Here's a QnA set for your viva from beginner to advanced levels based on the provided keywords. I've also included some cipher-solving techniques and methods for solving RSA, Hill, and Playfair ciphers on pen and paper.

QnA for Viva Preparation

1. What is Public Key Encryption?

- Answer: Public key encryption uses two keys – a public key (shared openly) and a private key (kept secret). It ensures secure communication by encrypting data with the public key, which only the private key can decrypt.

2. What is Private Key Encryption?

- Answer: Private key encryption (or symmetric encryption) uses a single key for both encryption and decryption. Examples include AES and DES algorithms.

---

3. What is AES (Advanced Encryption Standard)?

- Answer: AES is a symmetric encryption algorithm that uses 128, 192, or 256-bit keys. It is widely used for secure data transmission.

- Related Question: How does AES differ from DES?

- Answer: AES has larger key sizes and is more secure than DES, which only uses a 56-bit key.

4. What is DES (Data Encryption Standard)?

- Answer: DES is a symmetric key encryption algorithm with a 56-bit key. Although once widely used, it is now considered insecure due to advances in computing power.

---

5. What is Ransomware?

- Answer: Ransomware is a type of malware that encrypts a victim's data and demands payment (a ransom) to decrypt it.

- Example: WannaCry ransomware.

6. What is a Trojan?

- Answer: A Trojan (or Trojan Horse) is malware disguised as legitimate software to trick users into installing it. Once inside, it can steal data, create backdoors, or install other malware.

---

7. What is a Virus?

- Answer: A computer virus is a malicious code that replicates by attaching itself to other files or programs. It can corrupt files, steal information, or slow down systems.

8. What is a Keylogger?

- Answer: A keylogger is a software or hardware tool that records keystrokes to steal sensitive information like passwords or credit card numbers.

---

9. What is Wireshark? How is it used?

- Answer: Wireshark is a network protocol analyzer used to capture and analyze network traffic in real-time. It helps in troubleshooting and security analysis.

---

10. What is a VPN (Virtual Private Network)?

- Answer: A VPN encrypts internet traffic and routes it through a secure server, providing privacy and security. It hides the user's IP address and bypasses geo-restrictions.

11. What is a Firewall? How does it work?

- Answer: A firewall is a network security device that monitors and filters incoming and outgoing traffic based on predetermined security rules.

Cipher-Solving Techniques (Pen and Paper)

Below are step-by-step methods to solve some classic ciphers:

---

1. RSA Algorithm

1. Select two prime numbers: $p = 3$ and $q = 11$.

2. Calculate $n = p \times q$:

   $n = 3 \times 11 = 33$.

3. Calculate $\phi(n) = (p - 1) \times (q - 1)$:

   $\phi(n) = 2 \times 10 = 20$.

4. Choose an integer e such that $1 < e < \phi(n)$ and e is coprime with $\phi(n)$. Let's choose $e = 7$.

5. Calculate the private key d such that:

   $(d \times e) \mod \phi(n) = 1$.

   Using extended Euclidean algorithm, $d = 3$.

6. Encryption:

   Cipher text $C = M^e \mod n$, where $M = 4$ (message).

   $C = 4^7 \mod 33 = 16$.

7. Decryption:

   Plain text $M = C^d \mod n$.

   $M = 16^3 \mod 33 = 4$.

---

2. Hill Cipher

1. Choose a Key Matrix:

\(K = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \).

2. Message (in pairs): "HI" → \(\begin{bmatrix} 7 \\ 8 \end{bmatrix} \) (H=7, I=8).

3. Encryption:

Multiply \(K \) with the message matrix:

\(C = K \times M = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \times \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 38 \\ 39 \end{bmatrix} \).

4. Reduce modulo 26:

\(C = \begin{bmatrix} 12 \\ 13 \end{bmatrix} \) → "MN".

---

3. Playfair Cipher

1. Create a 5x5 Key Matrix using a Keyword:

Keyword: "MONARCHY" (no repeating letters).

```
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
```

2. Encrypt the message "HELLO":

Split into digrams: HE LL O → HE LX LO ("X" added as filler).

3. Encryption rules:

- If letters are in the same row: Replace with the letter to their right.
- If in the same column: Replace with the letter below.
- Else, form a rectangle and swap corners.

4. Encrypt "HE": H → "O", E → "R".

Result: OR LX LO.

---

4. VPN and Firewall Related Questions

1. What is the difference between VPN and Proxy?

- Answer: A VPN encrypts all internet traffic, while a proxy only routes specific applications through a different IP.

2. What are the types of Firewalls?

- Answer: There are packet-filtering firewalls, stateful firewalls, and application-layer firewalls.

This QnA and cipher-solving guide covers both theoretical and practical aspects of your topics. Let me know if you need further explanations!

EXTRAAA

Public Key Cryptography

Public Key Cryptography, also known as asymmetric cryptography, uses two keys: a public key and a private key.

The public key is used for encryption and can be shared openly. Anyone can use it to encrypt a message.

The private key is used for decryption and must be kept secret. Only the owner of the private key can decrypt messages encrypted with their public key.

This method is widely used in secure communications, digital signatures, and SSL/TLS protocols (e.g., HTTPS).

2. Private Key Cryptography

Private Key Cryptography, also known as symmetric cryptography, uses a single key for both encryption and decryption.

The key must be kept secret and shared securely between parties.

It is generally faster than public key cryptography but requires a secure method to share the key.

Examples include algorithms like AES (Advanced Encryption Standard) and DES (Data Encryption Standard).

3. AES (Advanced Encryption Standard)

AES is a symmetric encryption algorithm that encrypts data in blocks of 128 bits.

It can use key sizes of 128, 192, or 256 bits.

AES is known for its security and efficiency and is used widely in applications like VPNs, secure file storage, and HTTPS encryption.

Due to its strength, AES is considered very secure and is used as the encryption standard by the US government.

4. DES (Data Encryption Standard)

DES is an older symmetric key encryption method that encrypts data in 64-bit blocks using a 56-bit key.

It was once a standard for encrypting sensitive data but is now considered insecure due to its short key length, making it vulnerable to brute-force attacks.

DES has been largely replaced by AES and other more secure algorithms.

5. Ransomware

Ransomware is a type of malicious software (malware) that encrypts a victim's files and demands a ransom to restore access.

It often spreads through phishing emails or exploit kits and can lock users out of their computers or specific files.

Well-known examples include WannaCry and Ryuk.

Users are advised not to pay the ransom as it does not guarantee data recovery and encourages further attacks.

6. Trojan

A Trojan Horse, or simply Trojan, is a type of malware that disguises itself as legitimate software or is hidden within legitimate software.

Once installed, it can perform malicious actions like stealing data, creating backdoors, or downloading additional malware.

Trojans often require the user to download and run the infected software, usually from suspicious links or attachments.

7. Virus

A virus is a type of malware that attaches itself to files or programs and spreads to other computers when these files or programs are shared.

It can damage data, corrupt systems, or allow attackers to gain control over a compromised system.

Unlike worms, which spread independently, viruses usually require user interaction to execute and propagate.

8. RSA (Rivest–Shamir–Adleman)

RSA is a widely used asymmetric encryption algorithm based on the factorization of large prime numbers.

It uses a pair of keys: a public key for encryption and a private key for decryption.

RSA is commonly used in digital signatures, SSL/TLS, and other secure data transmission methods.

The security of RSA relies on the difficulty of factoring large integers, which makes it suitable for secure data exchange.

9. Hill Cipher

The Hill Cipher is a symmetric encryption technique that uses linear algebra to encrypt data.

It encrypts messages by using matrix multiplication with a key matrix.

The plaintext message is broken into blocks, and each block is represented as a vector.

These vectors are multiplied with the key matrix to produce the encrypted message.

Decryption involves using the inverse of the key matrix to recover the original message.

10. Playfair Cipher

The Playfair Cipher is a manual symmetric encryption technique invented by Charles Wheatstone in 1854.

It encrypts digraphs (pairs of letters) instead of single letters.

A 5x5 matrix of letters is used as the key, created using a keyword.

Each pair of letters is encrypted according to rules based on their position in the matrix.

It is stronger than simple substitution ciphers because it uses pairs of letters, making frequency analysis attacks more challenging.

11. VPN (Virtual Private Network)

A VPN creates a secure and encrypted connection over a less secure network, such as the internet.

It masks the user's IP address and encrypts all internet traffic between the user’s device and the VPN server, providing privacy and security.

VPNs are commonly used to access geo-restricted content, protect sensitive data on public Wi-Fi, and maintain privacy from ISPs and websites.

12. Firewall

A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on security rules.

It can be hardware, software, or both.

Firewalls act as a barrier between a trusted network (like a corporate network) and untrusted networks (like the internet).

They help prevent unauthorized access, block certain types of traffic (e.g., known malware IPs), and provide a layer of protection for internal networks.