Unit-1.0: Attacks on Computers and Computer Security & Cryptography Concepts

This unit lays the groundwork for understanding security threats and the fundamental concepts of cryptography.

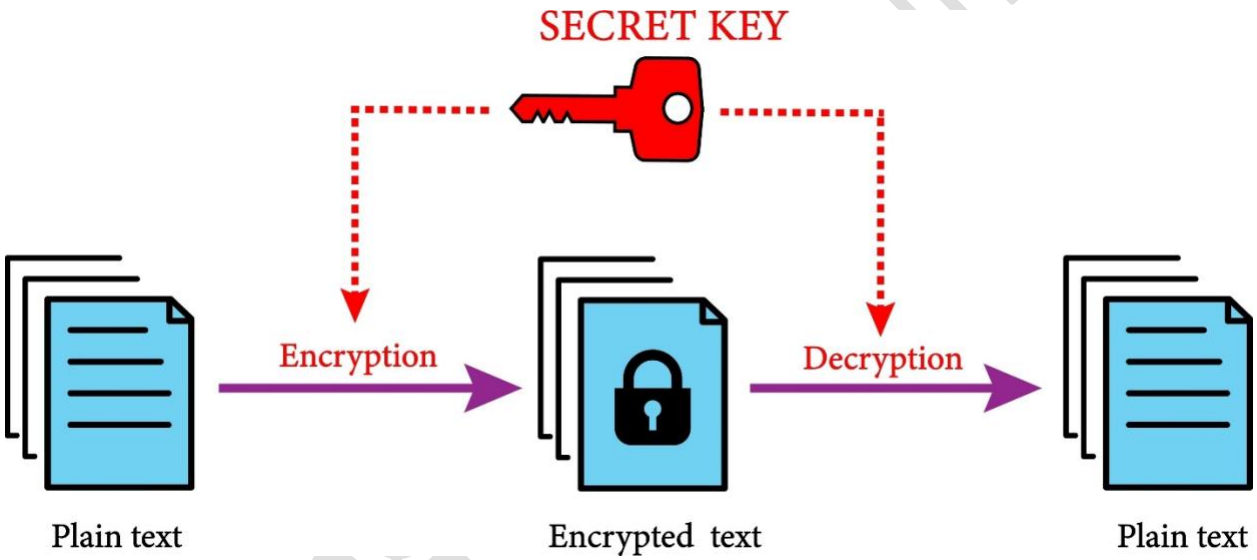
Attacks on Computers and Computer Security

- Introduction and The Need for Security: Computer security is necessary because information assets (data, systems, networks) are valuable and constantly under threat. The need stems from potential loss of Confidentiality, Integrity, and Availability (CIA Triad).
- Security Approaches: Involves strategies like prevention (stopping attacks before they happen), detection (identifying attacks in progress), and response (recovering from a successful attack).
- Principles of Security: The fundamental goals are the CIA Triad:
    - Confidentiality: Ensuring only authorized users can access information.
    - Integrity: Ensuring data is accurate and has not been tampered with.
    - Availability: Ensuring authorized users can access the information and systems when needed.
- Types of Security Attacks: Attacks can be passive (eavesdropping, traffic analysis) or active (modification, denial of service, spoofing, replay).
- Security Services: Services provided to counter attacks, such as authentication (verifying identity), access control (restricting resource access), data confidentiality, data integrity, and non-repudiation (proof of origin/delivery).
- Security Mechanisms: Methods used to provide security services, including encryption, digital signatures, hash functions, and access control lists.
- A Model for Network Security: A conceptual framework that outlines the steps for secure communication: the sender uses a security transformation (like encryption), sends the data over an insecure channel, and the receiver uses the inverse transformation (decryption).

Cryptography: Concepts and Techniques

- Plain text and Cipher text: Plain text is the original, readable message. Cipher text is the scrambled, unreadable message produced by an encryption algorithm.

- Substitution Techniques: Methods where each letter or group of letters in the plaintext is replaced by another letter or group of letters (e.g., Caesar Cipher).
- Transposition Techniques: Methods where the letters in the plaintext are rearranged or shuffled, but the actual letters remain the same (e.g., Rail Fence Cipher).
- Encryption and Decryption: Encryption is the process of converting plaintext to ciphertext using a key. Decryption is the reverse process, converting ciphertext back to plaintext using the key.
- Symmetric and Asymmetric Key Cryptography:
    - Symmetric (Secret) Key: Uses the same key for both encryption and decryption (e.g., AES). This is faster.



Shutterstock

Explore

* **Asymmetric (Public) Key:** Uses a **pair of keys**—a **public key** for encryption (known to everyone) and a **private key** for decryption (known only to the owner) (e.g., RSA). This is slower but solves the key distribution problem.

- Steganography: The art of concealing the existence of a message (e.g., hiding data inside an image file), unlike cryptography, which conceals the content.
- Key Range and Key Size: Key size refers to the number of bits in the key (e.g., 128-bit). A larger key size exponentially increases the key range (number of possible keys), making brute-force attacks computationally infeasible.

- Possible Types of Attacks (Cryptanalysis): Ciphertext-only (attacker only has ciphertext), Known-plaintext (attacker has some plaintext/ciphertext pairs), Chosen-plaintext (attacker can choose plaintext to be encrypted), Chosen-ciphertext (attacker can choose ciphertext to be decrypted).

Unit-2.0: Symmetric Key Ciphers

This unit focuses on the mechanisms and standards for symmetric encryption.

- Block Cipher principles & Algorithms (DES, AES):
    - Block Cipher: An encryption scheme that processes the plaintext input in fixed-size blocks (e.g., 64-bit or 128-bit) and produces a ciphertext block of the same size.
    - DES (Data Encryption Standard): An older, 64-bit block cipher using a 56-bit key. It is considered insecure today due to the small key size.
    - AES (Advanced Encryption Standard): The current standard, a 128-bit block cipher with key sizes of 128, 192, or 256 bits. It is based on the Rijndael algorithm.
- Block cipher modes of operation: Methods to encrypt sequences of data blocks securely and handle inputs longer than the block size. Common modes include:
    - ECB (Electronic Codebook): Simple but insecure, as identical plaintext blocks result in identical ciphertext blocks.
    - CBC (Cipher Block Chaining): Each ciphertext block is dependent on all preceding plaintext blocks, introducing chaining/randomness using an Initialization Vector (IV).
    - CTR (Counter): Turns a block cipher into a stream cipher, encrypting a counter instead of the actual data block.
- Stream Ciphers: Encrypt data one bit or one byte at a time, generating a key stream that is XORed with the plaintext. They are generally faster than block ciphers.
- RC4: A widely used, though now partially deprecated, stream cipher.
- Location and placement of encryption function: Where encryption is applied in a network, such as link encryption (at the data link layer, securing individual links) or end-

to-end encryption (at the application layer, securing communication between endpoints).

- Key distribution: The challenge of securely sharing the secret key between two parties in symmetric cryptography. Methods include physical delivery, key distribution centers, or using public-key cryptography to encrypt the symmetric key.

Unit-3.0: Asymmetric Key Ciphers

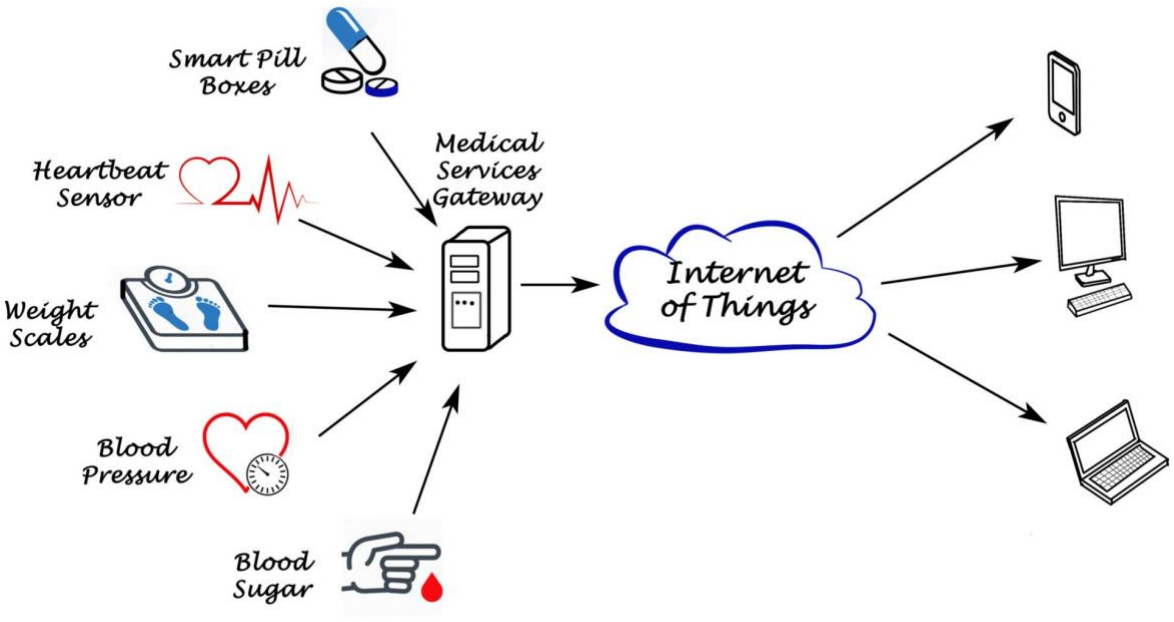
This unit explores public-key cryptography, which solves the key distribution problem.

- Principles of public key cryptosystems: Based on trapdoor one-way functions—functions that are easy to compute in one direction (encryption) but computationally infeasible to reverse (decryption) without a special piece of information (the private key).
- Algorithms (RSA, Diffie-Hellman):
    - RSA (Rivest–Shamir–Adleman): Used for both encryption/decryption and digital signatures. Its security relies on the difficulty of factoring large numbers.
    - Diffie-Hellman (DH) Key Exchange: Used *only* for securely establishing a shared symmetric key over an insecure channel. Its security relies on the difficulty of the discrete logarithm problem.
- Key Distribution (using Public Key): The public key system itself is often used to solve the symmetric key distribution problem. For example, Alice uses Bob's public key to encrypt a newly generated session key (a temporary symmetric key) and sends it to Bob, who decrypts it with his private key. They then use the fast symmetric key for the rest of the session.

Unit-4.0: Message Authentication Algorithms and Hash Functions

This unit focuses on ensuring data integrity and verifying identity.

- Authentication requirements: The need to verify that a message is genuine (originated from the alleged sender and has not been altered).
- Functions (for Authentication): These include Message Authentication Codes (MACs) and Hash Functions.
- Message authentication codes (MACs): A short block of data generated by a symmetric key function that depends on both the message and a secret key. The receiver re-calculates the MAC and verifies it matches the received MAC, assuring authenticity and integrity.
- Hash Functions: A mathematical function that converts an input (message) of any size into a fixed-size string of characters (called a hash value or message digest). Key properties:
    - One-way: Easy to compute the hash, but infeasible to reverse (find the original message from the hash).
    - Collision Resistance: Infeasible to find two different inputs that produce the same hash output.
- Secure hash algorithm (SHA): A family of widely used hash functions (e.g., SHA-256, SHA-3).
- Whirlpool: A cryptographic hash function designed by Vincent Rijmen and Paulo Barreto.
- HMAC (Hash-based Message Authentication Code): A mechanism for calculating a MAC involving a cryptographic hash function and a secret key. It adds key-dependent security to the standard hash function.
- Digital Signatures: The public-key equivalent of a handwritten signature. The sender uses their private key to encrypt the message's hash. The receiver uses the sender's public key to decrypt the hash and verify it against a locally computed hash of the message, proving authenticity, integrity, and non-repudiation.



Getty Images

Explore

- Authentication Applications:
    - Kerberos: A network authentication protocol that uses a Ticket Granting Server (TGS) and symmetric-key cryptography to verify user identities on a network.
    - X.509: A standard for Public Key Infrastructure (PKI) certificates, which digitally binds a public key to an identity (e.g., a person or organization).
    - Authentication Service: A general term for services that verify identity.
    - Public—Key Infrastructure (PKI): The system that manages and verifies digital certificates. It includes a Certificate Authority (CA) that issues and revokes certificates.
    - Biometric Authentication: Using unique biological characteristics (fingerprint, iris scan) to verify identity.

Unit-5.0: E-Mail Security & IP Security

This unit covers securing application-layer communication (email) and the network layer (IP).

E-Mail Security

- Pretty Good Privacy (PGP): A popular program that provides confidentiality (encryption) and authentication (digital signatures) for email and data storage, using a combination of symmetric and asymmetric cryptography.
- S/MIME (Secure/Multipurpose Internet Mail Extensions): The standard for encrypting and digitally signing email using PKI certificates.

IP Security (IPsec)

- IP Security overview: A suite of protocols used to secure IP communication at the network layer. It provides authentication, integrity, and confidentiality for data transmitted across IP networks.
- IP Security architecture: Defines the main components of IPsec, including the Authentication Header (AH) and Encapsulating Security Payload (ESP).
- Authentication Header (AH): Provides connectionless integrity and data origin authentication for IP packets (but no confidentiality).
- Encapsulating Security Payload (ESP): Provides confidentiality (encryption) and often also integrity and authentication.
- Combining security associations: Specifies how AH and ESP can be used together in different modes (Transport Mode for end-to-end, Tunnel Mode for VPNs).
- Key management: The process of creating, distributing, and destroying the security keys used by AH and ESP, typically handled by the Internet Key Exchange (IKE) protocol.

Unit-6.0: Web Security, Intruders, Virus and Firewalls & Case Studies

This unit covers securing the web, defending against malware, and network protection.

Web Security

- Web security considerations: Protecting web transactions from eavesdropping, modification, and denial of service.
- Secure Socket Layer (SSL) and Transport Layer Security (TLS): Cryptographic protocols used to secure communication over a computer network (e.g., HTTPS). TLS is the successor to SSL. They provide server authentication, data encryption, and integrity.
- Secure electronic transaction (SET): A protocol standard designed specifically for securing credit card transactions over the internet (though largely superseded by secure payment gateways using TLS/SSL).

Intruders, Virus and Firewalls

- Intruders: Individuals who attempt to gain unauthorized access to a computer system.
- Intrusion detection: Techniques and systems (IDS) used to monitor network or system activities for malicious or policy-violating events and alert on them.
- Password management: Secure practices for creating, storing, and using strong passwords.
- Virus and related threats: Malware that self-replicates and attaches to other programs (Virus), malware that appears benign but is destructive (Trojan Horse), and self-replicating independent programs (Worm).
- Countermeasures: Antivirus software, patches, system hardening, and user education.
- Firewall design principles: A firewall is a system that enforces an access control policy between two or more networks (often a private internal network and the public internet). Principles include blocking all traffic that isn't explicitly permitted.
- Types of firewalls:
    - Packet-Filtering: Inspects individual packet headers (basic, fast).
    - Stateful Inspection: Keeps track of the state of active connections (more secure than packet-filtering).
    - Application-Level Gateway (Proxy): Filters traffic based on application data (most secure, but slower).

Case Studies on Cryptography and Security

- Secure Inter-branch Payment Transactions: This would analyze how cryptographic protocols (like SSL/TLS, and digital signatures) are used to secure financial data transfer and non-repudiation between bank branches.
- Cross site Scripting (XSS) Vulnerability: An analysis of how attackers inject malicious scripts into trusted websites and the defensive measures (e.g., input validation, output encoding) needed to prevent it.
- Virtual Elections: Examining the security challenges and cryptographic solutions (e.g., homomorphic encryption, zero-knowledge proofs, digital signatures) required to ensure the integrity, confidentiality, and verifiability of electronic voting systems.

🔐 Advanced Encryption Standard (AES)

AES is the current standard for **symmetric-key block cipher** encryption, adopted by the U.S. government and used worldwide. It replaced the outdated DES algorithm.

Core Properties

- **Type:** Symmetric-key (uses the same key for encryption and decryption).
- **Algorithm:** Based on the **Rijndael** algorithm.
- **Block Size:** Always **128 bits** (16 bytes).
- **Key Sizes:** Can use **128, 192, or 256 bits**.
- **Structure:** It is a **substitution-permutation network (SPN)**, meaning it relies on a series of fixed substitutions and permutations (shuffling) rather than the Feistel structure used by DES.

The Round Structure

AES performs a specific number of transformation rounds depending on the key size: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

Each round (except the last one) involves four main transformations applied to the **State**, which is a 4×4 matrix holding the 128-bit data block:

1. **SubBytes (Substitution):**
    - This step provides **non-linearity** in the cipher.
    - Every byte in the State matrix is replaced with a corresponding byte value from a fixed lookup table called the **S-box (Substitution Box)**.
2. **ShiftRows (Permutation):**
    - This step provides **diffusion** (spreading the influence of one plaintext bit over many ciphertext bits).
    - The rows of the State matrix are cyclically shifted to the left by different offsets (Row 0 is shifted 0 bytes, Row 1 by 1 byte, Row 2 by 2 bytes, and Row 3 by 3 bytes).
3. **MixColumns (Diffusion):**
    - This step also provides **diffusion**, mixing the bits within columns.

- The bytes of each column are transformed using a mathematical operation based on multiplication in a finite field ($GF(2^8)$). This combines the four bytes in each column.
- *Note: This step is omitted in the final round.*

4. **AddRoundKey (XOR Operation):**
    - This step introduces the **key material** into the process.
    - The 128-bit round key (derived from the original secret key using a **Key Expansion** routine) is bitwise **XORed** with the current State matrix.

The iterative and complex nature of these four operations ensures that the resulting ciphertext is highly resistant to cryptanalysis.

🔑 Rivest–Shamir–Adleman (RSA) Algorithm

RSA is the fundamental algorithm for **asymmetric-key cryptography**, used primarily for **key exchange** and **digital signatures**.

Core Principles

- **Type:** Asymmetric-key (uses a public key for encryption and a private key for decryption/signing).
- **Security Basis:** Its security relies on the mathematical difficulty of **factoring the product of two large prime numbers**.

Key Generation Steps

A user (let's call her Alice) performs these steps to generate her key pair:

1. **Choose Two Large Primes (p and q):** These are kept secret.
2. Calculate n (Modulus):

$$n = p \times q$$

n becomes part of the public key.

3. Calculate $\phi(n)$ (Euler's Totient Function):

$$\phi(n) = (p-1) \times (q-1)$$

$\phi(n)$ is kept secret.

4. **Choose e (Public Exponent):**
    - Choose an integer e such that $1 < e < \phi(n)$.
    - e must be **coprime** to $\phi(n)$ (i.e., their greatest common divisor is 1: $\text{gcd}(e, \phi(n)) = 1$).
    - e becomes the other part of the public key.
5. **Calculate d (Private Exponent):**
    - Calculate d as the multiplicative inverse of e modulo $\phi(n)$.

$$d \cdot e \equiv 1 \pmod{\phi(n)}$$

    - This d is Alice's secret key.

- **Alice's Public Key:** (e, n)
- **Alice's Private Key:** (d, n)

Encryption and Decryption

Scenario: Bob wants to send a message (M) to Alice using her public key (e, n).

1. Encryption (by Bob)

Bob computes the ciphertext (C) using Alice's public key (e, n):

$$C = M^e \pmod{n}$$

2. Decryption (by Alice)

Alice computes the original message (M) from the ciphertext (C) using her private key (d, n):

$$M = C^d \pmod{n}$$

Digital Signature (Using RSA)

RSA can also be used for digital signatures to ensure **integrity** and **non-repudiation**.

- Signing: Alice uses her private key (d) to "decrypt" the hash (H) of her message (M).

$$\text{Signature } (S) = H(M)^d \pmod{n}$$

- Verification: Bob uses Alice's public key (e) to "encrypt" the signature (S) and compares the result to the hash he computes locally.

$$H' = S^e \pmod{n}$$

If $H' = H(M)$, the signature is valid.

The process of key generation and using the private key for signing and the public key for verification is fundamental to securing communications on the web.