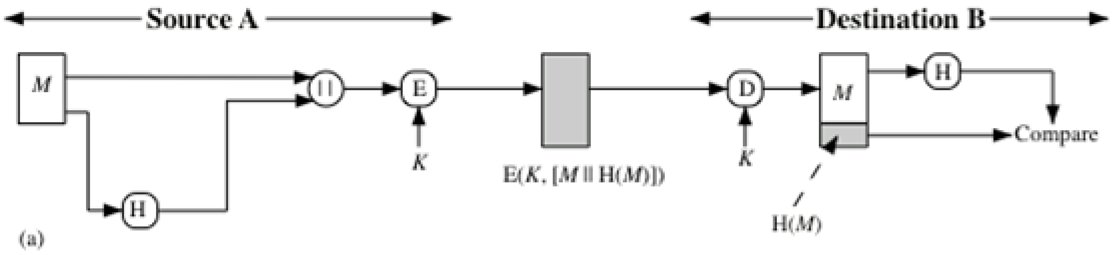
TEST 2

Question 1:

1.1.(3 marks)

The following schemas illustrate a variety of ways in which a hash code can be used to provide message authentication.

Schema 1:



Where:

M: plaintext
E: Encryption
K: secret key
H: Hash function
D: Decryption
S: seed value

For each schema above:

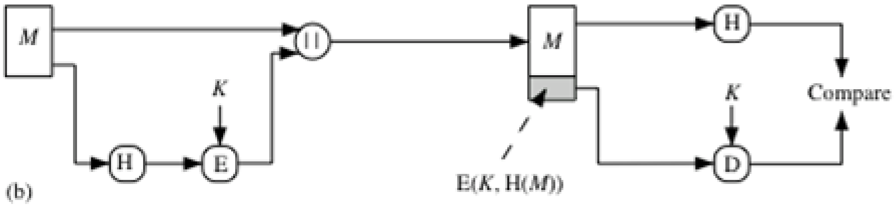
Describe the operation of this schema.

What are the advantages of this schema?

What are the disadvantages of this schema?

Answer:

Schema 2:



Where:

M: plaintext
E: Encryption
K: secret key
H: Hash function
D: Decryption
S: seed value

For each schema above:

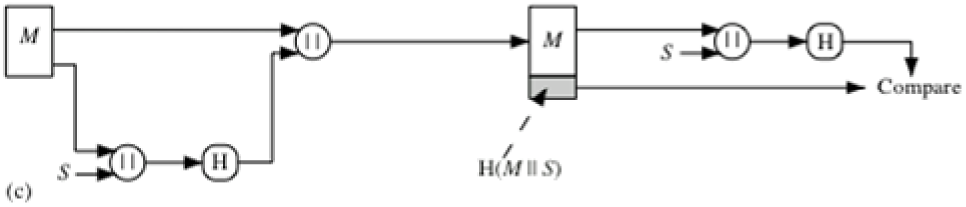
Describe the operation of this schema.

What are the advantages of this schema?

What are the disadvantages of this schema?

Answer:

Schema 3:



Where:

M: plaintext

E: Encryption

K: secret key

H: Hash function

D: Decryption

S: seed value

For each schema above:

Describe the operation of this schema.

What are the advantages of this schema?

What are the disadvantages of this schema?

Answer:

1.2. (2 marks)

Propose your own schema for the purpose of authentication and confidentiality.

Describe the operation of your own schema.

What are the advantages of your own schema?

What are the disadvantages of your own schema?

Answer:

Question 2:

2.1 (3 marks)

Alice would like to send a message to Bob that avoids any external entity on the Internet from reading and observing that message. Which of the keys would Alice best use – as shown in the box on the diagram in Figure 2.1 below.

Explain your answer.

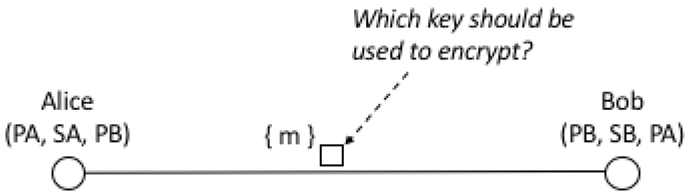


Figure 2.1 Alice Sending Message to Bob Using Encryption

Note: Explain your answer in details

Answer:

2.2 (2 marks)

Alice would like to use Diffie-Hellman Key Exchange to send a message to Bob that includes authentication and secrecy. Which of the two key would Alice best use – as shown in the two boxes on the diagram in Figure 2.2 below. Explain your answer.

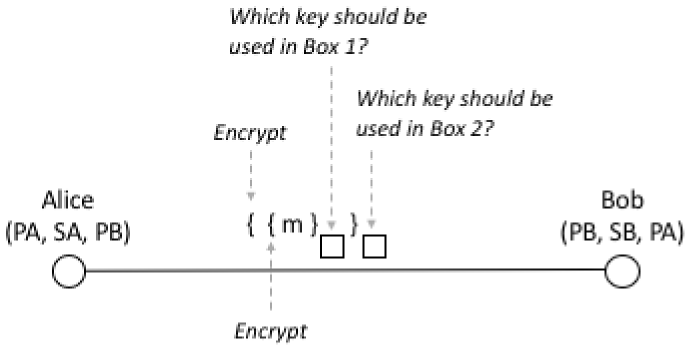

Which key should be used in Box 1?
Which key should be used in Box 2?
Encrypt
Alice
(PA, SA, PB)
{ { m } }
Bob
(PB, SB, PA)
Encrypt

Figure 2.2. Alice and Bob Using Diffie-Hellman Key Exchange

Note:

- **Students have to follow the steps and complete the tasks in details in order to have the results. If the students only write the result, that is, that result is not marked or recorded.**

- **Students do examination on word file and answer by English**