Symmetric Encryption

Part 1

Cryptography

- Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries.
- It deals with developing and analyzing protocols that prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.
- In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security.

Core Principles of Cryptography

- Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

Data Confidentiality

- Principle and practice of ensuring that sensitive or confidential data is protected from unauthorized access, disclosure, or exposure.
- It involves implementing measures and controls to restrict access to confidential information, ensuring that only authorized individuals or entities can access and view it.

Data Integrity

- Data integrity in information security refers to the assurance that data remains accurate, consistent, and trustworthy over time.
- It ensures that data is protected from unauthorized modifications, corruption, or tampering, and that it retains its intended meaning and reliability.

Core Principles of Cryptography

Authentication

- Authentication in information security is the process of verifying the identity of an individual or entity.
- It ensures that the claimed identity is valid and trustworthy.

Non-repudiation

- Non-repudiation refers to the assurance that a sender of a message cannot deny sending it and a receiver cannot deny receiving it.
- It provides proof of the integrity and origin of a communication, making it legally binding and irrefutable.
- Non-repudiation is achieved through techniques such as digital signatures and audit trails, which ensure that actions or transactions can be traced back to the responsible parties, preventing them from denying their involvement in the communication or transaction.

Types of Cryptography

- There are several types of cryptography, each with its own applications and security properties:
  - **Symmetric-key cryptography:** Uses a single shared key for both encryption and decryption.
  - **Asymmetric-key cryptography (Public-key cryptography):** Uses a pair of keys, a public key for encryption and a private key for decryption.
  - **Hash functions:** Transform data into a fixed-length hash value, used for data integrity verification and password storage.
  - **Digital signatures:** Use asymmetric-key cryptography to verify the authenticity and integrity of digital documents or messages.
  - **Key exchange algorithms:** Securely exchange encryption keys between parties to establish secure communication channels.
  - **Homomorphic encryption:** Allows computations to be performed on encrypted data without decrypting it.
  - **Quantum cryptography:** Uses principles of quantum mechanics to provide secure communication and key distribution.

Related Terminologies

Cryptanalysis (Codebreaking)

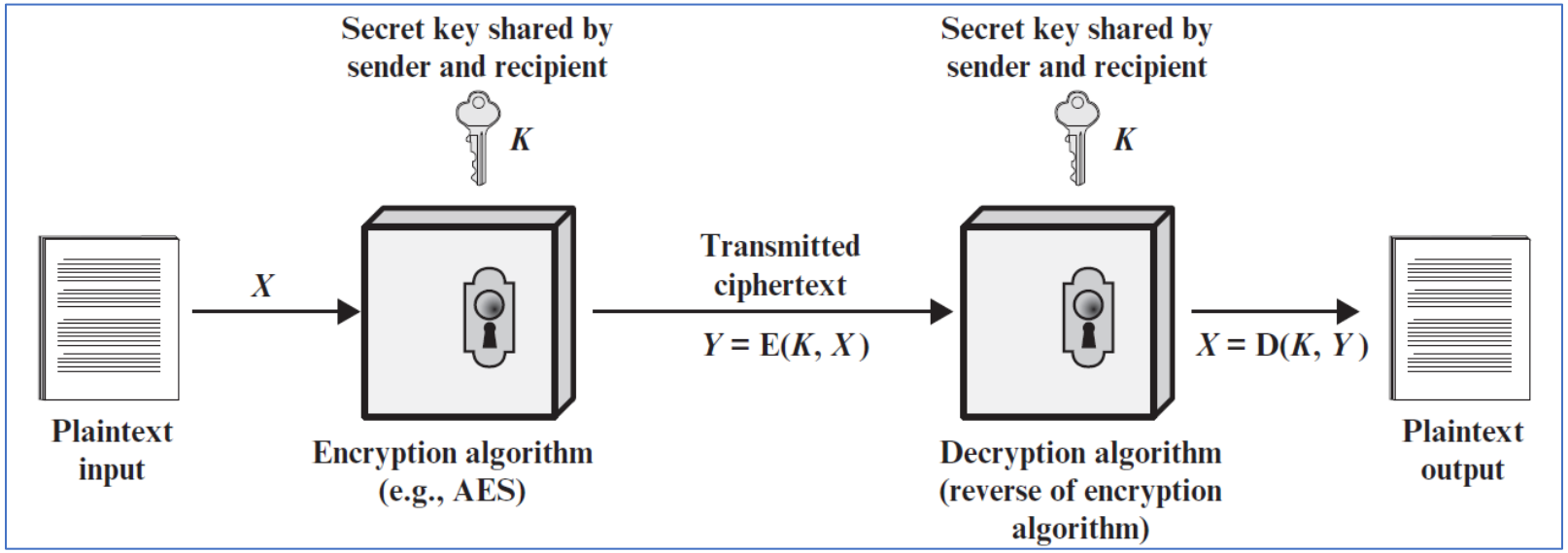
- The process of studying and analyzing cryptographic systems to uncover their vulnerabilities and decrypt encrypted messages without knowing the secret key.
- It involves analyzing patterns, algorithms, and weaknesses in order to break the encryption and gain unauthorized access to the protected information.

Cryptology

- The study and practice of secure communication and data protection.
- It encompasses both cryptography, which focuses on encryption and decryption techniques, and cryptanalysis, which involves analyzing and breaking encrypted messages.

Symmetric Cryptography

- Symmetric encryption is a cryptographic technique where the same secret key is used for both the encryption and decryption processes.
- Also known as **Conventional**, **Private-key**, or **Single-key cryptography**.
- The sender uses this key to transform plaintext into ciphertext, and the recipient uses the same key to reverse the process and recover the original plaintext.



Symmetric Cryptography

- A symmetric encryption scheme has five ingredients:
  1. **Plaintext**: This is the original intelligible message or data that is fed into the algorithm as input.
  2. **Encryption algorithm (Cipher):** The encryption algorithm performs various substitutions and transformations on the plaintext.
  3. **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
  4. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
  5. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Related Terminologies, Requirements, and Assumptions

Related Terminologies

- **Encrypt (Encipher):** The action of converting plaintext to ciphertext.
- **Decrypt (Decipher):** The action of recovering plaintext from ciphertext.

Two Requirements

- The following two requirements must be fulfilled for a symmetric encryption scheme to work:
  1. A strong encryption algorithm that is complex enough, and
  2. A secret key known only to sender and receiver (also, sometimes known to trusted third parties).

Assumption

- It is assumed that the encryption and decryption algorithm is known to the public (including adversaries and attackers).

Mathematical Representation

- The operation of encryption and decryption can be denoted as the following:

$$Y = E\ (X, K)$$

$$X = D\ (Y, K)$$

Notation	Meaning
X	Plaintext
Y	Ciphertext
K	Symmetric Encryption Key (Secret Key)
E	Encryption Algorithm
D	Decryption Algorithm

Video Demonstration

- https://www.youtube.com/watch?v=AQDCe585Lnc
- https://www.youtube.com/watch?v=FmWH1gMvOD8
- https://www.youtube.com/watch?v=hP7-kuHBLD4

Classical Substitution Cipher

- A classical substitution cipher is a type of encryption technique where each letter in the plaintext is replaced with a different letter from the alphabet, or by some numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.
- To decrypt the ciphertext, the recipient needs to know the exact substitution mapping and reverse the process by replacing each ciphered letter with its corresponding plaintext letter.
- Examples: Caesar Cipher, Vigenère Cipher, Simple Substitution Cipher, Atbash Cipher, Polybius Square, Playfair Cipher, and so on.

Caesar Cipher

- The Caesar cipher is one of the simplest and oldest encryption techniques.
- It was named after Roman Emperor Julius Caesar who used this cipher technique.
- It involves shifting each letter of the plaintext a certain number of positions down the alphabet.
- For example, with a shift of 3, "A" would become "D," "B" would become "E," and so on.
- This substitution process is applied to the entire message, resulting in the ciphertext.
- To decrypt the message, the recipient performs the reverse shift, shifting each letter back up the alphabet.
- The Caesar cipher is a type of substitution cipher and can be easily cracked through frequency analysis.
- Despite its simplicity, the Caesar cipher laid the foundation for modern encryption techniques.

Caesar Cipher

Caesar Cipher 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

- Replace by 3rd letter on the right (shift +3).

Plaintext	Ciphertext
cyber security	FBEHU VHFXULWB

- Replace by 7th letter on the left (shift -7).

Plaintext	Ciphertext
cyber security	VRUXK LXVNKBMR

Mathematical Representation of Caesar Cipher

- **Alphabets with numbers**

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **Encryption**

$$Y = E(X, K) = (X + k) \, mod \, (26)$$

- **Decryption**

$$X = D(Y, K) = (Y - k) \, mod \, (26)$$

- **Online Caesar Cipher**

https://cryptii.com/pipes/caesar-cipher

Exercise on Caesar Cipher

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Key = +5

Plaintext	Ciphertext
computer science	?

- Key = -4

Ciphertext	Plaintext
YWAOWN YELDAN	?

Exercise on Caesar Cipher

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Key = +5

Plaintext	Ciphertext
computer science	HTRUZYJW XHNJSHJ

- Key = -4

Ciphertext	Plaintext
YWAOWN YELDAN	caesar cipher

Cryptanalysis of Caesar Cipher

- For English alphabet set, there are only 26 possible ciphers.
- Within any ciphertext, letter ‘A’ maps to either ‘A’, ‘B’, ‘C’, …, ‘Z’
- Cryptanalysis would simply try each letter in turn to try to find plaintext.
- Therefore, a Brute Force Search will break Caesar Cipher within a short time.
- Codebreaking must know that the ciphertext was coded using Caesar cipher.