1. Write a program for default passwords, printed passwords and password in plain text form. Draw flowchart, algorithm and attach output results for the same.

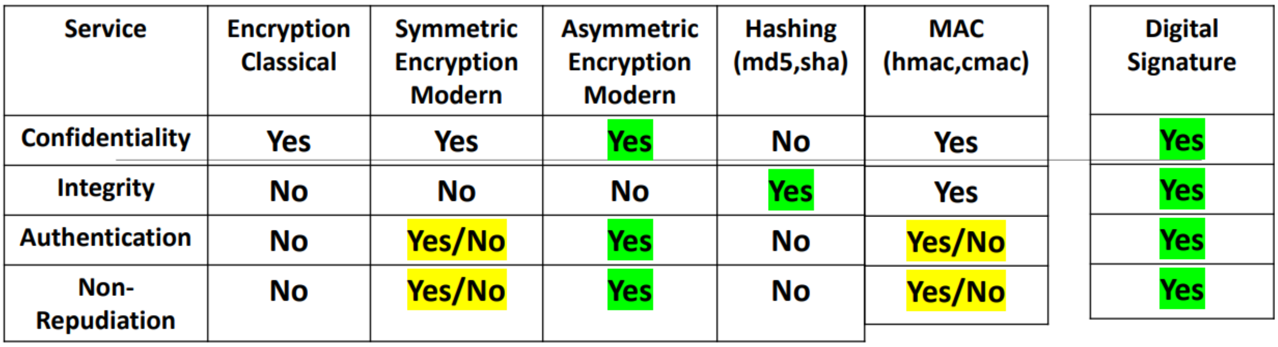
2. Explain RSA algorithm in detail with example.
   ANS (Pg 3-47,3-52)

3. Explain any two of following with example
   i. Playfair Cipher
   ii. Hill Cipher
   iii. Vigenère cipher
   iv. One-Time Pad cipher
   v. Monoalphabetic cipher

   ANS (Pg 2-3,2-15)

4. Compare in Tabular fashion, Confidentiality, Integrity, Authentication and Non repudiation for following security techniques
   a. Classical Encryption/Decryption
   b. Symmetric Encryption
   c. Asymmetric Encryption
   d. Hashing Technique
   e. MAC technique
   f. Digital Signature System

   ANS



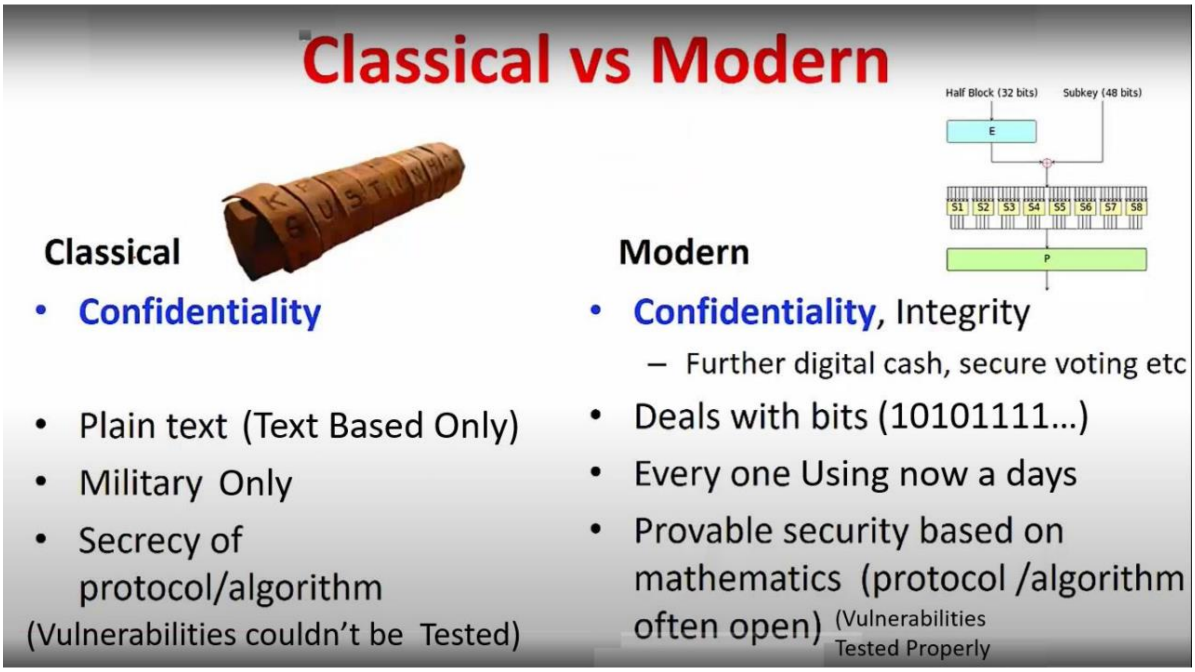
Service	Encryption Classical	Symmetric Encryption Modern	Asymmetric Encryption Modern	Hashing (md5,sha)	MAC (hmac,cmac)	Digital Signature
Confidentiality	Yes	Yes	Yes	No	Yes	Yes
Integrity	No	No	No	Yes	Yes	Yes
Authentication	No	Yes/No	Yes	No	Yes/No	Yes
Non-Repudiation	No	Yes/No	Yes	No	Yes/No	Yes

5. Draw and explain DES algorithm in detail.

   ANS.
   https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/

6. Compare classical Vs Modern Cryptography.

   ANS



Classical vs Modern

Classical

- Confidentiality
- Plain text (Text Based Only)
- Military Only
- Secrecy of protocol/algorithm

(Vulnerabilities couldn't be Tested)

Modern

- Confidentiality, Integrity
  - Further digital cash, secure voting etc
- Deals with bits (10101111...)
- Every one Using now a days
- Provable security based on mathematics (protocol /algorithm often open) (Vulnerabilities Tested Properly

7. What is DoS attack? What is DDoS attack? How to Mitigate it?
   ANS.
   https://www.geeksforgeeks.org/difference-between-dos-and-ddos-attack/
   https://developer.okta.com/books/api-security/dos/how/

8. Write a program of encryption and decryption for transposition cipher. Draw flowchart, algorithm and attach output results for the same.

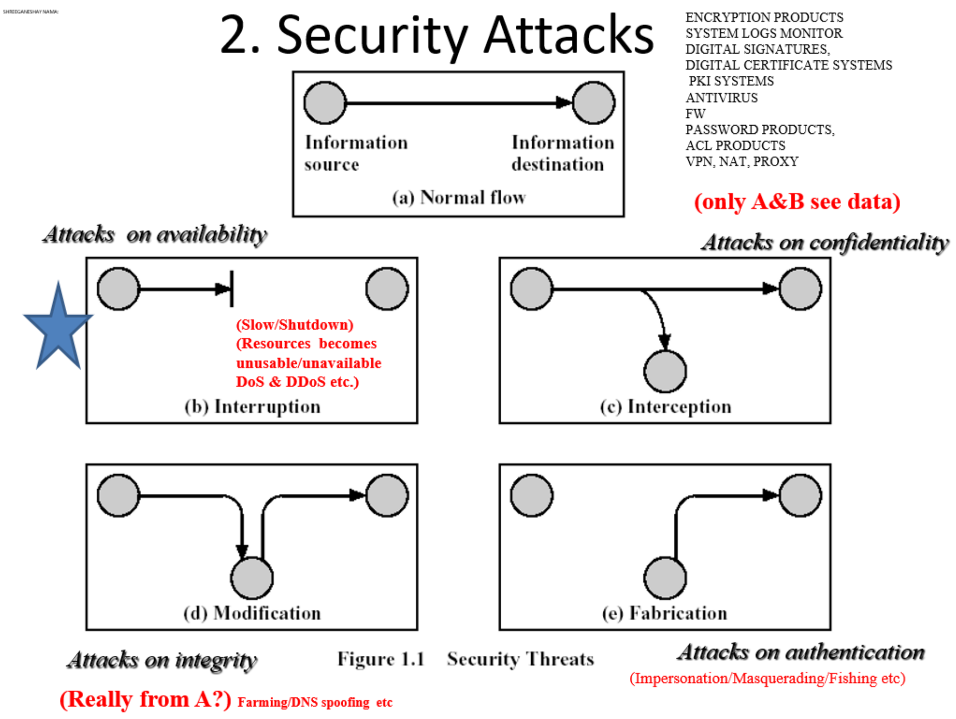
9. Use key
   a. MEGABUCK, or
   b. PICTENTG, or
   c. NBAISOKR

   d. for message: please transfer one million dollars to my swiss bank account six two two four

10. Explain C, I, A, Authentication and Non-Repudiation.
    ANS. Pg(1-4,1-5,1-11,1-13)

11. Explain the Interruption, Interception, Modification and Fabrication attack. Correlatethe said attacks with C,I,A, Authentication and Non-Repudiation.

ANS. Pg(1-8,1-9,1-10)



SHREEGANESHAY NAMA:

2. Security Attacks

ENCRYPTION PRODUCTS
SYSTEM LOGS MONITOR
DIGITAL SIGNATURES,
DIGITAL CERTIFICATE SYSTEMS
PKI SYSTEMS
ANTIVIRUS
FW
PASSWORD PRODUCTS,
ACL PRODUCTS
VPN, NAT, PROXY

(only A&B see data)

Figure 1.1 Security Threats

(Really from A?) Farming/DNS spoofing etc

(Impersonation/Masquerading/Fishing etc)

12. Write a program of encryption and decryption for Substitution Cipher-Caesar Cipher. Draw flowchart, algorithm and attach output results for the same.

13. Use key

    a. 3, or

    b. 5, or

    c. 7

    d. for message: please transfer one million dollars to my swiss bank account six two two four

21. Demonstrate installation and configuration of mobile Security app. Explain the different features and record the different working snapshots for the same.

22. What is WEP and WAP security techniques? Explain the details.
ANS.
https://www.geeksforgeeks.org/difference-between-wep-and-wpa/

23. What are the different wireless components used for Wi-Fi, Bluetooth Communications?

ANS

1. Transceiver: The transceiver is a device that combines both transmitter and receiver functions. It converts data into radio signals for transmission and receives radio signals and converts them back into data.
2. Antenna: An antenna is used to transmit and receive electromagnetic waves. It helps in transmitting and receiving signals effectively by improving signal strength and coverage.
3. Radio Frequency (RF) Module: The RF module contains the circuitry required to transmit and receive RF signals. It includes components such as amplifiers, filters, and frequency synthesizers.
4. Baseband Processor: The baseband processor handles the digital processing of signals. It takes care of tasks such as modulation, demodulation, error correction, and data encoding/decoding.
5. Power Amplifier: The power amplifier boosts the signal strength before transmitting it through the antenna. It ensures that the signal is strong enough to reach the intended destination.
6. Bluetooth Specific Components: In addition to the above components, Bluetooth communication requires specific components like a Bluetooth controller and a Bluetooth stack. The Bluetooth controller manages the Bluetooth protocol, while the stack handles the software implementation of the Bluetooth protocol.
7. Wi-Fi Specific Components: Wi-Fi communication utilizes components such as Wi-Fi chipset, Wi-Fi radio, and Wi-Fi modem. These components are responsible for implementing the Wi-Fi protocol and enabling wireless connectivity.

24. Write details about ISM band frequencies, BT standards & Wi-Fi standards.

ANS

ISM Band Frequencies:

The Industrial, Scientific, and Medical (ISM) bands are frequency ranges allocated for unlicensed use in various countries worldwide. These bands allow for the operation of a wide range of wireless devices and technologies. The most commonly used ISM band frequencies are:

1. 2.4 GHz ISM Band: This band is widely used for various wireless technologies, including Wi-Fi, Bluetooth.
2. 5.8 GHz ISM Band: This band is less congested compared to the 2.4 GHz band and is used for higher-speed wireless technologies such as Wi-Fi 5 (802.11ac) and Wi-Fi 6 (802.11ax).

BT Standards (Bluetooth):

1. Bluetooth 1.x: The initial Bluetooth standard, offering basic data transmission and voice communication capabilities.
2. Bluetooth 2.x: Introduced Enhanced Data Rate (EDR), enabling faster data transfer rates and improved power control.
3. Bluetooth 3.0 + HS: This version introduced High-Speed (HS) capability, utilizing Wi-Fi technology for faster data transfer between devices.
4. Bluetooth 4.x: Featured Low Energy (LE) or Bluetooth Smart, designed for low-power applications like wearables, fitness devices, and sensors.
5. Bluetooth 5.x: Introduced longer range, higher data transfer rates, and improved connection stability. It also added support for Bluetooth mesh networking.

Wi-Fi Standards:
Some of the significant Wi-Fi standards include:

1. Wi-Fi 1 (802.11b): Maximum data transfer rate of 11 Mbps using the 2.4 GHz band.

2. Wi-Fi 2 (802.11a/g): These standards brought faster data rates of up to 54 Mbps using the 5 GHz band (802.11a) and the 2.4 GHz band (802.11g).

3. Wi-Fi 3 (802.11n): Introduced in 2009, it offered increased data rates, improved range, and better reliability. It supported both the 2.4 GHz and 5 GHz bands.

4. Wi-Fi 4 (802.11ac): Introduced in 2013, it brought significant speed improvements and supported the 5 GHz band. It offered multi-user MIMO (MU-MIMO) technology and better performance in crowded environments.

5. Wi-Fi 5 (802.11ac): This version further improved speed, capacity, and overall performance compared to Wi-Fi 4. It introduced features like beamforming and wider channels.

6. Wi-Fi 6 (802.11ax): Released in 2019, Wi-Fi 6 provides faster speeds, reduced latency, improved efficiency, and better performance in crowded areas. It introduced OFDMA and other advanced features.

7. Wi-Fi 6E (802.11ax): This extension of Wi-Fi 6 operates in the 6 GHz frequency band, offering additional spectrum for improved performance and reduced congestion.

25. Compare symmetric and asymmetric key cryptography. (Min 8 Points).

    ANS. Pg (2-22)

26. Explain Transport and tunnel mode in IPSec.

    ANS. Pg (5-33)

27. Demonstrate installation and configuration of Steganography technique in view of network security. Explain the different features and record the different working snapshots for the same.

28. Draw and explain the block diagram of Steganography for Image as data.

    ANS. Pg(2-24)

29. Compare Steganography versus Cryptography.

    ANS. Pg(2-26)

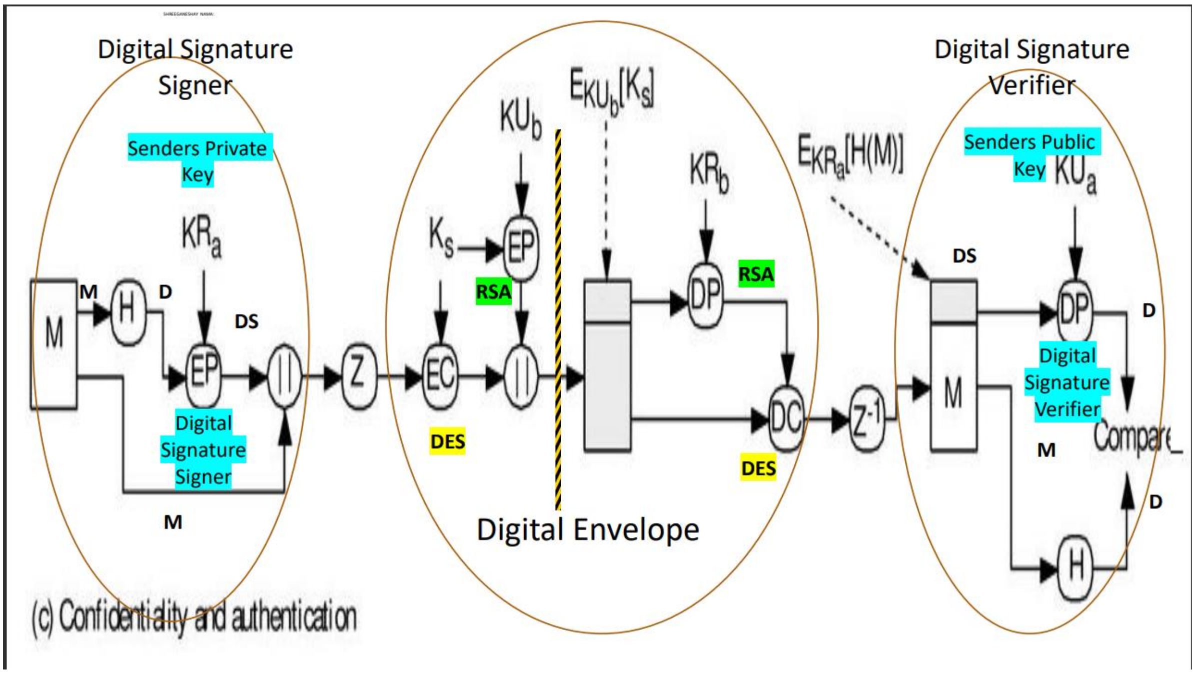
34. Draw and explain the following block diagrams

    a. Digital Signature system.

       ANS. https://www.geeksforgeeks.org/digital-signatures-certificates/

    b. End to End Email Communication system with Hashing, Digital signature and Digital Envelope processing blocks.

ANS.



35. Install and configure firewall for Host security. Explain the different features and record the different working snapshots for the same.

36. Draw and explain following. A)Packet filtering firewall **Pg(6-34,6-35)** B)Application Layer Firewall **Pg(6-38,6-39)**

    C) Circuit Level Gateway firewall **Pg(6-39)**

37. Compare Firewall Versus Antivirus.

    ANS. https://www.geeksforgeeks.org/difference-between-firewall-and-antivirus/

38. Compare IDS and IPS in detail.

    ANS. Pg(6-25)

42. Demonstrate process to ensure Security of web browser (Google Chrome) with respect to A) Cookies settings B) Website Blocking C) Phrase/Word blocking. Explain the different features and record the different working snapshots for the same.

43. What are different types of cookies?
    ANS.

    Types of Cookies
    Cookies are divided based on their attributes, such as source, duration, and purpose.

    Cookies Based on Source

    First-party cookies − The user's browser sets first-party cookies when they visit a website. The information gathered by first-party cookies is used to calculate page views, sessions, and the number of users. Ad agencies and advertisers primarily utilize it to locate potential ad targets.

    Third-party cookies − These are set by domains that the user does not visit directly. This occurs when publishers include third-party elements on their website (such as a chatbot, social plugins, or advertisements).

    Cookies Based on Duration

    Session cookie − A session cookie is a file that a website server delivers to a browser with an identification (a string of letters and numbers) for temporary use during a set period. By default, session cookies are enabled. Their goal is to make individual webpages load faster and improve website navigation.

    Persistent cookies − Persistent cookies are those that remain in the browser for an extended length of time. They will only be erased when the cookies expire or the users clear them from the browser after being installed.

Cookies Based on Purpose

Necessary cookies − These are cookies that have to be present for a website to work.

Non-Necessary cookies − These cookies help keep track of the behavior on a browser.

44. What are advantages and drawback of cookies?

    ANS.

Advantages of Cookies

1. User Friendly

Cookies are extremely user friendly. The client can choose what they need to do with cookies. All the browsers come with settings to clear history including the cookies. Manually users could find the cookies text files stored in the hard drive. Users can choose to edit and delete them.

2. Availability

Cookies can also set to be made available for a longer period of time. Once the cookies are stored on the user's hard drive, it will be available as long as the user deletes them manually. Even if the server fails, information can be retrieved from the cookies.

3. Convenience

Besides websites, cookies can also remember information related to forms. So each time the user visits the site, the address form will be filled automatically. However, cookies will not remember confidential information such as credit card info.

4. Marketing

Most companies, especially, e-commerce sites tends to use cookies to target products to their customers. Information such as search term, keywords and geographical locations are gathered for their marketing campaign. Even social networking sites like Facebook use cookies to show relevant ads.

5. Configurations

Cookies can also be configured as per the requirement. For an example, it can be made to expire once the user closes the browser tab or set to exist only for a specific period of time.

6. Server Requirement

All the data related to cookies are stored on the hard drive without the use of server resources. No extra load or weight is added to the server. Therefore, less burden is placed on them which makes cookies easier to implement.

Disadvantages of Cookies

1. Browser Impacts

Cookies are not restricted based on internet usage. Whenever a user surfs the web, more and more cookies will be accumulated. Unless the user deletes them, these cookies will be a part of the hard drive space. This eventually slows down or lags the browser.

2. Security Risks

Since cookies are stored in the hard drive as text files, it posses some serious security risks. Any intruder can easily open these files and view the information. And also, not all the sites that collect information from cookies are legitimate. Some of them can be malicious that uses cookies for the purpose of hacking.

3. Size Limitations

Size limitations also exist on cookies. They cannot store large amount of information. Most cookies are able to store information only up to 4kb. Browsers too pose restrictions when it comes to number of cookies. Except internet explorer, all other browsers only allow up to 20 cookies for a single website.

4. Privacy Concerns

Apart from security, privacy is another concern for users in cookies. Whenever the user browses the internet, the cookie enabled sites will be recording all the online activities. Most users are unaware that such information are stored on their hard drive. As a result, this information can be accessed by any third parties including government agencies and businesses.

5. Manual Disabling

Browsers also comes with the option to disable cookies. Users who are highly security conscious could simply disable them. Even some browsers disable cookies automatically if the security level is set to high. Therefore, web applications will not work without cookies.

6. Encoding Information

Both encrypting and decrypting cookies is a difficult process since it requires additional coding. Due to the time involved in the encoding process, the application's performance will be affected.

45. Explain “Session Hijacking” by misusing cookies information.

ANS.

What is Cookie Hijacking?

Cookie hijacking, also called session hijacking, is a way for hackers to access and steal your personal data, and they may also prevent you from accessing certain accounts. Hijacking cookies is just as powerful, sometimes more so, as finding out your password. It’s possible that with cookie hijacking, hackers can gain limitless access to all of your resources. For example, an attacker may steal your identity or confidential company data; purchase items; or steal from your bank account.

How Does Cookie Hijacking Work?

Cookie hijacking can occur when a malware program waits for a user to log in to the website. Then, the malware steals the session cookie and sends it to the attacker. A cookie attack is often initiated when an attacker sends a user a fake login. The victim clicks the fake link, which lets the attacker steal the cookie – actually, anything the user types in can be captured by the attacker. The attacker then puts that cookie in their browser and is able to act as you. Sometimes, a fake link isn't even needed. If a user is in a session on an unsecured, public Wi-Fi connection, hackers can easily steal that data that's traveling through the connection. And this can happen even if the site is secure and your username and password are encrypted. Once the attacker has a user's session cookie, they can log in to a website and do pretty much anything you could do, including changing your password. And this is often automated, so it happens in just seconds. If the attacker then enables multifactor authentication (MFA) against the victim, they may never gain access to their accounts again.

46. Explain TLS and S/MIME used in Email Security. Compare PGP Vs S/MIME.

ANS.

https://www.internetsociety.org/resources/ota/2017/transport-layered-security-tls-for-email/

https://www.tutorialspoint.com/what-is-secure-multipurpose-internet-mail-extensions-s-mime

https://www.geeksforgeeks.org/difference-between-pgp-and-s-mime/

47. Implement Hash function technique for secured network using Suitable Hashing tool and Validate using available online tools/Website tools. Explain the different features and record the different working snapshots for the same.

48. Explain following applications of Hash functions in detail

a. Protection to password storage

ANS.

Hashing is a common method used to protect password storage. When a password is hashed, it is transformed into a fixed-length string of characters using a cryptographic algorithm. This hash value is then stored in the database instead of the actual password.

Here are some key aspects to consider when using hashing for password storage:

One-way function: A good hash function is designed to be computationally infeasible to reverse. It should be a one-way function, meaning that given a hash value, it should be difficult (if not impossible) to determine the original password.

Cryptographically secure hash algorithm: It is essential to use a cryptographically secure hash algorithm such as bcrypt, Argon2, or scrypt. These algorithms are specifically designed for password hashing and include features like key stretching, which makes the hashing process slower and more resistant to brute-force attacks.

Salt: A salt is a random value added to each password before hashing. Salting prevents attackers from using precomputed tables (rainbow tables) to reverse hash values. Each user should have a unique salt value, which is stored alongside the hash. The salt value is typically a random string of characters.

Unique salt per user: As mentioned earlier, it is crucial to use a unique salt value for each user. This ensures that even if two users have the same password, their hash values will be different. It adds an extra layer of protection against attacks like rainbow table or precomputed hash attacks.

Iteration count: A good hash function should be computationally expensive. By iterating the hashing process multiple times, the workload for an attacker attempting to guess passwords through brute force or dictionary attacks is significantly increased. The iteration count should be chosen to strike a balance between security and acceptable performance.

Secure storage: While hashing protects against obtaining the original password, it does not protect against other types of attacks like database breaches. It is essential to store the hash values securely, using appropriate measures like encryption, access controls, and regular security audits.

Password policies: In addition to hashing, it is crucial to enforce strong password policies. Educate users about creating strong passwords and consider implementing measures like password complexity requirements, account lockouts after a certain number of failed login attempts, and multi-factor authentication (MFA) for added security.

b. Data Integrity check

ANS.

Hashing: It is where the data inside a document is hashed using an algorithm such as Secure Hash Algorithm version 1 (SHA1) and Message Digest version 5 (MD5). This turns the data inside the file into a long text string known as a hash value; this is also known as a message digest.

Hashing the Same Data: If you copy a file and therefore have two files containing the same data, and if you hash them with the same hashing algorithm, it will always produce the same hash value. Even if from two different vendors.

Verifying Integrity: During forensic analysis, the scientist takes a copy of the data prior to investigation. To ensure that he/she has not tampered with it during investigation, he/she will hash the data before starting and then compare the hash to the data when he/she has finished. If the hash matches, then we know that the integrity of the data is intact.

One-way function: For the purpose of the exam, hashing is a one-way function and cannot be reversed.

HMAC authentication: In cryptography, an HMAC (sometimes known as either keyed-hash message authentication code or hash-based message authentication code) is a specific type of Message Authentication Code (MAC) involving a cryptographic hash function and a secret cryptographic key. We can have HMAC-MD5 or HMAC-SHA1; the exam provides both data integrity and data authentication.

Digital signature: This is used to verify the integrity of an email so that you know it has not been tampered with in transit. The private certificate used to sign the email that creates a one-way hash function and when it arrives at its destination the recipient has already been given a public key to verify that it has not been tampered with in transit. This will be covered in more depth later in this book.

49. What is Hash function? Explain How it works briefly? List the different applications of SHA2.

ANS. Pg(4-11)

The SHA-2 family of hashing algorithms are the most common hash functions in use. SHA-256 is particularly widespread. These hash functions are often involved in the underlying security mechanisms that help to protect our daily lives. You may have never noticed it, but SHA-2 is everywhere.

To begin with, SHA-2 is involved in many of the security protocols that help to protect much of our technology:

Transport Layer Security (TLS) — This is one of the most widely used security protocols. You will notice it most prominently when connecting to a website that begins with https rather than http. The s at the end stands for secure, which indicates that TLS is being used to encrypt the data between your device and the server. This makes SHA-2 an important part of many of the connections you make to websites when surfing online.

Internet Protocol Security (IPSec) — IPSec is used to secure the connection between two points, and it's most commonly seen in VPNs.

Pretty Good Privacy (PGP) — PGP is one of the most popular protocols for encrypting emails so that they can only be read by the recipient. It protects the messages from hackers and other parties that may be able to read the data, such as your ISP.

Secure/Multipurpose Internet Mail Extensions (S/MIME) — S/MIME is another prominent security protocol involved in email encryption.

Secure Shell (SSH) — SSH is most commonly used for remotely accessing computers and servers, but it also has port forwarding, tunneling and file transfer applications.

In addition to being a core component of the above-mentioned security protocols, the SHA-2 family has a range of other uses. These include:

Authenticating data — Secure hash functions can be used to prove that data hasn't been altered, and they are involved in everything from evidence authentication to verifying that software packages are legitimate.

Password hashing — SHA-2 hash functions are sometimes used for password hashing, but this is not a good practice. It’s better to use a solution that’s tailored to the purpose like bcrypt instead.

Blockchain technologies — SHA-256 is involved in the proof-of-work function in Bitcoin and many other cryptocurrencies. It can also be involved in proof-of-stake blockchain projects.

50. Simulate Diffie-Hellman secure key exchange protocol using Vlabs simulation tool. Explain the different features of above protocol and record the different working snapshots for the same.

51. Write short note on the following
    a. Transport and tunnel mode in IPSec. **Pg(5-33)**
    b. S/MIME for Email security. **(Refer Q46)**
    c. TLS explanation with Suitable example **(Refer Q46)**

52. Simulate Vernam Cipher for encryption and decryption using Vlabs simulation tool. Explain the different features of above technique with suitable example and record the different working snapshots for the same

69. Explain AH and ESP working in IPSec.
ANS. Pg(5-34,5-35,5-36,5-37)