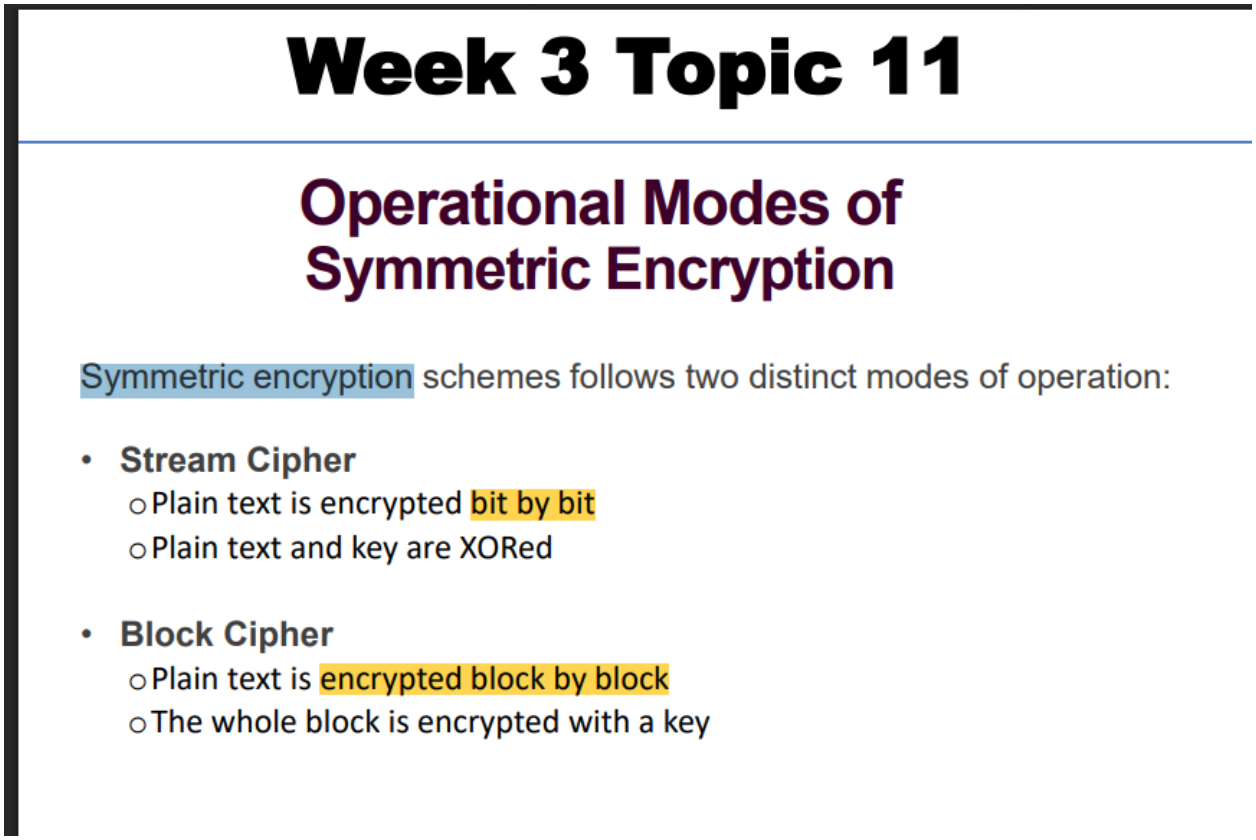
**By Maha Rana**

# CS627 Midterm Subjective Solved

**Short Questions:**

1. **What are the two modes of Symmetric Encryption?**
    - **Stream Cipher**: Encrypts plaintext bit by bit.
    - **Block Cipher**: Encrypts plaintext block by block.



## Week 3 Topic 11

### Operational Modes of Symmetric Encryption

Symmetric encryption schemes follows two distinct modes of operation:

- **Stream Cipher**
  - Plain text is encrypted bit by bit
  - Plain text and key are XORed
- **Block Cipher**
  - Plain text is encrypted block by block
  - The whole block is encrypted with a key

2. **Write down the CFE string for Microsoft Windows 2007?**

**By Maha Rana**

The **CFE string** (Common Platform Enumeration - CPE Formatted Entry) for **Microsoft Windows 2007** (likely referring to Windows 7) follows the standard CPE format used in cybersecurity tools like **Qualys, Nessus, and NIST's NVD (National Vulnerability Database).**

cpe:/o:microsoft:windows_7

**Breaking Down the CFE String:**

- `cpe:/o` → Represents an **operating system**
- `microsoft` → Vendor name
- `windows_7` → Product name

**Example for Specific Editions:**

- **Windows 7 Professional:**

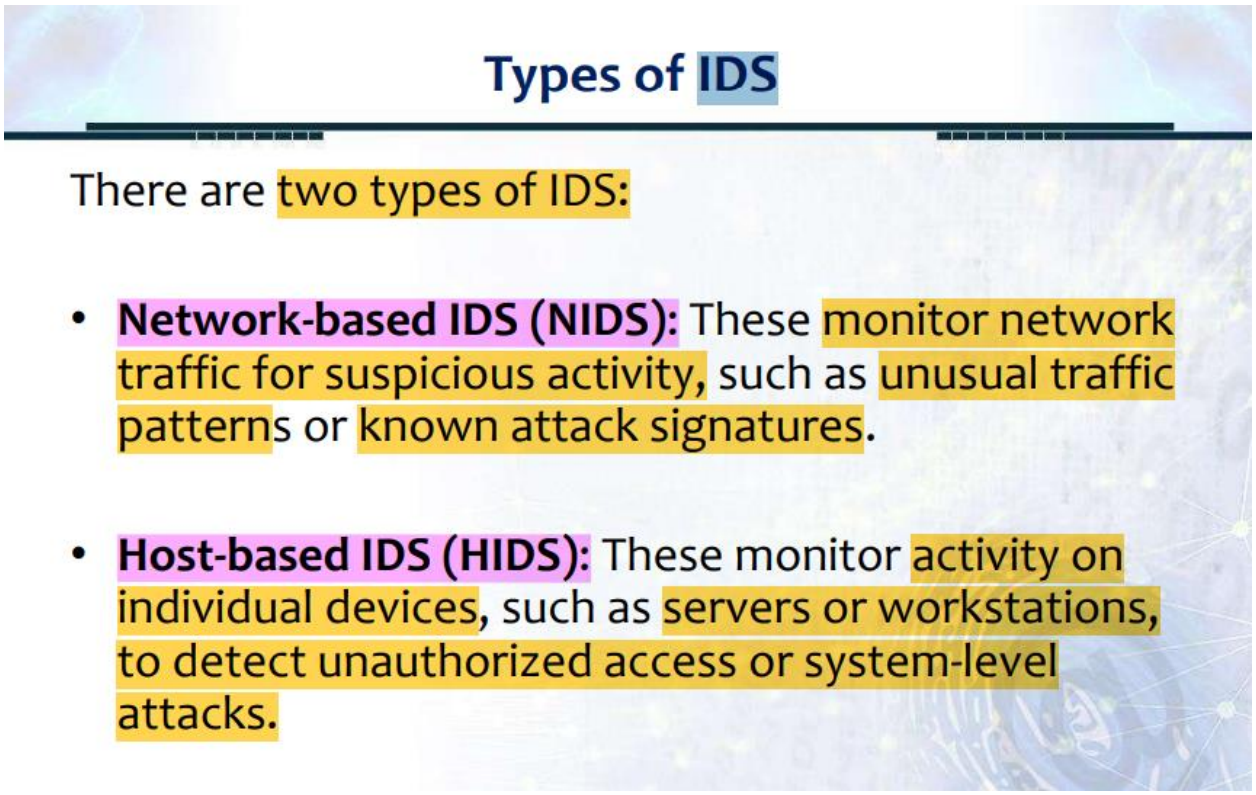
  `cpe:/o:microsoft:windows_7:professional`

- **Windows 7 Ultimate:**

  `cpe:/o:microsoft:windows_7:ultimate`

3. **What are the two types of IDS (Intrusion Detection Systems)?**
   - **Network-based IDS (NIDS)**: Monitors network traffic for suspicious activities.
   - **Host-based IDS (HIDS)**: Monitors activity on individual devices (hosts).

**By Maha Rana**




**Long Questions:**

1. **What are the challenges and vulnerability exploits? Write the names of two password vulnerabilities and how they can be exploited?**
    - **Challenges in Cybersecurity:**
        - Increasing complexity of systems.
        - Advanced persistent threats (APT).
        - Insider threats.
        - Lack of user awareness.
    - **Two Password Vulnerabilities & How They Are Exploited:**

1. **Brute Force Attack**: Attackers try all possible password combinations until they find the correct one.
2. **Rainbow Table Attack**: Attackers use precomputed hash values of common passwords to match against stolen password hashes.

**By Maha Rana**

**In the context of RSA, given that n = 143, e = 7, d = 103, how to encrypt when M = 30?**

**What are the two methods to save a password?**

**Plain Text Storage** *(not recommended as it is insecure).*

**Hashing with Salt** *(recommended to prevent attacks like Rainbow Table Attack).*

- **Encryption Formula:**

$$C = M^e \mod n$$

$$C = 30^7 \mod 143$$

- **Solution:**
  - Compute $30^7$ and take modulo 143.
  - This requires modular exponentiation, and the final result gives the ciphertext **C**.

**Short Questions:**

1. **Malware Examples**
   - Virus
   - Worm
   - Trojan Horse
   - Ransomware
   - Spyware
2. **AAA Authentication**
   - **AAA (Authentication, Authorization, and Accounting)** is a framework for controlling access to systems and resources.
     - **Authentication**: Verifies user identity.
     - **Authorization**: Grants permissions based on identity.

- **Accounting**: Tracks user activity for auditing.

3. **Difference Between Symmetric and Asymmetric Encryption**
   - **Symmetric Encryption:** Uses the same key for encryption and decryption (e.g., AES, DES).
   - **Asymmetric Encryption:** Uses a public key for encryption and a private key for decryption (e.g., RSA, Diffie-Hellman).

---

**Long Questions:**

1. **Types of Unique IDs**
   - **Username/Password**
   - **Biometric IDs (Fingerprint, Retina, Face Recognition)**
   - **Smart Cards & Tokens**
   - **One-Time Passwords (OTP)**
   - **RFID & NFC-based IDs**
2. **Diffie-Hellman Secret Key Calculation**

   Given:
   - Prime number PPP
   - Generator GGG
   - Private keys aaa and bbb

   Steps:

**By Maha Rana**

1. Both parties agree on a public prime $P$ and base $G$.
2. User-1 (Alice) selects a private key $a$ and computes:

$$A = G^a \mod P$$

3. User-2 (Bob) selects a private key $b$ and computes:

$$B = G^b \mod P$$

4. They exchange $A$ and $B$, then compute the shared secret key:

$$S = B^a \mod P = A^b \mod P$$

- This shared secret key $S$ is used for secure communication.

**Short Questions:**

1. **Two Password Storage Methods:**
   - **Plaintext Storage:** Storing passwords as they are (Not secure).
   - **Hashed Storage with Salt:** Storing password hashes with added randomness (Recommended).
2. **What is Vulnerability in Cybersecurity?**
   - A **vulnerability** is a weakness in a system, software, or network that can be exploited by attackers to gain unauthorized access or cause damage.
3. **Difference Between Asymmetric and Symmetric Encryption:**

| Feature | Symmetric Encryption | Asymmetric Encryption |
|---|---|---|
| Keys | Single key for encryption & decryption | Public key for encryption, private key for decryption |
| Speed | Faster | Slower |
| Examples | AES, DES | RSA, Diffie-Hellman |
| Use Case | Securing data at rest | Secure key exchange & digital signatures |

**By Maha Rana**

## Long Questions:

1. **Access Control Policies:**
    - **Mandatory Access Control (MAC):**
        - Access is determined by system-defined policies based on security labels and clearance levels.
        - Used in military and government systems.
    - **Discretionary Access Control (DAC):**
        - Access is determined by the owner of the resource.
        - Common in personal and small business systems.
    - **Role-Based Access Control (RBAC):**
        - Access is assigned based on organizational roles (e.g., Admin, User, Guest).
        - Used in corporate environments.
    - **Attribute-Based Access Control (ABAC):**
        - Access is based on attributes (e.g., time, location, user behavior).
        - Common in cloud-based environments.

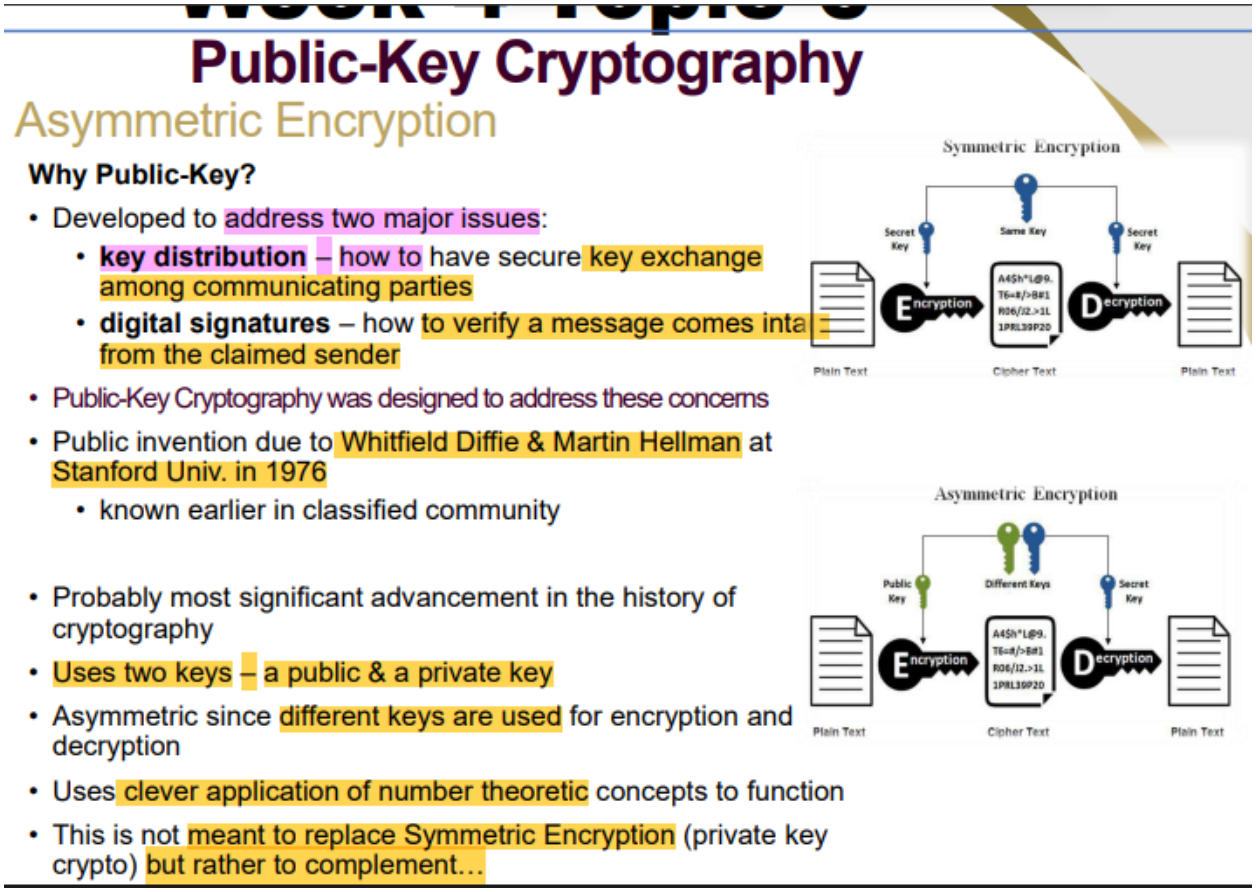


2. **Identify IDS (Intrusion Detection System) Types:**
    - **Network-based IDS (NIDS):** Monitors network traffic for suspicious activities.
    - **Host-based IDS (HIDS):** Monitors individual devices (hosts) for unusual behavior.
3. **Block Cipher - 5 Points or Attacks:**
    - **Block Ciphers:** Encrypt data in fixed-size blocks (e.g., 128-bit).
    - **Common Block Cipher Algorithms:** AES, DES, 3DES.
    - **Modes of Operation:** ECB, CBC, CFB, OFB, CTR.
    - **Key Size:** Larger key sizes provide better security.
    - **Attacks on Block Ciphers:**
        - **Brute Force Attack:** Trying all possible keys.
        - **Cryptanalysis Attacks:** Exploiting mathematical weaknesses in the cipher.
        - **Side-Channel Attacks:** Observing physical characteristics like power consumption.

**Short Questions:**

1. **What is Public Key in Cryptography?**
    - A **public key** is part of an asymmetric encryption system used to encrypt messages. It is shared publicly, while the corresponding **private key** is kept secret and used for decryption.

**By Maha Rana**




2. **Three Common Red Flags (for Identity Theft or Phishing Scams):**
    - **Unsolicited Calls or Emails** – Unexpected messages requesting personal information.
    - **High-Pressure Tactics** – Urgency or threats to force immediate action.
    - **Outdated Passwords** – Using weak or previously leaked passwords.
3. **Nessus Tool in Windows?**
    - **Nessus** is a vulnerability scanning tool used to identify security weaknesses in networks, operating systems, and applications. It helps organizations detect and fix vulnerabilities.
4. **What is a Digital Certificate?**

**By Maha Rana**

- A **Digital Certificate** is an electronic document that verifies the identity of a website, user, or device. It is issued by a **Certificate Authority (CA)** and includes a public key for secure communication.

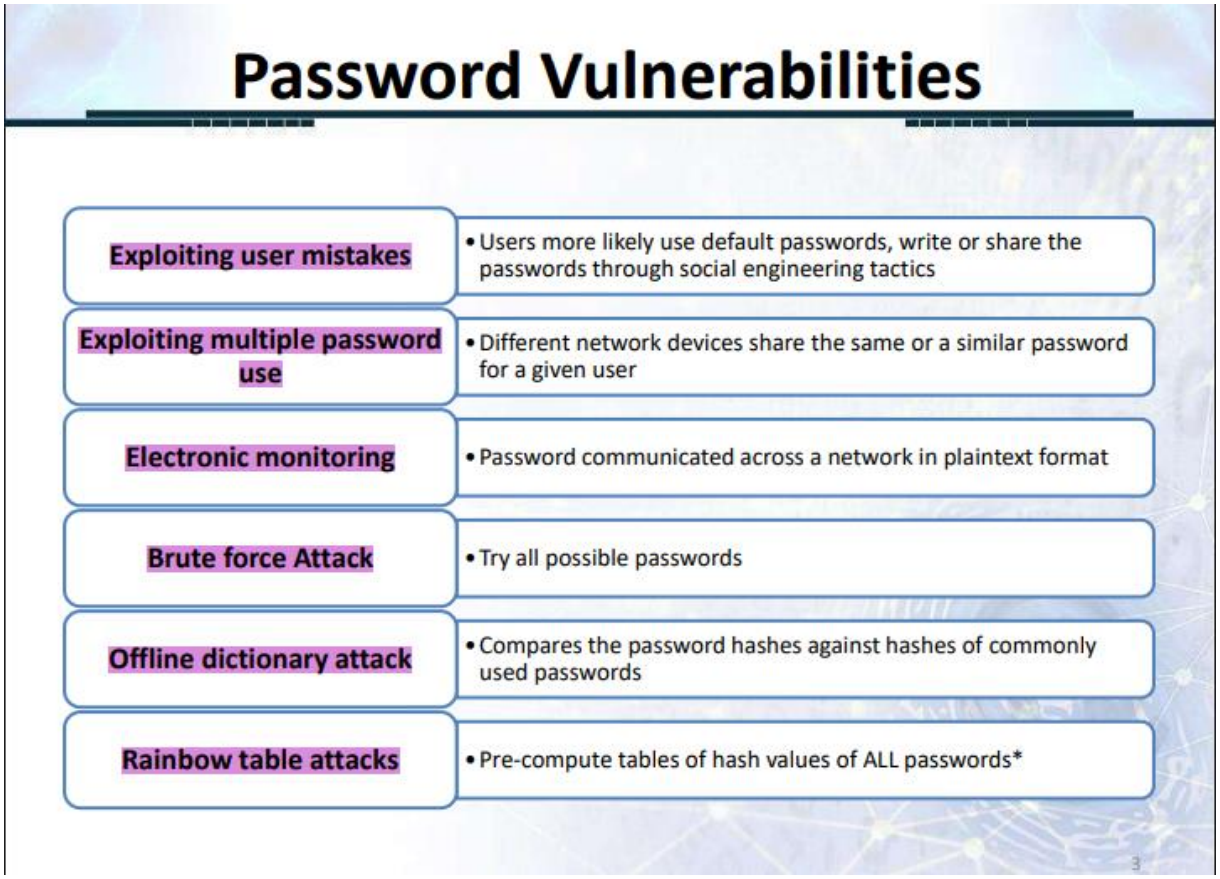
A Digital Certificate is **an electronic file that is tied to a cryptographic key pair and authenticates the identity of a website, individual, organization, user, device or server**. It is also known as a public key certificate or identity certificate.

https://www.boxentriq.com/code-breaking/hex-to-decimal-converter

---

## Long Questions:

1. **Write Password Vulnerabilities:**



2. **Convert "WELCOME" to Cipher Text with Key = 4 (Caesar Cipher Shift 4):**
    - **Caesar Cipher Formula:** $C=(P+4) \mod 26$ $C = (P + 4) \mod 26$ $C=(P+4) \mod 26$
    - **Plaintext:** `WELCOME`
    - **Shift by 4:**
        1. `W` → `A`
        2. `E` → `I`
        3. `L` → `P`
        4. `C` → `G`
        5. `O` → `S`
        6. `M` → `Q`
        7. `E` → `I`
    - **Ciphertext: AIPGSQI**
3. **IDS-Related 2 Options (Identifying IDS Type):**
    - **Network-based IDS (NIDS):** Monitors entire network traffic for suspicious activities.
    - **Host-based IDS (HIDS):** Monitors a specific device or system for unusual behavior.

---

**Short Questions:**

1. **Red Flags (for Phishing or Identity Theft)**
    - **Unsolicited Calls or Emails** – Unexpected requests for sensitive information.

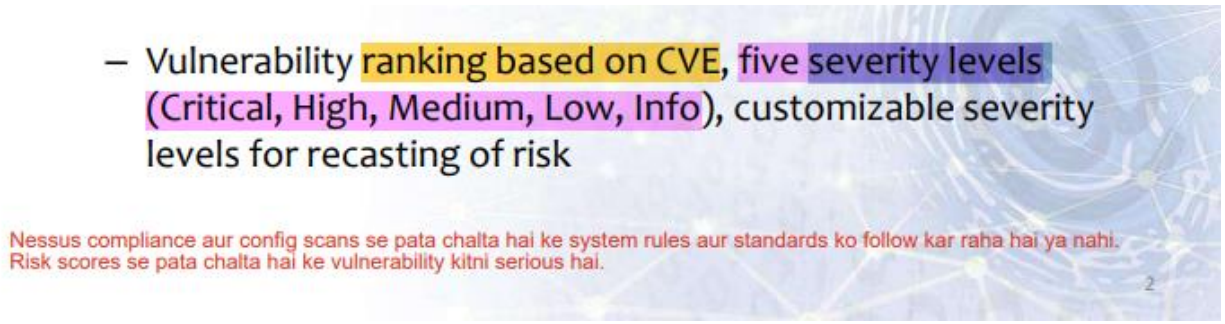
- **High-Pressure Tactics** – Messages creating urgency to take immediate action.
- **Outdated Passwords** – Using weak or previously exposed passwords.

2. **Nessus-Related Question**
   - **Nessus** is a **vulnerability scanning tool** used to detect security weaknesses in systems, applications, and networks.
   - It helps identify **misconfigurations, missing patches, and potential threats**.

**Long Questions:**

1. **Nessus Severity Levels (5 Levels)**
   - **Critical (10.0 - 9.0):** High-risk vulnerabilities that can be easily exploited (e.g., remote code execution).
   - **High (8.9 - 7.0):** Serious security flaws that attackers may exploit (e.g., SQL injection).
   - **Medium (6.9 - 4.0):** Moderate risks that may require user interaction to exploit (e.g., outdated software).
   - **Low (3.9 - 0.1):** Minor vulnerabilities with minimal impact (e.g., minor misconfigurations).
   - **Informational (0.0):** Non-security issues, like best practice recommendations.

**By Maha Rana**




2. **Find RSA Private Key (d) Given p, q, and e**

- Given:
  - $n = p \times q$
  - $e = 7$
  - Find $d$ such that:

$$d = e^{-1} \mod \phi(n)$$

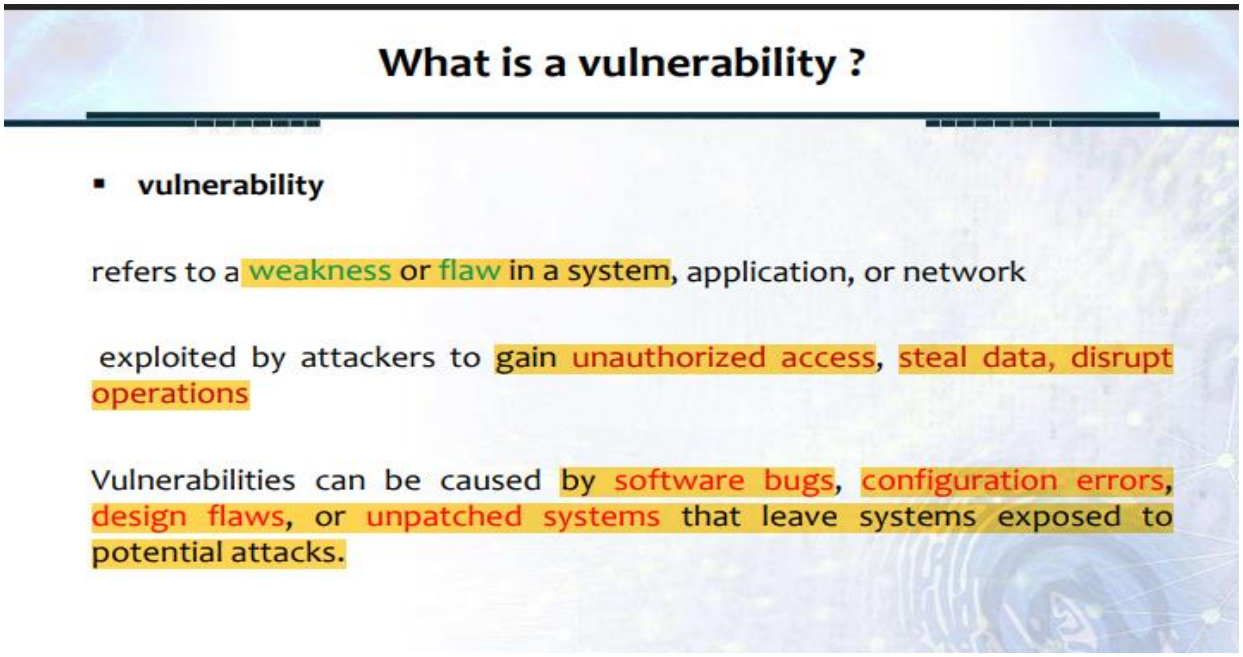
  - Where $\phi(n) = (p-1) \times (q-1)$.
  - Compute $d$ using **modular inverse**.

**Two Types of Vulnerabilities:**

**Not Exactly Found in your slides**

- **Software Vulnerabilities:** Flaws in applications (e.g., buffer overflow, SQL injection).
- **Network Vulnerabilities:** Weaknesses in network configurations (e.g., open ports, weak encryption).

**By Maha Rana**




**Short Questions:**

1. **Tools of Qualys:**
    - **Qualys Cloud Platform** – Centralized security & compliance solution.
    - **Qualys Vulnerability Management (VM)** – Scans and identifies system vulnerabilities.
    - **Qualys Web Application Scanning (WAS)** – Detects web-based threats and misconfigurations.
    - **Qualys Policy Compliance (PC)** – Ensures compliance with security policies.
    - **Qualys Malware Detection (MD)** – Detects malware in applications and websites.
2. **What is a Digital Certificate?**

- A **Digital Certificate** is an electronic document issued by a **Certificate Authority (CA)** that authenticates the identity of a website, individual, or organization.
- It includes a **public key** used for secure communication.
- Used in **SSL/TLS encryption** to secure internet transactions.

3. **Three Common Red Flags (for Phishing or Identity Theft):**
   - **Unsolicited Calls or Emails** – Unexpected messages requesting sensitive data.
   - **High-Pressure Tactics** – Urgent threats or rewards to manipulate users.
   - **Unusual Links or Attachments** – Suspicious URLs or files in emails.

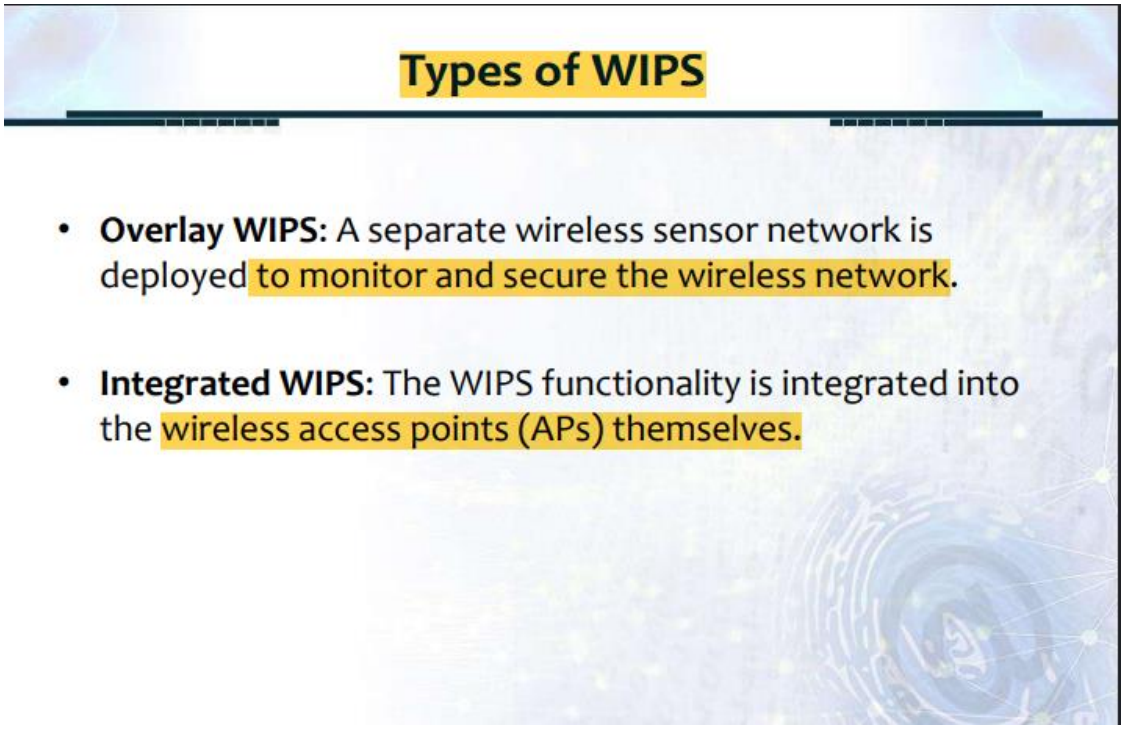
---

**Long Questions:**

1. **Confusion and Diffusion (Shannon's Principles for Cryptography):**
   - **Confusion:**
     - Makes the relationship between **plaintext, ciphertext, and the encryption key complex**.
     - Achieved using **substitution techniques** (e.g., S-boxes in AES).
     - **Goal:** Make it difficult for attackers to reverse-engineer the encryption.
   - **Diffusion:**
     - **Spreads plaintext influence over ciphertext** to obscure patterns.

- Achieved using **permutation/transposition** techniques.
- **Goal:** Minimize the effect of changing one bit of plaintext.

2. **Access Control Policies:**
   - **Mandatory Access Control (MAC):**
     - Access is controlled by security labels (e.g., military classification).
   - **Discretionary Access Control (DAC):**
     - Owners set access permissions (e.g., file sharing in Windows).
   - **Role-Based Access Control (RBAC):**
     - Access is based on organizational roles (e.g., Admin, User, Guest).
   - **Attribute-Based Access Control (ABAC):**
     - Access is determined by user attributes (e.g., location, device, behavior).
3. **Types of Wireless Intrusion Prevention Systems (WIPS):**



**By Maha Rana**

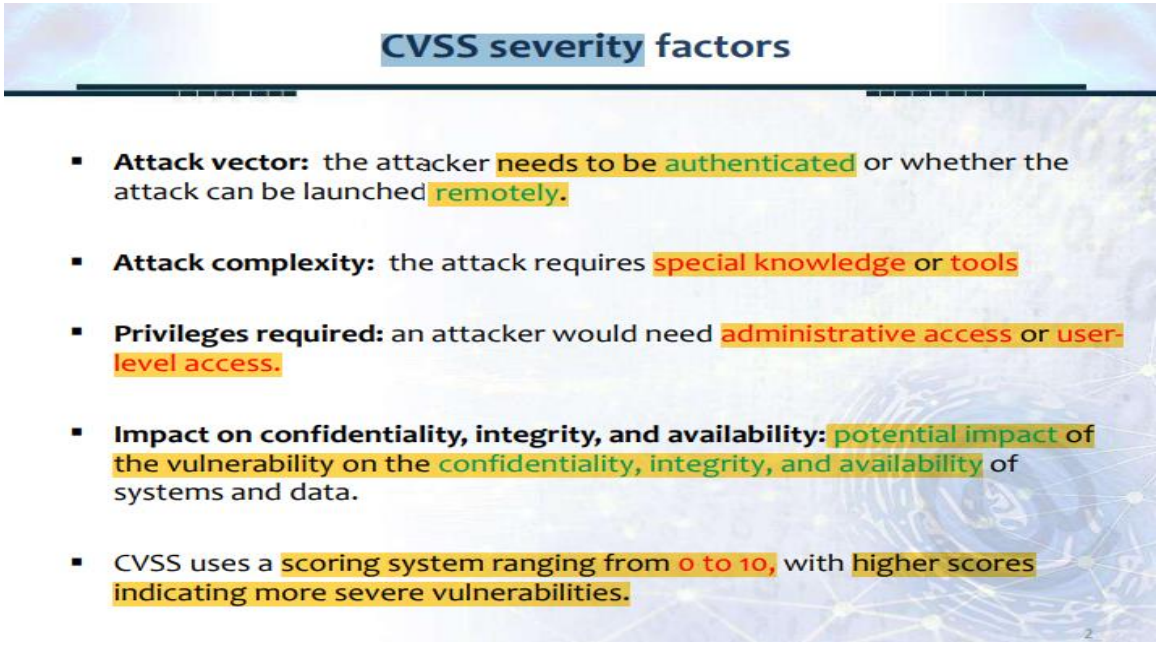
## Hellman's Formula Example:

Hellman's formula is primarily used in **Diffie-Hellman Key Exchange**, which is given by

$$S = B^a \mod P = A^b \mod P$$

- Example:
  - Let **P = 23, G = 5**
  - Alice chooses **a = 6** and Bob chooses **b = 15**
  - Alice computes: **$A = 5^6 \bmod 23 = 8$**
  - Bob computes: **$B = 5^{15} \bmod 23 = 19$**
  - Shared secret key: **$S = 19^6 \bmod 23 = 2$** (same for both parties)

1. **CVSS Severity Common Factors (Common Vulnerability Scoring System):**



2. **Password Vulnerabilities & Key Challenges:**
    - **Vulnerabilities:**
        1. **Brute Force Attack:** Trying all possible passwords.
        2. **Phishing Attack:** Tricking users into revealing passwords.
        3. **Rainbow Table Attack:** Using precomputed hash values to crack passwords.
    - **Key Challenges:**
        - Secure password storage (e.g., hashing with salt).
        - User habits (e.g., reusing passwords).
        - Managing forgotten passwords securely.

**3. Two Operational Modes of Symmetric Algorithms:**

**Stream Cipher:** Encrypts data bit-by-bit (e.g., RC4).

**Block Cipher:** Encrypts data in fixed-size blocks (e.g., AES, DES).

4. **Qualys Use for File and Folder Security:**

**Not Exactly Found in your slides**

**Qualys Policy Compliance (PC):** Ensures files & folders meet security policies.

**Qualys Vulnerability Management (VM):** Scans files/folders for security threats.

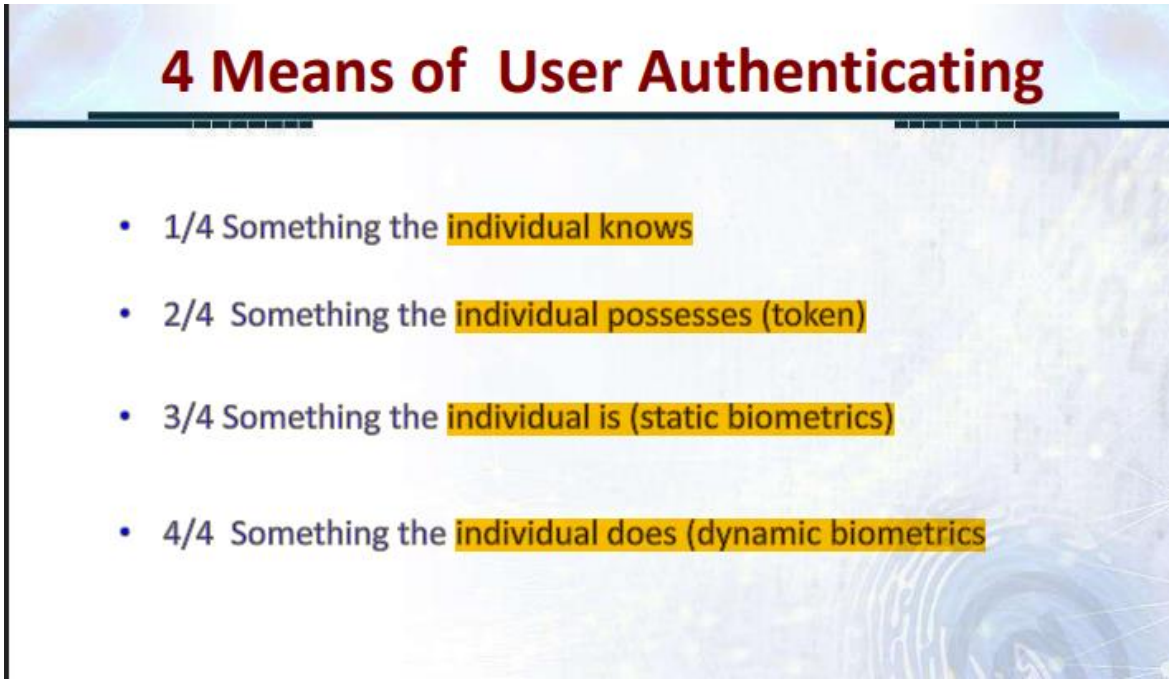
**Qualys File Integrity Monitoring (FIM):** Detects unauthorized changes in critical files.

**Short Questions:**

1. **Asymmetric vs. Symmetric Encryption:**

- **Symmetric Encryption:** Uses a single key for both encryption and decryption. Example: AES, DES.
- **Asymmetric Encryption:** Uses a public key for encryption and a private key for decryption. Example: RSA, Diffie-Hellman.

2. **Types of Cybersecurity Attacks:**
   - **Phishing Attack:** Trick users into revealing sensitive information.
   - **Malware Attack:** Using malicious software (e.g., viruses, ransomware).
   - **Denial of Service (DoS) Attack:** Overloading a network to disrupt services.
   - **Man-in-the-Middle (MitM) Attack:** Intercepting communication between two parties.
3. **Four Means of Authentication:**




4. **Difference Between Asymmetric and Symmetric Cryptography:**

**By Maha Rana**

| Feature | Symmetric Cryptography | Asymmetric Cryptography |
|---|---|---|
| Keys | Uses **one key** for encryption & decryption | Uses **two keys** (Public & Private) |
| Speed | Faster | Slower |
| Example | AES, DES, 3DES | RSA, Diffie-Hellman |
| Use Case | Securing data at rest | Secure key exchange & digital signatures |

## Spring 2025 Current Paper Provided by Mobeen ghuri

Cs627 current papers 2025:
Question 1: Three red flag
Three common red flags to watch
• Unsolicited calls or emails
• High-pressure tactics
• Outdated passwords

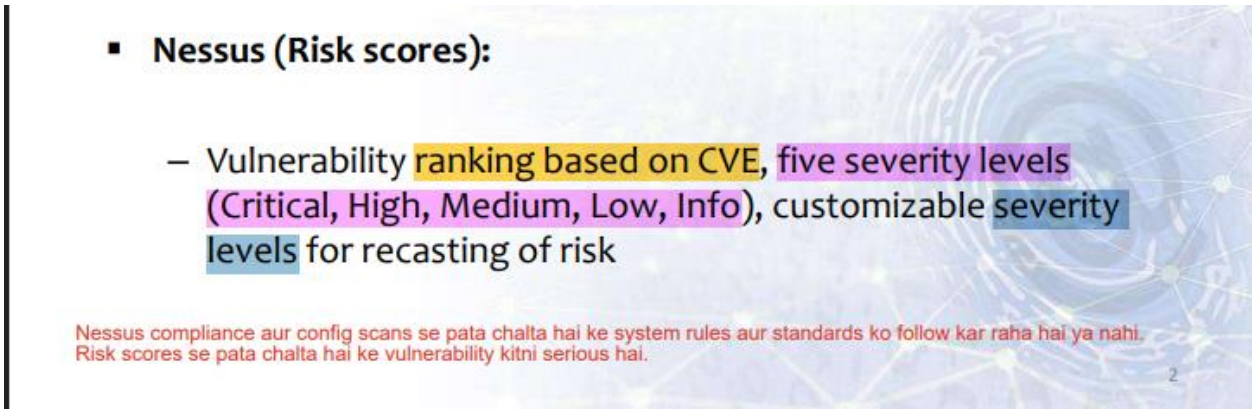
Question 2: Diff B/W Symmetric and Asymmetric
**Symmetric Encryption:**Uses the same key for encryption and decryption (e.g., AES, DES).
Need a strong encryption algorithm*
• Secure Key Exchange
• Its relatively fast

**Asymmetric Encryption:** Uses a public key for encryption and a private key for decryption (e.g., RSA, Diffie-Hellman
also knows as Public Key Cryptography
Public and private keys are mathematically related
• The private key is never shared
• Its relatively slow

Question 3: vigenere ciphers three steps?
**Three steps**
• Find the length of the key
• Divide the message into that many shift cipher encryptions.
• Use frequency analysis to solve the resulting shift ciphers.

Question 4: **Risk severity levels in the context of CVSS?**

**By Maha Rana**




Question 5: Two method of password storage?
Plain Text Storage (not recommended as it is insecure).
Hashing function (recommended to prevent attacks like Rainbow Table Attack).

Question 6: Full name of SCAP?
(Security Content Automation Protocol)

Question 7: Access control policies?
Mandatory access control (MAC)
• Discretionary access control (DAC)
• Role-based access control (RBAC)
• Attribute-based access control (ABAC)

Question 8: Features of Qualys?
Qualys:
– Cloud-based service
– On-premise device
–Complete suite
– Scalable and immediate deployment

Question 9: AAA ky name list krny thy?
Authentication, Authorization, and Accounting (AAA)

**Question 10:**confusion and diffusion?
Confusion refers to making the relationship between the Ciphertext and the Key as complex and involved as possible;
•Make use of Substitution
• Diffusion refers to dissipating the statistical structure of Plaintext over the bulk of Ciphertext

**By Maha Rana**

•Make use of Transposition

**Question 11**: IDS ke type given thi name likhny thy?
There are two types of IDS:
• Network-based IDS (NIDS): These monitor network traffic for suspicious activity, such as unusual traffic patterns or known attack signatures.
• Host-based IDS (HIDS): These monitor activity on individual devices, such as servers or workstations, to detect unauthorized access or system-level attacks.

Question 12:
What are the challenges and vulnerability exploits? Password?
Challenges in Cyber security:
- ♣ Increasing complexity of systems.
- ♣ Advanced persistent threats (APT).
- ♣ Insider threats.
- ♣ Lack of user awareness.

Two Password Vulnerabilities & How They Are Exploited:
1. Brute Force Attack: Attackers try all possible password combinations until they find the correct one.
2. Rainbow Table Attack: pre-compute table of hash values of all password

Question 13: Example given thi un mn sy identify Honeypot tool example?
KFSensor: A Windows-based honeypot that simulates vulnerable services and applications.
Honeyd: A customizable honeypot that can simulate multiple operating systems and services.
Cowrie: A high-interaction honeypot that simulates a full SSH environment.

Question 14: types of intrusion given thi name mention krny thy ?
There are different types of intrusions, including:
• External Intrusion: when an attacker attempts to gain access to a network from outside.
• Internal Intrusion: when an attacker gains access to a network from within, such as an employee with malicious intent.
• Insider Threat: when an employee or contractor intentionally or unintentionally causes harm to a network.
• Distributed Denial of Service (DDoS): when an attacker floods a network with traffic to disrupt normal operations.

**By Maha Rana**

Question 15: five names of block cipher mode of symmetric encryption?
Electronic Code Book (ECB) Mode • Cipher Block Chaining (CBC) Mode • Cipher Feedback Mode (CFB) • Output Feedback Mode (OFM) • Counter mode (CTR)
Question 16: Two operational modes of symmetric?
• Stream Cipher
oPlain text is encrypted bit by bit
oPlain text and key are XORed
• Block Cipher
oPlain text is encrypted block by block
oThe whole block is encrypted with a key

Question 17: types of wips identify krni thi  statement given thi ?

Overlay WIPS: A separate wireless sensor network is deployed to monitor and secure the wireless network. • Integrated WIPS: The WIPS functionality is integrated into the wireless access points (APs) themselves.

Question 18: What is Vulnerability in Cyber security?
A vulnerability is a weakness in a system, software, or network that can be exploited by attackers to gain unauthorized access or cause damage.

Question 19: Types of cyber security attack?
o Phishing Attack: Trick users into revealing sensitive information
o Malware Attack: Using malicious software
o Denial of Service (DoS) Attack: Overloading a network to disrupt services.
Brute force attacks
SQL Injection

**Question: 20**
DES AES ka table given tha jis mn parameters diya thy, key length, block size, internal working dono mn in parameters ko fill krna tha ?

| | DES | Triple DES | AES |
|---|---|---|---|
| Plaintext block size (bits) | 64 | 64 | 128 |
| Ciphertext block size (bits) | 64 | 64 | 128 |
| Key size (bits) | 56 | 112 or 168 | 128, 192, or 256 |

By Maha Rana

## Note

**May Allah grant you success, ease your efforts, and bless you with wisdom and perseverance. Keep your faith strong, for with prayer, every challenge becomes an opportunity. and please remember me in your prayers.**

**I hope this file helps you a lot, I have tried my best to find the most relevant and authenticated answers for the questions. However, in some cases, the questions might slightly differ from the ones in your slides. I recommend that every student kindly verify the answers on their own before using them. I am not responsible for any discrepancies.**

**Best wishes for Mids!**
**Maha ☺**