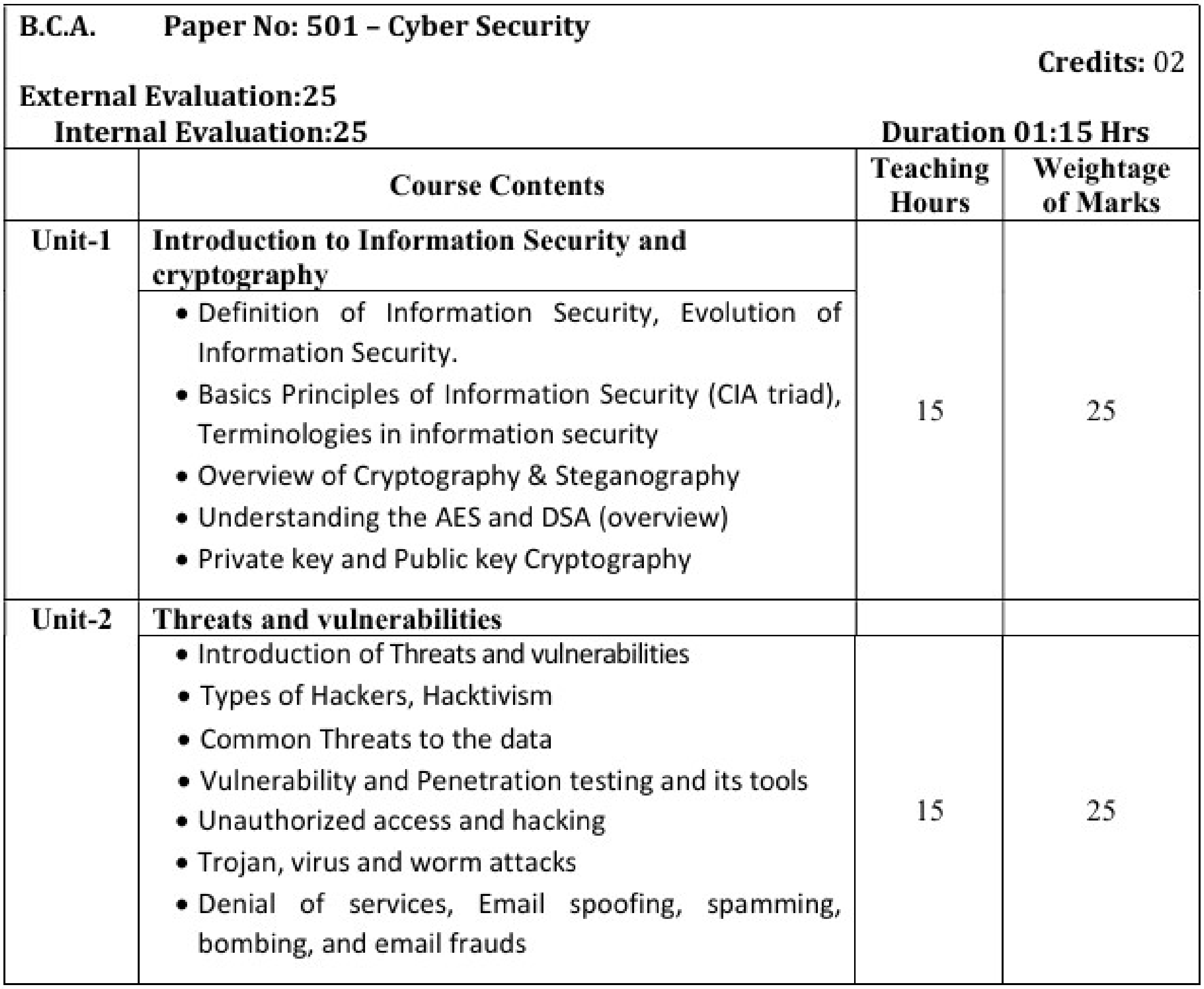


B.C.A. Paper No: 501 – Cyber Security

Credits: 02

External Evaluation:25

Internal Evaluation:25 **Duration 01:15 Hrs**

	Course Contents	**Teaching Hours**	**Weightage of Marks**
Unit-1	**Introduction to Information Security and cryptography** • Definition of Information Security, Evolution of Information Security. • Basics Principles of Information Security (CIA triad), Terminologies in information security • Overview of Cryptography & Steganography • Understanding the AES and DSA (overview) • Private key and Public key Cryptography	15	25
Unit-2	**Threats and vulnerabilities** • Introduction of Threats and vulnerabilities • Types of Hackers, Hacktivism • Common Threats to the data • Vulnerability and Penetration testing and its tools • Unauthorized access and hacking • Trojan, virus and worm attacks • Denial of services, Email spoofing, spamming, bombing, and email frauds	15	25

UNIT -1

Definition of Information Security, Evolution of Information Security.

Definition of Information Security:

Information Security (Info Sec) refers to the practice of protecting information and information systems from unauthorized access, disclosure, modification, destruction, or disruption. The goal is to ensure the **confidentiality**, **integrity**, and **availability** of data — commonly known as the **CIA Triad**.

Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

What is Information Security?

- Information Security (Info Sec) refers to the practice of protecting information from:
- Unauthorized access
- Disclosure(leak, escape)
- Modification
- Destruction(demolition(pulling down)
- Disruption(disturbance)

Why is Information Security Important?

- Protects **personal and financial data**
- Prevents **cyber-attacks**
- Safeguards **intellectual property**
- Maintains **trust** and **regulatory compliance**

Key Objectives of Information Security:

1. **Confidentiality** – Ensuring that only authorized individuals have access to information.
2. **Integrity** – Protecting information from being altered or tampered with.
3. **Availability** – Making sure that information and systems are accessible when needed.

Evolution of Information Security:

The evolution of information security can be divided into key phases:

1. Pre-Computer Era (Before 1960s)

- Security was physical (e.g., safes, locks, file cabinets).
- Information was stored on paper; protection was limited to physical access control.

2. Mainframe Era (1960s–1970s)

- Large centralized computers began storing digital data.
- Access control lists (ACLs) and password protection were introduced.
- Security was focused mainly on physical and logical access.

3. Networking and Internet Era (1980s–1990s)

- Emergence of local area networks (LANs) and the internet increased data sharing.
- Security threats became more complex (e.g., viruses, hacking).
- Introduction of firewalls, antivirus software, and encryption techniques.

4. Modern Era (2000s–2010s)

- Growth of e-commerce, social media, and mobile computing increased vulnerabilities.
- Cyber security became a strategic business concern.
- Security measures included intrusion detection systems (IDS), virtual private networks (VPNs), and multi-factor authentication (MFA).

5. Current Era (2020s–Present)

- Rise of **cloud computing**, **IoT**, **AI**, and **remote work** has expanded the threat landscape.
- Advanced threats like ransomware, zero-day attacks, and nation-state cyber warfare.
- Focus on **Zero Trust Architecture**, **AI-powered threat detection**, and **cyber resilience**.
- Compliance with global standards and regulations (e.g., GDPR, HIPAA, ISO/IEC 27001) is essential.

Basics Principles of Information Security (CIA triad)

The **CIA Triad** is a foundational model in Information Security, representing the three core principles:

1. Confidentiality

- Ensures that information is accessible only to those who have authorized access.
- Protects sensitive data from unauthorized users.
- **Techniques:** Encryption, access controls, authentication.
-

2. Integrity

- Maintains the **accuracy** and **completeness** of data.
- Prevents unauthorized modification of information.
- **Techniques:** Checksums, hashing, digital signatures, version control.

3. Availability

- Ensures that information and systems are accessible to authorized users **when needed**.
- Includes maintaining hardware, performing repairs, and defending against DoS (Denial-of-Service) attacks.
- **Techniques:** Redundancy, failover, backups, and network security tools.

Terminologies in information security

Term	Definition
Asset	Anything valuable to an organization, such as data, hardware, or software.
Threat	A potential cause of an unwanted incident that may result in harm.
Vulnerability	A weakness in a system that can be exploited by a threat.
Risk	The potential for loss or damage when a threat exploits a vulnerability.
Attack	Any attempt to expose, alter, disable, destroy, steal, or gain unauthorized access.
Exploit	A piece of software or a sequence of commands that takes advantage of a vulnerability.
Firewall	A security system that controls incoming and outgoing network traffic based on rules.
Malware	Malicious software (e.g., viruses, worms, trojans) designed to harm systems.
Phishing	A social engineering attack that tricks users into revealing confidential information.
Authentication	Verifying the identity of a user or system (e.g., passwords, biometrics).
Authorization	Granting access to resources based on permissions.
Encryption	Converting data into a secure format to prevent unauthorized access.
Incident Response	The process of detecting, responding to, and recovering from security incidents.

Overview of Cryptography & Steganography

Definition:

Cryptography is the science of securing information by transforming it into an unreadable format, only understandable to those possessing a key.

Goals (Security Services):

1. **Confidentiality** – Ensures data is only accessible to authorized parties.
2. **Integrity** – Ensures data is not altered during transit.
3. **Authentication** – Confirms the identity of the sender or receiver.
4. **Non-repudiation** – Prevents denial (rejection) of sending/receiving a message.

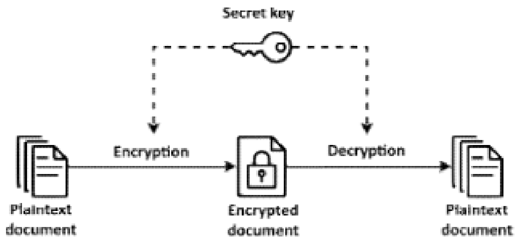
Cryptography is the science of securing information by transforming it into an unreadable format (cipher text) using mathematical techniques, so that only authorized parties can access it.

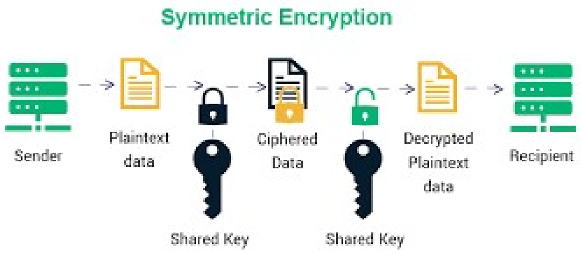
Purpose:
To ensure **confidentiality**, **integrity**, **authentication**, and **non- repudiation[**Ensuring that the signer cannot deny having signed the document.] **(Negation)** of information.

Types of Cryptography:

- **Symmetric Key Cryptography (Private Key):**
  Same key is used for both encryption and decryption.

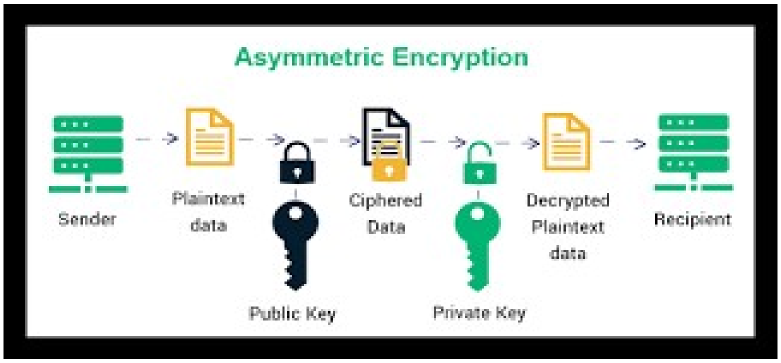
  Symmetric key cryptography, also known as secret key cryptography, uses the same key for both encrypting and decrypting data. This means a single secret key is shared between the sender and receiver for secure communication. It's a fast and efficient method, often used for encrypting large amounts of data.

- 



- **Asymmetric Key Cryptography (Public Key):**
  Uses a pair of keys – public for encryption and private for decryption.

Asymmetric cryptography, also known as public-key cryptography, utilizes a pair of mathematically linked keys: a public key and a private key.
The public key is freely shared, while the private key is kept secret.
This system enables secure communication, digital signatures, and other security applications.



Key Concepts:

- **Public Key:**

Used for encrypting data or verifying digital signatures. Anyone can obtain and use a public key.

Example: Secure Website (HTTPS):

- When you visit a secure website (HTTPS), the server has a public and private key pair.
- Your browser uses the server's public key to establish a secure, encrypted connection.
- This ensures that only the server with the corresponding private key can decrypt the information exchanged.

Public-key cryptography involves using a key pair: a public key for encryption and a private key for decryption. A common example is RSA, used in secure websites (HTTPS) and digital signatures. Other examples include Diffie-Hellman (for key exchange), ECDSA (used by Bitcoin), and DSA (Digital Signature Algorithm).

(In cyber security, RSA stands for Rivest, Shamir, Adleman. It is a public-key cryptosystem used for secure data transmission, particularly over the internet. The algorithm is named after its inventors: Ron Rivest, Adi Shamir, and Leonard Adleman.)

- **Digital Signatures:**
  - A digital signature is an electronic, encrypted stamp of authentication on digital information like documents, emails, or software. It verifies the sender's identity and confirms the information hasn't been altered. Essentially, it's the digital equivalent of a handwritten signature, but with cryptographic security features.

    Public key cryptography is used to create digital signatures, which verify the authenticity and integrity of a document or message.

- A special cryptographic function (called a hash function or hash algorithm) — This creates a hash value (a mishmash of letters and characters) of a fixed length, which masks the true size of the input and ensures the integrity of the data.

  Ex. When you visit a secure website like https://www.bank.com, public key encryption is used behind the views to encrypt data between your browser and the bank's server.

  Public keys are important because they help protect sensitive information and send it securely. **For example**, imagine sending a confidential letter that's only intended for the recipient. You might consider sending the letter in a locked box, but you would also have to send the key.

- **Private Key:**
  Used for decrypting data or creating digital signatures. Only the key's owner should have access to it.

  Example: block chain

  Private key encryption is often used to encrypt data stored or transmitted between two parties. For example, when you log in to a website using a username and password, the password is often encrypted using a private key before it is transmitted to the web server.

Applications:

- Secure email communication
- Online banking and e-commerce
- Digital signatures
- VPNs and secure web browsing (HTTPS)

---

2. Steganography

Definition:
Steganography is the art of hiding the **existence** of information by embedding(inserting) it into other non-secret media like images, audio, video, or text.
Purpose:
To conceal(hide) the **presence** of a message so that it goes undetected.

Types of Steganography:

- **Image Steganography:** Hiding data within image files by altering pixel values.
- **Audio Steganography:** Hiding data in audio files using slight changes in amplitude or frequency.
- **Text Steganography:** Concealing(hide) messages within text using patterns, spacing, or invisible characters.
- **Video Steganography:** Combining image and audio techniques in video formats.

Applications:

- secret communication
- Watermarking for copyright protection
- Secure transmission in strong environments

Aspect	Cryptography	Steganography
Goal	Protect content	Hide the existence of content
Visibility	Encrypted message is visible	Message is hidden within cover data
Detection	May attract attention	Aims to avoid doubt
Used Together	Often used with steganography for enhanced security (e.g., encrypted message hidden in an image)	

Summary:

- **Cryptography** mix up a message to protect its meaning.
- **Steganography** hides a message to protect its existence.
- Both are crucial in **information security**, and when combined, they offer **robust(healthy) data protection**.

Understanding the AES and DSA (overview)

AES (Advanced Encryption Standard) and DSA (Digital Signature Algorithm) are both cryptographic algorithms, but they serve very different purposes and are used in different contexts. Let's break them down individually:

AES (Advanced Encryption Standard)

Purpose

AES is a symmetric encryption algorithm used to securely encrypt and decrypt data. It's designed to replace the older DES (Data Encryption Standard) and is widely used in various security protocols like VPNs, and file encryption.

Key Features :

- Block cipher : AES processes fixed-size blocks (128 bits).
- Security : AES is considered highly secure and is widely used in modern encryption applications.
- Efficiency : AES is efficient in hardware and software, making it suitable for a range of devices from mobile phones to servers.

2. DSA (Digital Signature Algorithm)

Purpose

DSA is an asymmetric cryptographic algorithm used for generating and verifying digital signatures. It's used to ensure the authenticity and integrity of data and is commonly used in protocols and in the creation of digital certificates.

Key Features :

- **Asymmetric** : DSA uses a pair of keys (public and private).
- **Authentication and Integrity** : DSA ensures that a message came from a specific sender (authentication) and that it hasn't been modified (integrity).
- **Public Key Infrastructure (PKI) :** DSA is commonly used in systems that rely on public key cryptography, like digital certificates.
- **Both are fundamental in securing communications**, but they serve different roles in the cryptographic landscape. AES is focused on securing data, while DSA ensures that data has not been tampered with and verifies the identity of the sender.

Private key and public key cryptography

Private key and public key cryptography are the two main types of cryptographic systems that underpin most of modern digital security. These systems help with secure communication , authentication , data integrity , and non-repudiation . Let's break them down:

1. **Private Key Cryptography (Symmetric Cryptography)**

In private key cryptography , also known as symmetric encryption , the same key is used for both encryption and decryption .

How it Works:

- The sender and receiver both share a secret key .
- The sender uses this key to encrypt the message.
- The receiver , who also knows the key, uses it to decrypt the message.

Example:

Encryption : Bob wants to send Alice a secret message. He encrypts it with a shared secret key.

Decryption : Alice receives the encrypted message and uses the same key to decrypt it.

Key Features:

- Symmetric means the same key is used for both encryption and decryption.
- Efficiency : Symmetric algorithms (like AES) are faster than asymmetric ones.
- Key Distribution Problem : The challenge with symmetric encryption is how to securely share the secret key between the sender and receiver without someone else intercepting it.
- **Examples** : AES, DES, 3DES, RC4, etc.

Strengths:

- **Fast encryption** : Because the algorithms are computationally simpler, they can be more efficient, especially for large datasets.
- Widely used for bulk data encryption, such as in file encryption and VPNs

Weaknesses:

- **Key distribution problem** : Sharing the key securely without someone intercepting it is difficult. If someone else gets access to the secret key, they can decrypt the data.

2. Public Key Cryptography (Asymmetric Cryptography)

Public key cryptography (also called asymmetric encryption) uses two keys : a public key and a private key . These keys are mathematically linked, but you cannot derive one from the other.

How Do They Work Together?

In practice, private and public key cryptography are often used together in what's called a hybrid encryption system . This combines the strengths of both types of encryption to secure data efficiently. Here's how it typically works:

1. **Key Exchange** : First, public key cryptography is used to securely exchange a symmetric key (private key) between the sender and receiver.
2. **Data Encryption** : Once both parties have the shared symmetric key, they use symmetric encryption (like AES) to encrypt the actual data because it's much faster.
3. **Secure Communication** : If the data needs to be transmitted, the symmetric key can be encrypted using the receiver's public key, ensuring that only they can decrypt it with their private key.

For example, in TLS/SSL (used in HTTPS):

- When you visit a website, your browser and the website's server exchange public keys and perform a handshake.
- They then use asymmetric encryption to exchange a symmetric session key.
- After that, they use the symmetric key for fast, secure encryption of your data.
- Public and Private Key in Action: Example with Digital Signatures

Digital Signatures provide a way to verify both the authenticity and integrity of a message. Here's how it works:

1. **Signing** :

- Alice wants to send a signed message to Bob.
- Alice takes the hash of the message (a fingerprint of the message).
- She encrypts the hash with her private key , creating the signature.
- Alice sends the original message along with the signature to Bob.

2. **Verification** :

Bob receives the message and the signature.
Bob computes the hash of the message he received.

Bob uses Alice's public key to decrypt the signature and retrieve the original hash.

- If the decrypted hash matches the one Bob computed, then he knows that the message hasn't been altered and that it came from Alice (since only Alice could have created the signature with her private key).

Key Differences Between Public and Private Key Cryptography

Feature	**Private Key (Symmetric)**	**Public Key (Asymmetric)**
Number of Keys	One key (shared between parties)	Two keys (public and private)
Encryption/Decryption	Same key used for both encryption and decryption	Different keys for encryption and decryption
Key Distribution	Must share the secret key securely	Public key can be shared openly
Speed	Faster (efficient for large data)	Slower (computationally more intensive)
Use Case	File encryption, VPNs, bulk data encryption	Secure communication, digital signatures, SSL/TLS
Example Algorithms	AES, DES, 3DES, RC4	RSA, DSA, ECC, ElGamal

Conclusion

- Private key cryptography is faster and more efficient but comes with the challenge of securely exchanging the secret key.
- Public key cryptography solves the key distribution problem and provides additional functionality like digital signatures but tends to be slower.
- Both types of cryptography often work together in modern systems to provide both security and efficiency.