5. (a) **Define the Man-in-the-Middle Attack on Diffie-Hellman Key-Exchange Protocol.**

Ans:

The **Diffie-Hellman key exchange protocol** is a cryptographic method used to establish a shared secret key between two parties that can be used to perform secret communication on a public network while preventing eavesdropping. However, this protocol is vulnerable to a **man-in-the-middle attack**.

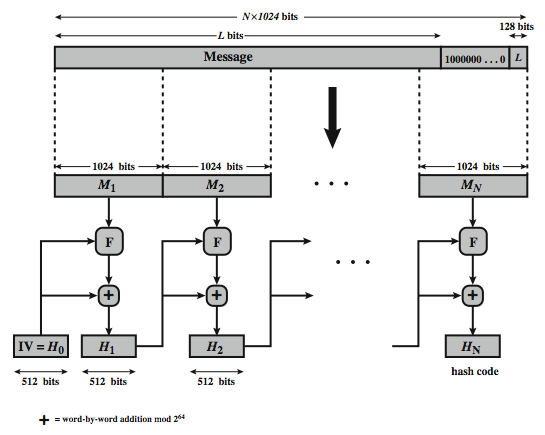
1. Darth prepares by creating two private / public keys
2. Alice transmits her public key to Bob
3. Darth intercepts this and transmits his first public key to Bob. Darth also calculates a shared key with Alice
4. Bob receives the public key and calculates the shared key (with Darth instead of Alice)
5. Bob transmits his public key to Alice
6. Darth intercepts this and transmits his second public key to Alice. Darth calculates a shared key with Bob
7. Alice receives the key and calculates the shared key (with Darth instead of Bob)

* Darth can then intercept, decrypt, re-encrypt, forward all messages between Alice & Bob

5. (b) **Describe SHA-512 Algorithm.**

Ans:

**SHA-512** stands for **Secure Hash Algorithm 512-bit**. [It is a cryptographic hash function that takes an input message of any length and produces a fixed-size output of 512 bits (64 bytes)](https://komodoplatform.com/en/academy/sha-512/). [The algorithm is used to convert text of any length into a fixed-size string, which is commonly used for email addresses hashing, password hashing, and digital record verification](https://komodoplatform.com/en/academy/sha-512/).



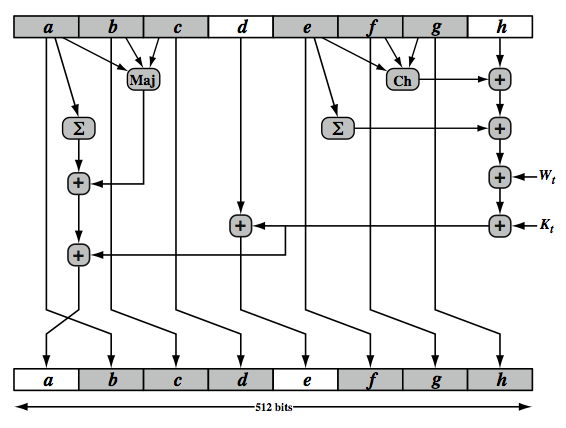


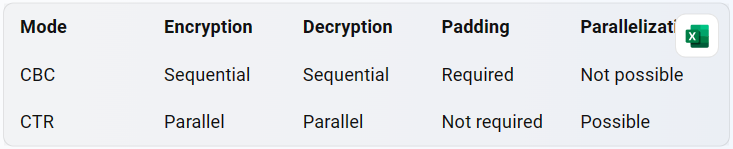
Figure: SHA-512 Round Function

5. (c) **Compare between CBC and CTR mode of operation.**

Ans:

**CBC and CTR comparison**

|  |  |
| --- | --- |
| **Cipher Block Chaining (CBC)** | **Counter (CTR)** |
| Padding needed | No padding |
| No parallel processing | Parallel processing |
| Separate encryption and decryption functions | Encryption function alone is enough |
| Random IV or a nonce | Unique nonce |
| Nonce reuse leaks some information about initial plaintext block | Nonce reuse will leak information about the entire message |



6. (a) Describe a symmetric key distribution scenario with confidentiality and authentication.

Ans:

In a symmetric key distribution scenario with confidentiality and authentication, two parties (Alice and Bob) want to communicate securely over an insecure channel. They share a secret key that is used for encryption and decryption of messages. The following steps describe how this can be achieved:

1. Alice and Bob agree on a secret key that will be used for encryption and decryption of messages.
2. Alice encrypts the message using the secret key and sends it to Bob.
3. Bob receives the encrypted message and decrypts it using the secret key.
4. To ensure confidentiality, Alice and Bob must keep the secret key secure from eavesdroppers.

To ensure authentication, Alice and Bob can use a message authentication code (MAC) to verify the integrity of the message. A MAC is a cryptographic checksum that is generated using a secret key and appended to the message. The following steps describe how this can be achieved:

1. Alice generates a MAC for the message using a secret key that is shared with Bob.
2. Alice sends the message along with the MAC to Bob.
3. Bob receives the message and computes the MAC using the same secret key.
4. If the computed MAC matches the received MAC, then Bob can be sure that the message has not been tampered with.

6.(b) Discuss on HMAC Algorithm.

Ans: