Cryptography and Cyber Security

Activity

Name:Harshith.H.D.
Dept:CSE(3rd year)
Sec:A
Date:29.09.24

Code Implementation

Write a simple program in Python (or another language) to simulate the Diffie-Hellman key exchange. Include comments explaining each part of the code.

Solution:

```
def diffie_hellman_key_exchange(p, g, alice_private_key,
bob_private_key):

    A = (g ** alice_private_key) % p
    B = (g ** bob_private_key) % p
    shared_secret_key_alice = (B ** alice_private_key) % p
    shared_secret_key_bob = (A ** bob_private_key) % p
    return shared_secret_key_alice, shared_secret_key_bob

if __name__ == "__main__":

    p = 23
    g = 5
```

```
    alice_private_key = 6
    bob_private_key = 15
```

```
    shared_secret_alice, shared_secret_bob =
diffie_hellman_key_exchange(p, g, alice_private_key, bob_private_key)
```

```
    print(f"Alice's computed shared secret key: {shared_secret_alice}")
    print(f"Bob's computed shared secret key: {shared_secret_bob}")
```

```
    if shared_secret_alice == shared_secret_bob:
        print("Success! Alice and Bob share the same secret key.")
    else:
        print("Error! The secret keys do not match.")
```

Output:

Alice's computed shared secret key: 2
Bob's computed shared secret key: 2
Success! Alice and Bob share the same secret key.

Quiz Creation

Develop a quiz with 10 questions about the Diffie-Hellman cipher. Include multiple- choice, true/false, and short answer questions.

Solution:

1. What is the primary purpose of the Diffie-Hellman key exchange?

- A) To encrypt data directly
- B) To sign digital documents
- C) To generate a shared secret key over an insecure channel
- D) To compress data

Answer: C

2. Which of the following is required in Diffie-Hellman key exchange?

- A) A symmetric encryption algorithm
- B) A trusted third party
- C) Large prime number and a base
- D) Digital signatures

Answer: C

3. True or False: Diffie-Hellman is mainly used for public key encryption.

Answer: False
Explanation: Diffie-Hellman is used to exchange keys securely, not for direct encryption of data.

4. Which of the following are the public values in the Diffie-Hellman process?

- A) Private keys of both parties
- B) Prime number ppp and base ggg
- C) Shared secret key
- D) None of the above

Answer: B

5. What is the shared secret key based on in Diffie-Hellman key exchange?

- A) Both public and private keys
- B) Alice and Bob's private keys
- C) Alice's public key
- D) Bob's public key

Answer: A
Explanation: The shared key is computed using each participant's private key and the other's public key.

6. True or False: In Diffie-Hellman, both participants must generate the same shared secret key if the calculations are done correctly.

Answer: True

7. Why is the Diffie-Hellman key exchange considered secure?

- A) Because the prime number and base are secret
- B) Because the private keys are never shared over the network
- C) Because it uses symmetric encryption
- D) Because it uses a trusted third party

Answer: B
Explanation: The private keys are never transmitted, making it hard for an attacker to derive the shared secret.

8. In Diffie-Hellman, if Alice's private key is 6 and Bob's private key is 15, and the agreed-upon public values are p=23 and g=5, what is Alice's public value A?

Answer:

$A=g^a \bmod p$

$A=5^6 \bmod 23= 15625 \bmod 23=8$

9. What is a major vulnerability of the Diffie-Hellman key exchange?

- A) It requires too many public keys
- B) It is susceptible to man-in-the-middle attacks
- C) The shared key is publicly transmitted
- D) Both participants need to share their private keys

Answer: B
Explanation: A man-in-the-middle attack can intercept the communication and establish separate shared keys with both parties.

10. What improvement can be added to Diffie-Hellman to prevent man-in-the-middle attacks?

- (Short Answer)

Answer: Digital signatures or using a Public Key Infrastructure (PKI) can help verify the identity of the participants, preventing man-in-the-middle attacks.

Infographic Design:

Design an infographic that visually explains the steps of the Diffie-Hellman exchange. Use icons and minimal text for clarity.

Solution: