Alice and Bob wish to communicate with each other over the Internet. Each uses RSA, the common asymmetric cryptography protocol. Thus, each has his/her own private key and knows the public key of the other. Let us denote private key of Alice as Pr(A), private key of Bob as Pr(B), public key of Alice as Pu(A), and public key of Bob as Pu(B).

Please use the following notation in presenting your answers:

E\_K (M): Message M is encrypted using key K

D\_K (M): Message M is decrypted using key K

Alice wants to send a message to Bob so that no one else can read it. Let us denote the message as M\_1.

How would Alice send the message?

Let us denote the message Alice sent as M\_3. How would Bob decipher the message?

In this situation, Alice does not care if anyone can read her message. But she does care that no one in the middle can change the message (in an undetectable manner). Let us denote the message as M\_2.

How would Alice send the message?

What would Bob do to verify that the message indeed came from Alice?

Answer:

Scenario 1: Alice wants to send a message (M1) to Bob securely.

1. Alice encrypts the message M1 using Bob's public key (Pu(B)): E\_Pu(B)(M1).
2. Alice sends the encrypted message E\_Pu(B)(M1) to Bob.
3. Bob receives the encrypted message and decrypts it using his private key (Pr(B)): D\_Pr(B)(E\_Pu(B)(M1)).
4. Bob can now read the original message M1.

Scenario 2: Alice wants to send a message (M2) to Bob securely, with integrity protection.

1. Alice calculates a cryptographic hash of the message M2, denoted as Hash(M2).
2. Alice encrypts both the message M2 and the hash value Hash(M2) using Bob's private key (Pr(B)): E\_Pr(B)(M2) and E\_Pr(B)(Hash(M2)).
3. Alice sends both the encrypted message E\_Pr(B)(M2) and the encrypted hash E\_Pr(B)(Hash(M2)) to Bob.
4. Bob receives the encrypted message and the encrypted hash.
5. Bob decrypts both using Alice's public key (Pu(A)): D\_Pu(A)(E\_Pr(B)(M2)) and D\_Pu(A)(E\_Pr(B)(Hash(M2))).
6. Bob verifies the integrity by calculating the hash of the received message M2 and comparing it with the decrypted hash value. If they match, the message has not been tampered with.

Scenario 3: Alice wants to send a message (M3) to Bob without caring about confidentiality but ensuring integrity.

1. Alice calculates a cryptographic hash of the message M3, denoted as Hash(M3).
2. Alice appends the hash value Hash(M3) to the message M3: M3 || Hash(M3).
3. Alice signs the combined message using her private key (Pr(A)): Sign\_Pr(A)(M3 || Hash(M3)).
4. Alice sends the signed message Sign\_Pr(A)(M3 || Hash(M3)) to Bob.
5. Bob receives the signed message.
6. Bob verifies the integrity and authenticity by using Alice's public key (Pu(A)) to verify the signature: Verify\_Pu(A)(Sign\_Pr(A)(M3 || Hash(M3))).
7. If the verification is successful, Bob can be confident that the message originated from Alice and has not been tampered with.

Each scenario addresses different security objectives which depend on the requirements of the communication and the level of security needed