1. **What do you understand by Digital Privacy?**
2. **Explain Vulnerability.**
3. **What do you understand by Hacking?**
4. **Explain Wi-Fi eavesdropping?**
5. **What is MITM?**
6. **What is freenet?**
7. **What is Connection leak testing?**
8. **What is Electronic signature?**
9. **Which tools can be used for Disk Encryption?**
10. **What do you understand by Intellectual Property Rights?**
11. **What is mail bombing?**
12. **What is Biometric authentication?**
13. **What is Digital Forensic?**
14. **What is the use of VPN and how it secures your internet browsing?**
15. **What is the role and use of Windows BitLocker?**
16. **What are Copy Rights?**
17. **Name any four forensic tools.**
18. **Explain Firewall and Antivirus?**
19. **What are the various methods to secure your Social media IDs?**
20. **What is Malware?**
21. **What are different types of hackers? Explain in detail.**
22. **Name any two tools for wireless hacking.**
23. **What is a Honeypot?**
24. **What is Network Sniffing give two examples?**
25. **What is the difference between Phishing and Pharming?**
26. **What are the differences between Virus and Worms? Explain with explain.**
27. **What do you understand by Stalking on internet?**
28. **Explain Dictionary attacks? Explain different type of dictionary attacks in detail.**

A dictionary attack is a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an [encrypted](https://www.techtarget.com/searchsecurity/definition/encryption) message or document.

Dictionary attacks work because many computer users and businesses insist(Request) on using ordinary words as passwords. These attacks are usually unsuccessful against systems using multiple-word passwords and are also often unsuccessful against passwords made up of upper-case and lower-case letters and numbers in random combinations.

In systems with strong password requirements, the brute-force method of attack, in which every possible combination of characters and spaces is tested up to a certain maximum length, can sometimes be effective. However, a [brute-force attack](https://www.techtarget.com/searchsecurity/definition/brute-force-cracking) can take a long time to produce results.

Strong, randomized passwords cannot be easily predicted, and they are highly unlikely to be included in the predetermined password library. Because a dictionary attack's guess attempts are limited to a preselected list, it is essentially impossible to crack nonpredictable passwords.

A dictionary attack is a type of cyberattack in which an attacker systematically tries to guess passwords or encryption keys by using a predefined list of potential values, often derived from a dictionary or a set of known words. Here are different types of dictionary attacks:

1. \*\*Simple Dictionary Attack:\*\*

- \*Description:\* In a simple dictionary attack, the attacker uses a list of commonly used passwords or words from a dictionary to try and gain unauthorized access.

- \*Method:\* The attacker systematically goes through each word in the dictionary, trying them as passwords until the correct one is found.

- \*Countermeasures:\* Users are encouraged to use complex and unique passwords that are less likely to be found in standard dictionaries.

2. \*\*Brute-Force Dictionary Attack:\*\*

- \*Description:\* This type combines the dictionary attack with brute-force methods, where the attacker not only uses words from a dictionary but also systematically tries variations, such as adding numbers or special characters.

- \*Method:\* The attacker iterates through the dictionary and applies various modifications to each word, expanding the search space.

- \*Countermeasures:\* Strong password policies and multi-factor authentication can help mitigate the risk of brute-force attacks.

3. \*\*Hybrid Dictionary Attack:\*\*

- \*Description:\* This attack combines elements of both dictionary attacks and brute-force attacks. It involves using a dictionary of words along with variations, making it more potent than a simple dictionary attack.

- \*Method:\* The attacker combines words from the dictionary with common variations, such as appending numbers or symbols.

- \*Countermeasures:\* Employing strong password policies and regularly updating passwords can help reduce the risk of successful hybrid dictionary attacks.

4. \*\*Rainbow Table Attack:\*\*

- \*Description:\* In a rainbow table attack, precomputed hash values for all possible password combinations are stored in a table. The attacker then compares the hash of the target password against the precomputed values.

- \*Method:\* Instead of computing the hash on-the-fly, the attacker looks up the hash value in the rainbow table to find the corresponding password.

- \*Countermeasures:\* Salting passwords (adding random data to each password before hashing) can thwart rainbow table attacks by making precomputed tables impractical.

5. \*\*Credential Stuffing:\*\*

- \*Description:\* Credential stuffing involves using known username-password pairs obtained from previous data breaches and trying them on various online platforms.

- \*Method:\* Attackers take advantage of the fact that many users reuse passwords across multiple accounts.

- \*Countermeasures:\* Educating users about the risks of password reuse and implementing multi-factor authentication can help mitigate the impact of credential stuffing attacks.

It's crucial for individuals and organizations to be aware of these types of attacks and implement robust security measures to protect against unauthorized access. This includes using strong, unique passwords, regularly updating credentials, and incorporating additional security layers like multi-factor authentication.

1. **What are different types of Computer Security Risks? Discuss in detail.**

Computer security risks encompass a wide range of threats and vulnerabilities that can compromise the confidentiality, integrity, and availability of information stored and processed by computer systems. Here are different types of computer security risks, each with its own characteristics and potential consequences:

1. \*\*Malware:\*\*

- \*\*Definition:\*\* Malicious software (malware) includes viruses, worms, Trojans, ransomware, spyware, and other harmful programs designed to disrupt or damage computer systems.

- \*\*Characteristics:\*\* Malware can be distributed through infected software, email attachments, or compromised websites. Once inside a system, it can replicate, steal information, or render the system unusable.

2. \*\*Phishing Attacks:\*\*

- \*\*Definition:\*\* Phishing involves fraudulent attempts to obtain sensitive information such as usernames, passwords, and credit card details by posing as a trustworthy entity.

- \*\*Characteristics:\*\* Phishing attacks often come in the form of deceptive emails, messages, or websites that appear legitimate. Users are tricked into providing sensitive information, which can then be used for unauthorized access.

3. \*\*Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:\*\*

- \*\*Definition:\*\* DoS attacks flood a system, network, or service with excessive traffic to make it unavailable. DDoS attacks involve multiple sources coordinating the attack.

- \*\*Characteristics:\*\* These attacks overload servers or networks, causing slowdowns or complete outages. They can be used for extortion, revenge, or simply to disrupt operations.

4. \*\*Man-in-the-Middle (MitM) Attacks:\*\*

- \*\*Definition:\*\* MitM attacks involve intercepting and potentially altering communication between two parties without their knowledge.

- \*\*Characteristics:\*\* Attackers can eavesdrop on communication, capture sensitive data, or inject malicious content. Common examples include Wi-Fi eavesdropping and session hijacking.

5. \*\*SQL Injection:\*\*

- \*\*Definition:\*\* SQL injection involves inserting malicious SQL code into input fields to manipulate a database and gain unauthorized access or retrieve sensitive information.

- \*\*Characteristics:\*\* Vulnerable web applications can be exploited, allowing attackers to execute arbitrary SQL queries and potentially compromise the entire database.

6. \*\*Cross-Site Scripting (XSS):\*\*

- \*\*Definition:\*\* XSS attacks involve injecting malicious scripts into websites that are then viewed by other users.

- \*\*Characteristics:\*\* Attackers can steal session cookies, redirect users to malicious websites, or deface web pages. XSS is often used to exploit vulnerabilities in poorly secured websites.

7. \*\*Social Engineering:\*\*

- \*\*Definition:\*\* Social engineering relies on manipulating individuals to divulge confidential information or perform actions that may compromise security.

- \*\*Characteristics:\*\* Attackers use psychological tactics to exploit human behavior, often through impersonation, pretexting, or creating a sense of urgency to trick individuals into revealing sensitive information.

8. \*\*Zero-Day Exploits:\*\*

- \*\*Definition:\*\* Zero-day exploits target vulnerabilities in software or hardware that are unknown to the vendor and, therefore, unpatched.

- \*\*Characteristics:\*\* Attackers can take advantage of the time window between the discovery of a vulnerability and the release of a patch to compromise systems. Zero-day exploits are highly valuable in cybercriminal communities.

9. \*\*Insider Threats:\*\*

- \*\*Definition:\*\* Insider threats involve individuals within an organization who misuse their access and privileges to compromise security intentionally or unintentionally.

- \*\*Characteristics:\*\* Insiders may be employees, contractors, or business partners. They can leak sensitive information, intentionally or unintentionally introduce malware, or engage in other malicious activities.

10. \*\*Physical Security Threats:\*\*

- \*\*Definition:\*\* Physical security threats involve the risk of unauthorized access, theft, or damage to computer systems and infrastructure.

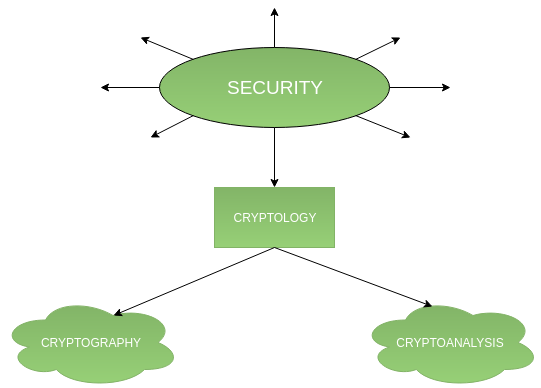
- \*\*Characteristics:\*\* These threats include theft of hardware, destruction of equipment, or unauthorized access to data centers. Physical security measures, such as access controls and surveillance, are essential to mitigate these risks.

To effectively address these computer security risks, organizations often implement a combination of technical solutions, policies, and user education programs to create a robust security posture. Regular updates, patches, and security audits are also crucial to stay ahead of emerging threats.

1. **What is DDoS?**
2. **Explain Vulnerability.**
3. **What is MITM?**
4. **What is plain text and cipher text in cryptography?**
5. **What is need of nodal authority in cyber security?**
6. **What is Malware?**
7. **Name any two tools for wireless hacking.**
8. **What is non-repudiation?**
9. **What is a Honeypot?**
10. **What is authentication?**
11. **What is symmetric key cryptography with one example?**
12. **What is Network Sniffing give two examples?**
13. **What is the role of social engineering?**
14. **What is threat management?**
15. **What is SQL Injection?**
16. **Explain the concept of cryptography by using diagrammatical approach**

Cryptography is an important aspect when we deal with network security. ‘Crypto’ means secret or hidden. Cryptography is the science of secret writing with the intention of keeping the data secret. Cryptanalysis, on the other hand, is the science or sometimes the art of breaking cryptosystems. Both terms are a subset of what is called **Cryptology.**

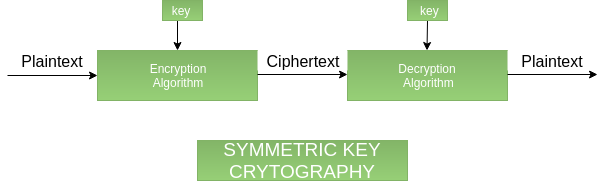
**Classification:** The flowchart depicts that cryptology is only one of the factors involved in securing networks. Cryptology refers to the study of codes, which involves both writing (cryptography) and solving (cryptanalysis) them. Below is a classification of the crypto terminologies and their various types.



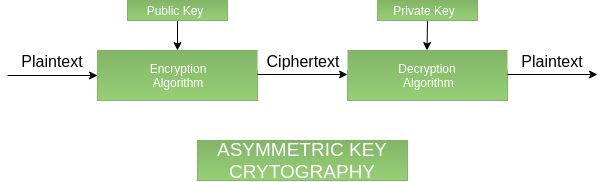
### Cryptography:

Cryptography is classified into symmetric cryptography and asymmetric cryptography. Below are the description of these types.

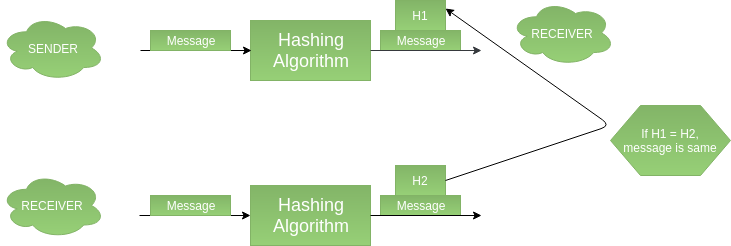
1. **Symmetric key cryptography –** It involves the usage of one secret key along with encryption and decryption algorithms which help in securing the contents of the message. The strength of symmetric key cryptography depends upon the number of key bits. It is relatively faster than asymmetric key cryptography. There arises a key distribution problem as the key has to be transferred from the sender to the receiver through a secure channel.



1. **Asymmetric key cryptography:** It is also known as public-key cryptography because it involves the usage of a public key along with the secret key. It solves the problem of key distribution as both parties use different keys for encryption/decryption. It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.



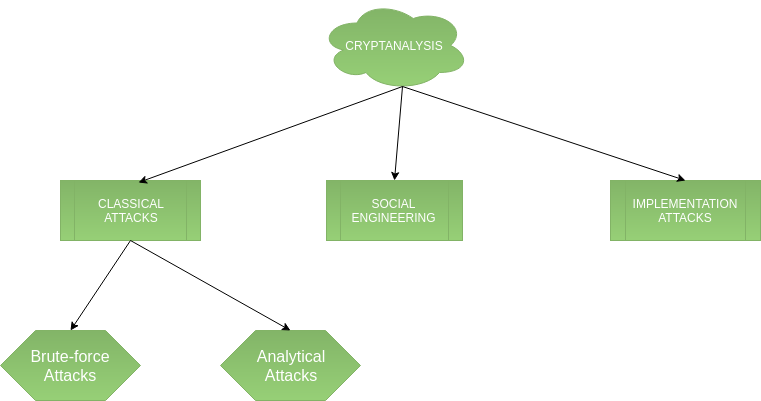
1. **Hashing:** It involves taking the plain text and converting it to a hash value of fixed size by a hash function. This process ensures the integrity of the message as the hash value on both, the sender’s and receiver’s sides should match if the message is unaltered.



### Difference between Hash functions, Symmetric, and Asymmetric algorithms:

| **Feature** | **Hash functions** | **Symmetric algorithms** | **Asymmetric algorithms** |
| --- | --- | --- | --- |
| **Number of Keys** | 0 | 1 | 2 |
| **Length of keys recommended by NIST** | 256 bits | 128 bits | 2048 bits |
| **Example** | SHA-256, SHA3-256, SHA-512 | AES or 3DES | RSA, DSA, ECC |

### Cryptanalysis:



1. **Classical attacks:** It can be divided into:  
   **a) Mathematical analysis:** It’s a type of attack that takes advantage of structural flaws in a specific algorithm.  
   **b) Brute-force attacks:** The attacker uses a Brute Force Attack (BFA) to try all potential keys in order to figure out the key. If the key is long, the attack will take a long time to execute. Brute-force attacks run the encryption algorithm for all possible cases of the keys until a match is found. The encryption algorithm is treated as a black box. Analytical attacks are those attacks that focus on breaking the cryptosystem by analyzing the internal structure of the encryption algorithm.
2. **Social Engineering attack:** It is something that is dependent on the human factor. Tricking someone to reveal their passwords to the attacker or allowing access to the restricted area comes under this attack. People should be cautious when revealing their passwords to any third party which is not trusted.
3. **Implementation attacks:** Implementation attacks such as side-channel analysis can be used to obtain a secret key. They are relevant in cases where the attacker can obtain physical access to the cryptosystem.

### Advantages:

1. **Precision:**Crypto-terminologies provide precise and well-defined terms and concepts that help to ensure a clear understanding of the underlying principles of cryptography.
2. **Standardization:** Crypto-terminologies help to standardize the language used in cryptography, which can help to reduce confusion and promote interoperability between different cryptographic systems.
3. **Clarity:**Crypto-terminologies help to promote clarity and accuracy in communication about cryptography, which can help to improve the effectiveness of security measures.
4. **Consistency:**Crypto-terminologies help to ensure consistency in the use of cryptographic concepts and techniques, which can help to reduce the risk of errors or misunderstandings.

### Disadvantages:

1. **Complexity:**Crypto-terminologies can be complex and difficult to understand, which can be a barrier to effective communication about cryptography.
2. **Jargon:**Crypto-terminologies can be viewed as jargon by those who are not familiar with the terminology, which can lead to confusion and miscommunication.
3. **Obfuscation:** Crypto-terminologies can be used to obfuscate the true nature of cryptographic techniques, which can be a concern in situations where transparency and openness are important.
4. **Accessibility:**Crypto-terminologies may be inaccessible to those who are not experts in the field, which can limit the ability of non-experts to understand and contribute to discussions about cryptography.
5. **Explain Firewall and working of Firewall?**
6. **Explain the different Threats to Information System?**
7. **Explain Foot printing and Reconnaissance?**

**Long Answer Type Questions:**

1. **What is a digital signature? Explain concept with appropriate diagram.**
2. **What is Steganography, explain steganalysis attacks with suitable example?**
3. **Explain the difference between Virus, Worms and Trojan?**
4. **What is Security Attack? Differentiate between Active and Passive Attack.**
5. **What are the main components of IOT infrastructure, explain what an embedded system on an IOT device is?**
6. **Explain Salami Attacks with example.**
7. **Write a short note on:-** 
   1. **Message Authentication.**
   2. **Virtual Private Network.**
   3. **Digital Signature Certificate.**
   4. **Cryptanalysis tools.**
8. **What is the difference between Authority and Authorization?**
9. **Explain secure file sharing with a suitable example?**
10. **What do you understand by Web browser privacy configuration? Discuss in detail.**
11. **Explain the difference between Encryption and Cryptography with suitable examples.**
12. **Explain various Law Enforcement roles and responses?**
13. **Discuss the difference between Digital Signature and Electronic Signature?**
14. **Discuss multitask encryption tools in detail.**
15. **‘Cyber Space is a consensual hallucination’. What is the role of law in such world?**
16. **What is the difference between Hacking and Cracking?**
17. **Explain the various steps in detail for Evidence Preservation.**
18. **What is Cloud Forensics and Network forensics? Explain in detail with examples.**
19. **Write a short note on: -**
    1. **Mobile Forensics.**
    2. **Software forensic.**
    3. **Chain of Custody.**
    4. **Wi-Fi cracking tools.**
20. **What do you understand by Sniffing? Explain different types of Sniffing.**
21. **What all information an attacker can obtain through Foot-printing and how?**
22. **What is DNS Poisoning? Explain in detail about the defense with examples.**
23. **Explain various Social Engineering attacks and how to avoid them?**
24. **What is Cross-Site Scripting? Explain in detail with examples.**
25. **Write a short note on: -**
    1. **DDoS Attack.**
    2. **SQL Injection.**
    3. **Botnet.**
    4. **Penetration testing.**