1 & 2)