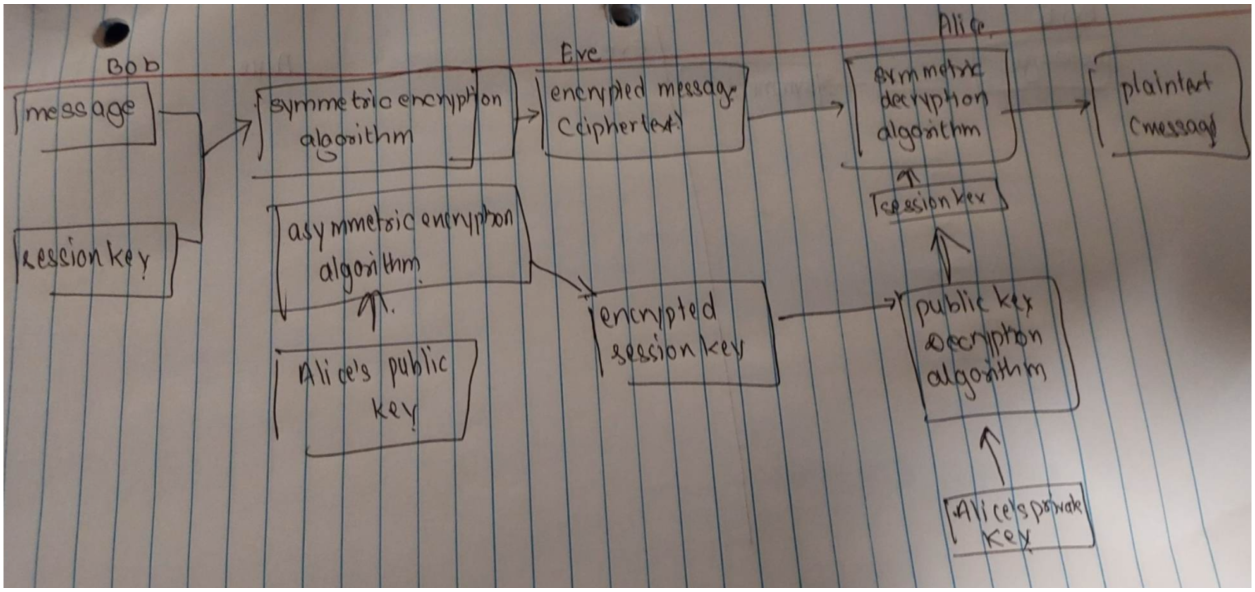
Question no.1

Draw a diagram to show the steps described in the following process (Page 81 of the book "Network Security Essentials, Applications, and Standards, Second Edition") This question assumes that Alice has a private key and a public key. When Bob wishes to communicate with Alice, Bob can do the following:

1. Bob prepares a message.
2. Bob creates a session key.
3. Bob encrypts the message using symmetric key cryptography and the session key.
4. Bob encrypts the session key using asymmetric key cryptography and Alice's public key.
5. Bob attaches the encrypted session key to the encrypted message and sends it to Alice.
6. Alice decrypts the session key using her private key.
7. Alice uses the decrypted session key to decrypt the message.

The diagram should include Alice, Bob, and Eve.


Bob
Eve
Alice
message
session key
symmetric encryption algorithm
asymmetric encryption algorithm
Alice's public key
encrypted message (ciphertext)
encrypted session key
symmetric decryption algorithm
session key
public key decryption algorithm
Alice's private key
plaintext (message)

Question no.2

Why Asymmetric key cryptography alone cannot resolve Internet security issues?

⇨ Asymmetric key cryptography, also known as public-key cryptography, is an essential component of Internet security. However, it cannot completely resolve all the security issues on its own. One of the primary reasons is scalability. Asymmetric key cryptography is computationally expensive compared to symmetric key cryptography, which means that it can be challenging to use it on a large scale. Additionally, asymmetric key cryptography is vulnerable to man-in-the-middle attacks if the public key is not properly authenticated.

A strong and scalable security solution for the Internet is often provided by combining asymmetric and symmetric key cryptography with other security measures like digital certificates to meet these problems.

Please assess the following statements and give your reasons:

- Encryption in symmetric key cryptography provides authentication.

⇨ This statement is not entirely correct. While encryption in symmetric key cryptography can provide some level of authentication, it is not its primary purpose. The main goal of symmetric key cryptography is to provide confidentiality for data by encrypting it with a secret key. Authentication, on the other hand, refers to the process of verifying the identity of the sender and the integrity of the message.

It can provide authentication to some extent by using a technique called a Message Authentication Code (MAC). MAC is a small piece of data that is generated using a secret key and is appended to the message. The recipient of the message can then verify the MAC using the same secret key to ensure that the message has not been tampered with in transit. However, this is not the primary purpose of symmetric key cryptography, and other cryptographic techniques such as digital signatures are typically used to provide a more robust authentication mechanism.

- Encryption in asymmetric key cryptography provides authentication.

⇨ It does not provide authentication on its own. Asymmetric key cryptography is also known as public-key cryptography. The primary goal of asymmetric key cryptography is to provide a secure way to exchange messages and establish secure communication channels without having to share a secret key.

While encryption in asymmetric key cryptography can provide some level of message integrity, it does not provide authentication on its own. To achieve authentication, digital signatures are typically used in combination with asymmetric key cryptography. A digital signature is created using the sender's private key and is appended to the message. The recipient of the message can then verify the signature using the sender's public key to ensure that the message is authentic and has not been tampered with in transit.

Question no.3

NSA prefers exportable security algorithms easier to break or harder to break.

- ⇨ The preferences of the NSA regarding the security of encryption algorithms are not clear. However, historically, the NSA has been known to advocate for the use of weaker cryptographic algorithms for export purposes. There have also been concerns that the

NSA may attempt to influence the development of new encryption standards to make them more vulnerable to attacks.

Question no.4

To achieve the same level of security, which one needs to use a larger key size? Symmetric key cryptography or asymmetric key cryptography? Please explain your answer

⇨ To achieve the same level of security, symmetric key cryptography requires a larger key size than asymmetric key cryptography.

In symmetric key cryptography, both the sender and the receiver share the same secret key, which is used for both the encryption and decryption of messages. To maintain the confidentiality of the message, the key size must be sufficiently large to make it difficult for an attacker to guess the key. The larger the key size, the more possible key combinations there are, and the more difficult it becomes to break the encryption.

In contrast, in asymmetric key cryptography, each user has a public key and a private key. The public key can be shared widely, while the private key is kept secret. The key size in asymmetric key cryptography is typically much smaller than in symmetric key cryptography because it is not necessary to keep the private key secret. Instead, the security of the system relies on the computational difficulty of factoring large numbers.

Overall, the key size required to achieve a given level of security depends on the specific cryptographic algorithm and its implementation. However, in general, symmetric key cryptography requires a larger key size to achieve the same level of security as asymmetric key cryptography.

Question no.5

Symmetric key cryptography and asymmetric key cryptography are complementary. Please explain why and how?

⇨ Symmetric key cryptography and asymmetric key cryptography are complementary because they each have strengths and weaknesses that can be used together to provide a more secure communication channel. While symmetric key cryptography is efficient and fast, it has a significant weakness in that the key must be securely distributed between sender and recipient. Asymmetric key cryptography provides a solution to this problem by allowing for secure key exchange but is relatively slow and inefficient. By using both approaches together, the benefits of each can be combined to create a more secure and efficient communication system.

For example, one common approach is to use asymmetric key cryptography to establish a secure communication channel between the sender and the recipient and then use symmetric key cryptography to encrypt the actual data being transmitted over that channel. This approach allows for the efficient encryption of large amounts of data using a secure key that is distributed over a secure channel. Another common use of both types of cryptography is to use symmetric key cryptography for data encryption, and then use asymmetric key cryptography to securely exchange the symmetric key between the sender and the recipient.

Question no.6

What are the principal ingredients of a public-key cryptosystem?

⇨ The principal ingredients of a public-key cryptosystem are:

1. Key exchange: Public-key cryptography can be used to securely exchange a secret key between two parties, which can then be used for symmetric encryption. The Diffie-Hellman key exchange

protocol is a popular example of a key exchange algorithm that uses public-key cryptography.

2. Encryption algorithm: An algorithm that uses the public key to encrypt data.
3. Decryption algorithm: An algorithm that uses the private key to decrypt the encrypted data.
4. Digital signature algorithm: An algorithm that uses the private key to generate a digital signature, which can be verified using the corresponding public key to ensure that the data has not been tampered with.
5. Key exchange protocol: A protocol used for securely exchanging public keys between two parties to establish a secure communication channel.

Question no.7

List and briefly define three uses of a public-key cryptosystem.

1. Key exchange: Public-key cryptography can also be used to securely exchange secret keys for symmetric-key cryptography. In this use case, the public key of the recipient is used to encrypt a secret key that is used for symmetric-key encryption. Once the recipient receives the encrypted key, they can use their private key to decrypt it and obtain the shared secret key. This ensures that the shared key is kept confidential and cannot be intercepted by an attacker.
2. Digital signatures: A public-key cryptosystem can be used to create digital signatures, which are used to verify the authenticity of a digital document or message. The sender can use their private key to sign the document, and the recipient can use the sender's public key to verify the signature.
3. Encryption and decryption: As you mentioned, public-key cryptography can be used for encryption and decryption. In this case, the recipient publishes their public key, which anyone can use to encrypt a message. The recipient can then decrypt the message

using their private key. This approach is often used in situations where it's difficult to securely share a secret key, such as when communicating over an unsecured network.

Question no.8

What is the difference between a private key and a secret key?

- ⇨ A private key is used in a public-key cryptography system, which is also known as asymmetric cryptography. In this system, each user has a pair of keys: a public key that is available to anyone, and a private key that is kept secret. The public key is used for encryption, and the private key is used for decryption. The private key is mathematically related to the public key, but it cannot be derived from the public key.
- ⇨ On the other hand, a secret key is used in a symmetric cryptography system. In this system, the same key is

used for both encryption and decryption, and the key is kept secret by the users who need to communicate securely. The key is shared between the sender and the recipient, and they use it to encrypt and decrypt messages. Because the same key is used for both encryption and decryption, symmetric cryptography is generally faster and more efficient than asymmetric cryptography.

Question no.9

How can public-key encryption be used to distribute a secret key?

Public-key encryption can be used to securely distribute a secret key between two parties who wish to communicate securely using symmetric encryption. This is how it works:

1. The two parties exchange public keys: First, the parties exchange their public keys with each other over an insecure channel, such as the internet. Each party keeps its private key secret.

2. One party generates a secret key: One of the parties, say party A, generates a random secret key to be used for symmetric encryption.
3. Encrypt the secret key: Party A encrypts the secret key using party B's public key. This encrypted message can only be decrypted using party B's private key.
4. Send the encrypted secret key to party B: Party A sends the encrypted secret key to party B over the insecure channel.
5. Decrypt the secret key: Party B uses its private key to decrypt the encrypted secret key sent by party A.
6. Secure communication: Now that party A and party B both have the same secret key, they can use it to securely communicate with each other using symmetric encryption.

By using public-key encryption to distribute the secret key, the parties can securely establish a shared secret key without the need for prior exchange of a secret key. This process provides an efficient way to establish secure communication channels between two parties over an insecure channel.