



Cryptography Fundamentals





Scope and Coverage

- 1 Introduction to module
 - 2 Overview of security
 - 3 Overview of cryptography
 - 4 Block ciphers
 - 5 Public-key ciphers
- 



Learning Outcomes

1

Cryptographic algorithm

Explain the most common types of cryptographic algorithm (i.e. block ciphers, public-key ciphers and hash algorithms)

2

About Security fundamentals

You can find out security fundamentals here.





Computer Security - Definition

“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 telecommunications).”

National Institute of Standards and Technology,
Special Publication 800-12, (October 1995).





Cryptography - Definition

“The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.”

National Institute of Standards and Technology, Special Publication 800-59, (August 2003).





Security Objectives

NIST gives three objectives (FIPS199):

1. Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

2. Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

3. Availability: Ensuring timely and reliable access to and use of information.





Loss of Security

The following defines a loss of security in each objective:


- ***Loss of Confidentiality:*** Unauthorized disclosure of information.
- ***Loss of Integrity:*** Unauthorized modification or destruction of information.
- ***Loss of Availability:*** Disruption of access to or use of information or information systems.





The CIA Triad

These requirements (Confidentiality, Integrity, Availability) are commonly known as the ***CIA triad***.

- There are many critiques that suggest that this does not provide a complete picture of security requirements.
 - The two most commonly cited “extra” requirements are:
 - ***Authenticity***
 - ***Accountability***
- 



Authenticity

- Being genuine, verified and trusted.
- Confidence in the validity of:
 - A transmission
 - A message
 - A message originator
- Verifying that users are who they say they are and that each message came from a trusted source.





Accountability

- Actions of an entity can be traced uniquely to that entity.
- Supports:
 - ❖ Non-repudiation
 - ❖ Deterrence
 - ❖ Fault isolation
 - ❖ Intrusion detection and prevention
 - ❖ Recovery
 - ❖ Legal action





Security Attacks

- It is useful to categories attacks as:
 - Passive attacks
 - Active attacks
- **Passive attacks** make use of information from a system but do not affect the system resources.
- **Active attacks** alter system resources or affect their operation.





Overview of Cryptography

Plain Text: Unencrypted information that may be input to an encryption operation. Note: Plain text is not a synonym for clear text. See clear text. (NIST)

Example: Prime minister will arrive at Gazipur at 4 pm

Cipher Text: Series of transformations that converts plaintext to cipher text using the Cipher Key. (NIST)

Example: !@#\$%^&*%@






Overview of Cryptography

Encryption: Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used.


Example:

Decryption: If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.

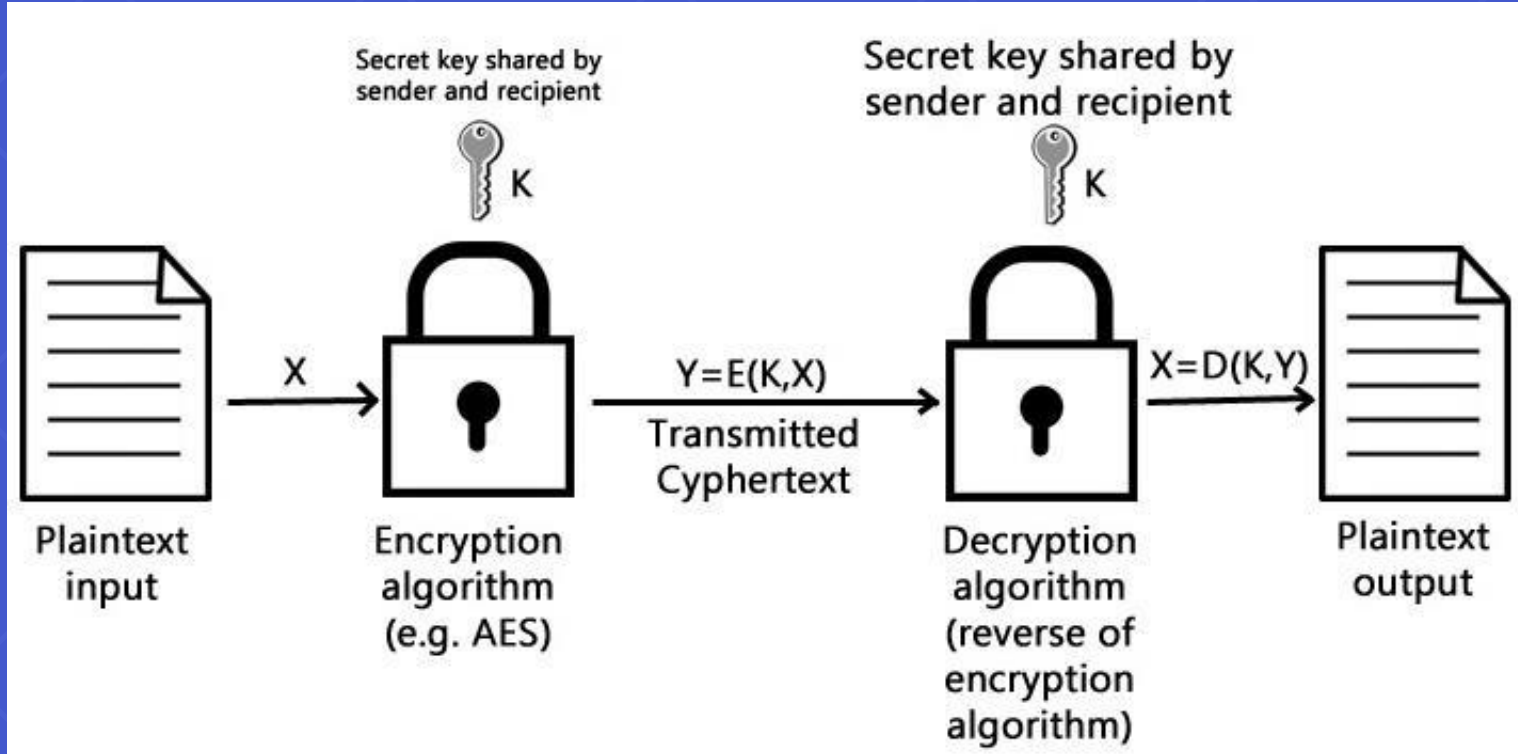




Cryptography

- A collection of mathematical techniques for protecting information
 - Most important technique is ***encryption/decryption***
 - ***Symmetric encryption*** (symmetric key encryption):
 - encrypt/decrypt a message using the same key
 - ***Key***: a piece of information or sequence of bits
 - ***Asymmetric encryption*** (asymmetric key encryption):
 - one key used for encryption (public key), another key used for decryption (private key)
- 

Symmetric Encryption





Elements of Symmetric Encryption

- Plaintext
- Encryption algorithm
- Secret key
- Ciphertext (encrypted text)
- Decryption algorithm





Principle of Symmetric Encryption

- Security of symmetric encryption depends on the secrecy of the key.
- It does not depend on the secrecy of the algorithm.

Why?

- It is difficult to invent new algorithms and keep them secret.
 - It is relatively simple to produce keys.
- 



Requirements for Symmetric Encryption

- Strong encryption algorithm:
 - The attacker should be unable to decrypt encrypted text, even if he/she knows several matching pairs of plaintext and encrypted plaintext.
- The private key must be kept secret:
 - Sender and receiver must have obtained copies of the secret key (private key) in a secure way and must keep the key secure.



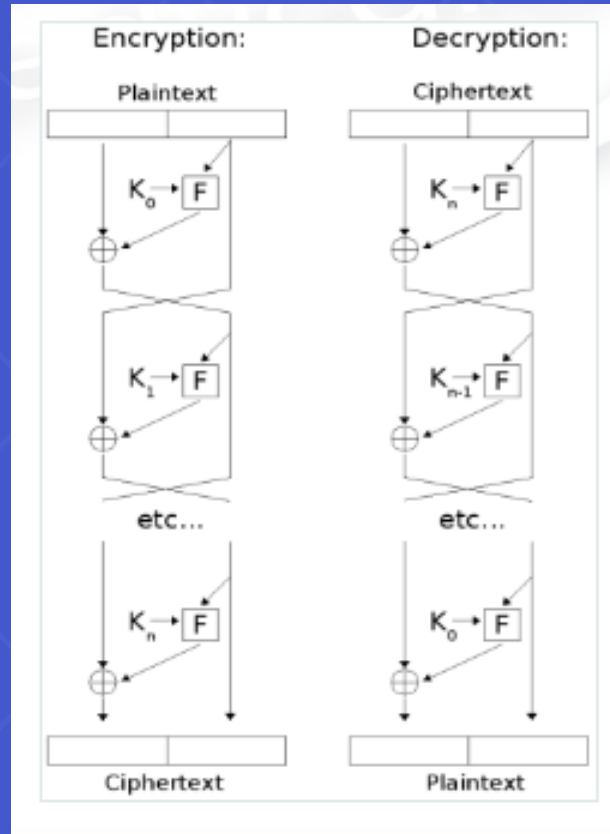


The Feistel Cipher

- A scheme used by almost all modern block ciphers.
 - The input is broken into two equal size blocks, generally called left (L) and right (R), which are then repeatedly cycled through the algorithm.
 - At each cycle, a function (f) is applied to the right block and the key, and the result is XORed into the left block.
 - The blocks are then swapped.
 - The XORed result becomes the new right block and the unaltered right block becomes the left block.
 - The process is then repeated a number of times.




The Feistel Cipher





Data Encryption Standard (DES)

- A standardized encryption algorithm approved by the U.S. government in 1977.
 - It uses a 56-bit key, which is sometimes stored with additional parity bits, extending its length to 64 bits.
 - DES is a block cipher and encrypts and decrypts 64-bit data blocks.
 - It is now considered insecure.
 - In 1998, a cracker could crack the key in 3 days.
- 




Advanced Encryption Standard (AES)

- AES replaced DES.
- A fast block cipher, with variable key length and block sizes (each can be independently set to 128, 192 or 256 bits).
- An official U.S. government standard since 2002.
- Now widely used for commercial and private encryption purposes.
- The algorithm is public, and its use is unrestricted, with no royalties or license fees owed to the inventors or the government.





Public Key Cryptography – 1

- Uses asymmetric key algorithms
 - The key used to encrypt a message is not the same as the key used to decrypt it.
 - Each user has a pair of cryptographic keys:
 - ***a public encryption key***, publicly available and widely distributed.
 - ***a private decryption key***, known only to the recipient.
- 

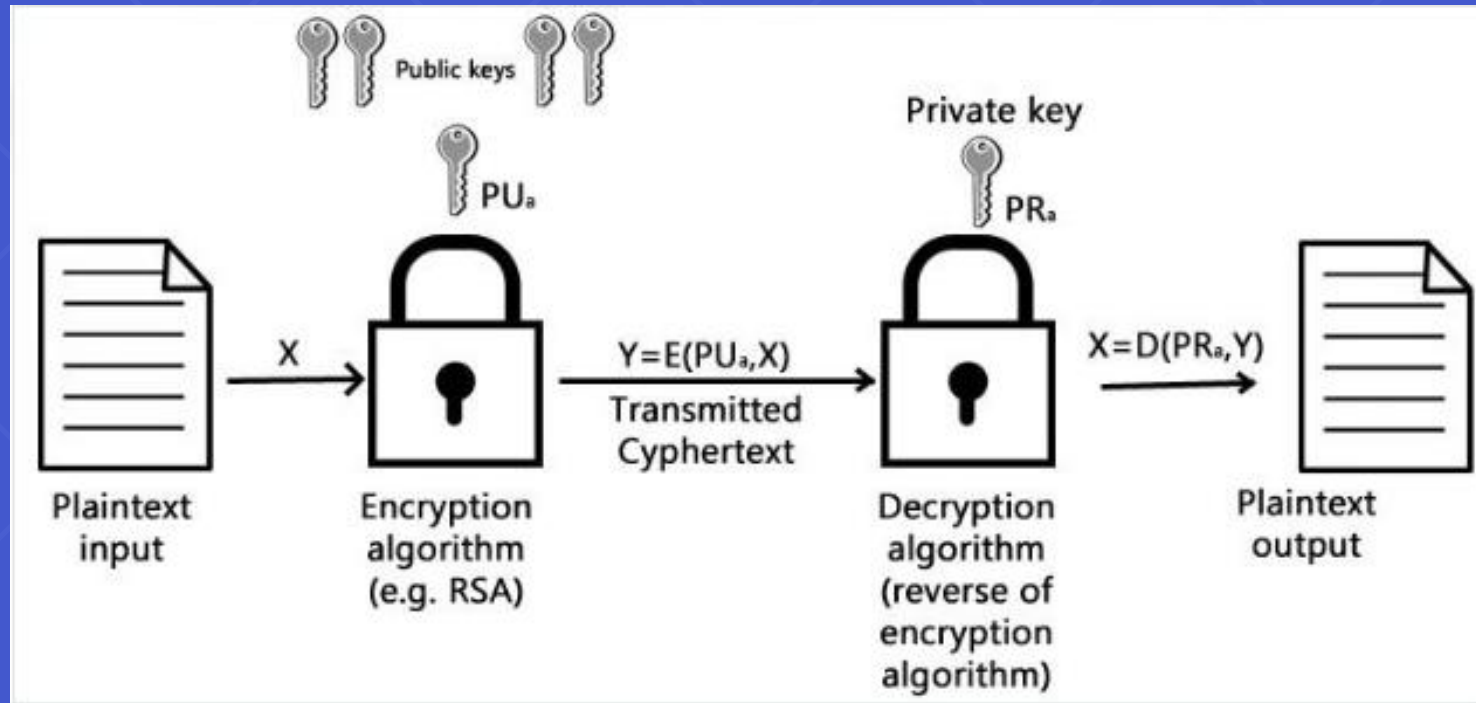


Public Key Cryptography - 2

- Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key.
- The keys are related mathematically.
- Parameters are chosen so that determining the private key from the public key is prohibitively expensive.




Public Key Cryptography





Public Key Cryptography – Applications

- ***Encryption/decryption:*** the sender encrypts a message with the recipient's public key.
 - ***Digital signature (authentication):*** the sender “signs” the message with its private key; a receiver can verify the identity of the sender using sender's public key.
 - ***Key exchange:*** both sender and receiver cooperate to exchange a (session) key.
- 



Hash Functions

- A ***hash function*** is a mathematical function that converts a large, possibly variably-sized amount of data into a small datum.
- Hashing is a method of binding the file contents together to ensure integrity.
 - Like using sealing wax on an envelope.
 - Only by breaking the seal can the contents be accessed, and any tampering is readily apparent.





Hash Function Requirements

- To be suitable for message authentication, a hash function H should have the following properties:
 - H can be applied to a block of data of any size
 - H produces a fixed-length output
 - $H(x)$ is easy to compute for any given x
 - For any value h it is very difficult (infeasible) to compute x such that $H(x)=h$
 - For any given x , it is very difficult (infeasible) to find y (not equal to x) such that $H(x) = H(y)$
 - It is very difficult (infeasible) to find any pair (x,y) such that $H(x) = H(y)$






The SHA-1 Secure Hash Algorithm

- Takes as input a message with a maximum length less than 2^{64} bits and produces as output a 160-bit message digest.
- The input is processed in 512-bit blocks.
- Each bit of the output is computed using all bits of the input.





SHA-1 Examples

- SHA1("The quick brown fox jumps over the lazy dog") =
2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
 - A small change in the message will, with overwhelming probability, result in a completely different hash.
 - SHA1("The quick brown fox jumps over the lazy cog") =
de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3
- 



Two-Factor Authentication (2FA)

- In today's world, online security is more important than ever.
- Two-factor authentication (2FA) is a simple and effective way to add an extra layer of security to your account.

❖ What is Two-Factor Authentication?

- Two-factor authentication (2FA) is a security process that requires two forms of identification to access an account.
- The first factor is typically a password or PIN, which you already know.
- The second factor is something you have or something you are, such as a fingerprint or a one-time code sent to your phone.





How Does Two-Factor Authentication Work?

- When you enable 2FA, you'll need to enter your password as usual, but you'll also be prompted for a second form of authentication.
- The second factor could be a code generated by an app, sent to your phone via text message, or even a physical key that you plug into your computer.
- Once you provide both factors of authentication, you'll be logged in to your account.





Examples

Examples of Two-Factor Authentication:

- Text message codes
- Authenticator apps like Google Authenticator and Microsoft Authenticator
- Physical security keys like YubiKey
- Biometric authentication like fingerprints and facial recognition





Examples

Examples of Two-Factor Authentication:

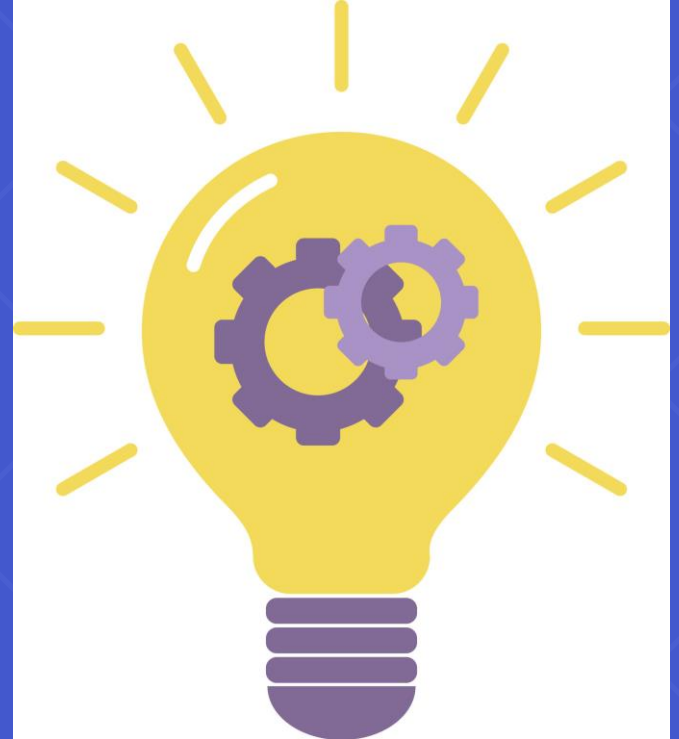
- Text message codes
- Authenticator apps like Google Authenticator and Microsoft Authenticator
- Physical security keys like YubiKey
- Biometric authentication like fingerprints and facial recognition



Intellectual Property

Intellectual Property (IP) refers to creations of the mind, such as inventions, literary and artistic works, symbols, names, and designs, used in commerce.

It is protected by law, which allows the creators or owners to have exclusive rights to their creations.





Types of Intellectual Property

- There are four main types of intellectual property:
 1. Patents: protect inventions and discoveries.
 2. Trademarks: protect words, symbols, and designs used to identify and distinguish goods or services.
 3. Copyrights: protect original works of authorship, such as books, music, and movies.
 4. Trade Secrets: protect confidential information that provides a competitive advantage.



ICT and Digital Security Act Bangladesh

- The ICT and Digital Security Act Bangladesh was passed in 2018 to address the growing concerns of digital security threats in the country.
- The act aims to protect against cybercrime, defamation, and other digital security issues.





ICT and Digital Security Act Bangladesh

- Official website link: <http://bdlaws.minlaw.gov.bd/act-1261.html>





Key Provisions

- The act includes provisions for punishment for offenses such as hacking, spreading propaganda, and cyber terrorism.
- It also includes provisions for the protection of personal data and privacy.
- The act allows law enforcement agencies to seize digital devices for investigation purposes.





Criticism

- The act has faced criticism for its potential to limit freedom of expression and for vague language that could be used to suppress dissent.
- Some critics have called for amendments to the act to ensure it does not violate fundamental rights.





Conclusion

- The ICT and Digital Security Act Bangladesh is an important step towards ensuring digital security in the country.
- While it has faced criticism, it is important to balance the need for security with the protection of fundamental rights.





THE END

ANY QUESTION?

