CSE-447
Assignment - 04

Submitted By:
Mohammad Shafkat Hasan
Section: 01
ID: 19101077

Date of Submission:
29th August 2023

ID: 19101077

Ans. To The Q. No. 1

Trudy can use a man-in-the-middle (MIM) attack to intercept the messages being sent between Alice and Bob and then relays them back to each of them, pretending to be the other party. Once Trudy has intercepted the messages, he can extract public keys of Alice and Bob, then use it to forge messages. When Bob receives this message, he will think it's from Alice and use the encryption key to decrypt it. In this way, Trudy can eavesdrop on the communication between Alice and Bob.

Ans. To The Q. No. 2

(a)

Alice's browser will issue a warning that the certificate verification has failed and give Alice the option to stop or continue. If Alice chooses to stop that mim attack will fail.

(b)

If Alice chooses to continue after the browser warning, the attack will succeed.

ID: 19101077

Ans. To The Q.No. 3

(a)

TGT is a ticket that is issued by Key Distribution center (KDC) to a user. It allows the user to request tickets for other services, such as file shares or printers in a network. Every TGT is encrypted with K_{KDC} secret key, so only the KDC can read it.

(b)

The TGT sent to Alice so that she can use it to request tickets for other services. If the TGT was stored on the KDC, Alice would have to log in to the KDC every time she wanted to access a service. This would be

a security inconvenient and would also be a risk.

(c)

The TGT is encrypted with Alice's key kA so that only Alice decrypt it. This prevents an attacker from intercepting the TGT and use it to authenticate