Abdelrahman Adel
17012296

PAGE
DATE

# Assignment 7

(1) ① Lack of Acknowledgements (ACKs)
② Flow control issues
③ Sequence Number uncertainty
④ Error handling
⑤ Session Termination issues
⑥ Security Protocols & Integrity checks

(2) It's not susceptible to reflection attacks

(3) $\{R+A\}_A$ & $\{R\}_{R+A}$

(4) Step 1:- Alice generates nonce $N_A$ & sends to Bob:

$$M_1 = (A, B, N_A, \{A, B, N_A, \text{"Request"}\}_{K_{AC}})$$

Step 2: Bob generate $N_B$ & sends the message:

$$M_2 = (A, B, N_A, N_B, \{A, B, N_A, \text{"Request"}\}_{K_{AC}}, \{B, N_B\}_{K_{BC}})$$

Step 3:- Carol decrypts Message & verifies key $K_{AB}$

~~$M_3 = (A, B, N_A \{N_A, K_{AB}$~~

$$M_3 = (A, B, N_A, N_B, \{N_A, K_{AB}\}_{K_{AB}}, \{N_B, K_{AB}\}_{K_{BC}})$$

Step 4:- $M_4 = (A, B, N_A \{N_A, K_{AB}\}_{K_{AC}})$

Step 5:- Alice Decrypts $M_4$ #

(5) The protocol isn't fully secure & has several vulnerabilities mainly for replay attacks

(6) We can try to make a Secret Key Based Design

1. Initialize each phone with unique key secret ke during the ~~authentication~~ activation process

2. Authentication:
   - Phone creates nonce N & sends to network
   - Network sends nonce N'
   - Phone responds with Hash of H(K, N||N')
   - Verifies the phone response.