Asymmetric Cryptography

Question 1 ***Pairing an IOT Device***

Alice wishes to pair her new IoT device and her laptop by having them exchange a symmetric key k. The devices will later use k to encrypt plaintext messages and send the ciphertexts to each other. Assume that there is a MITM on the network between the IoT device and the laptop. To defend against the MITM, Alice is considering the security of different pairing protocols. For each scenario below, select all true statements.

The "old key" refers to a symmetric key from some previous pairing. $\mathsf{Enc}(\mathsf{PK}; m)$ refers to public-key encryption of m with PK. Each subpart is independent.

Q1.1 The IoT device chooses k randomly and sends it to the laptop unencrypted over the network.

■ (A) MITM can decrypt the messages from the IoT device to the laptop

■ (B) MITM can decrypt the messages from the laptop to the IoT device

■ (C) At least one of the devices could accept an attacker's key that was not an old key

■ (D) MITM can make at least one of the devices to accept an old key

☐ (E) None of the above

☐ (F) ——

Solution: All because there is no security here.

Q1.2 The IoT device sends a message to the laptop asking for its public key PK. The laptop sends PK to the IoT device. The IoT device chooses k randomly and sends $\mathsf{Enc}(\mathsf{PK}; k)$ to the laptop.

■ (G) MITM can decrypt the messages from the IoT device to the laptop

■ (H) MITM can decrypt the messages from the laptop to the IoT device

■ (I) At least one of the devices could accept an attacker's key that was not an old key

■ (J) MITM can make at least one of the devices to accept an old key

☐ (K) None of the above

☐ (L) ——

Solution: MITM can supply its own PK to the IoT device so there is no security here.

Q1.3 Alice manually enters the publicly-known PK of the laptop into the IoT device. The IoT device chooses k randomly and sends $\mathsf{Enc}(\mathsf{PK}; k)$, to the laptop.

☐ (A) MITM can decrypt the messages from the IoT device to the laptop

■ (B) MITM can decrypt the messages from the laptop to the IoT device

■ (C) At least one of the devices could accept an attacker's key that was not an old key

■ (D) MITM can make at least one of the devices to accept an old key

☐ (E) None of the above

☐ (F) ——

Solution: MITM cannot read messages from the IoT device but can provide a corrupted k' to the laptop by encrypting it under the public key of the laptop.

Q1.4 Alice manually enters the publicly-known PK of the laptop into the IoT device, and the publicly-known verification key of the IoT device into the laptop. The IoT device chooses k randomly, computes $\mathsf{Enc}(\mathsf{PK}; k)$, and sends this ciphertext to the laptop along with a signature of the ciphertext from the IoT device. The laptop verifies the signature and rejects the key if the signature fails.

☐ (G) MITM can decrypt the messages from the IoT device to the laptop

☐ (H) MITM can decrypt the messages from the laptop to the IoT device

☐ (I) At least one of the devices could accept an attacker's key that was not an old key

■ (J) MITM can make at least one of the devices to accept an old key

☐ (K) None of the above

☐ (L) ——

Solution: The MITM can replay an old key.

Q1.5 The IoT device and the laptop run Diffie-Hellman key exchange to agree on the symmetric key.

■ (A) MITM can decrypt the messages from the IoT device to the laptop

■ (B) MITM can decrypt the messages from the laptop to the IoT device

■ (C) At least one of the devices could accept an attacker's key that was not an old key

☐ (D) MITM can make at least one of the devices to accept an old key

☐ (E) None of the above

☐ (F) ——

Solution: DH is vulnerable to MITM.

Option (D) is incorrect because a MITM cannot force the new key to match an old key (without solving the discrete log problem).

Q1.6 Alice manually enters the verification key of the IoT device into the laptop. The IoT device and the laptop run Diffie-Hellman key exchange to agree on k. The IoT device signs its DH public key and sends it with a signature to the laptop as part of this exchange. The laptop verifies the signature and rejects the key if the signature fails.

■ (G) MITM can decrypt the messages from the IoT device to the laptop

☐ (H) MITM can decrypt the messages from the laptop to the IoT device

■ (I) At least one of the devices could accept an attacker's key that was not an old key

☐ (J) MITM can make at least one of the devices to accept an old key

☐ (K) None of the above

☐ (L) ——

Solution: The attacker can still manipulate messages sent by the laptop.