

Lab 13

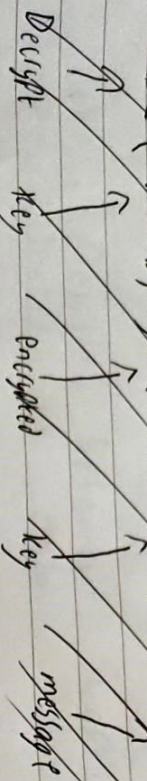
1) how would Alice send the message?

Alice should encrypt the message m_1 using Bob's Public key $P_u(B)$

$$E_{\{P_u(B)\}}(m_1)$$

Then Alice sends an encrypted message. Bob receives the message. Bob needs to decrypt using his Private key

$$D_{\{P_r(B)\}}(E_{\{P_u(B)\}}(m_1))$$



2) Let us denote the message Alice sent as M_1 . how would Bob decipher the message.

Bob uses Private key to decrypt the message. this looks like this

$$D_{\{P_r(B)\}}(E_{\{P_u(B)\}}(m_1))$$

this Private key is used to decrypt the message.

3) how would Alice send the message.

Alice could use a digital signature to sign the message.

makes a digest of message using a hash function $H(m_2)$. Alice would have to encrypt the message using her Private key

$$E_{\{P_r(A)\}}(H(m_2))$$

Alice attaches digest to the encrypted message.

$$M_2 || E_{\{P_r(A)\}}(H(m_2))$$

Alice can now send the message.

4) how would Bob verify the message was from Alice.

Bob would have to separate the digest from the original message. Then he would decrypt the encrypted message

$$D_{\{P_u(A)\}}(E_{\{P_r(A)\}}(H(m_2)))$$

Bob creates digest of the message using Alice's hash $H(m_2)$

Bob can compare decrypted digest with the received message digest. If they are the same the message was not edited.

Q3) ~~Server: fails to receive acknowledgement~~

Client: Decompress the received state using State 1. base state gets discarded

Server: gets acknowledgement of state 2

Client: received state changes with ID of 3

Server: fails to receive acknowledgement

Server: since 2, ID is 4 and packet is lost.

Client: Decompress received state using state 3. 1 and 2 get discarded.

Server: since state 3, ID is 15

Client: Acknowledgement 5 sent

Server: ACK received, server sent packet 6

4) compress string BABABAAA

Encoder	Output	String	Table	
66	B	256	BA	P = A
				C = empty

Encoder	Output	String	Table	
66	B	256	BA	P = B
65	A	257	AB	C = empty

Encoder	Output	String	Table	
66	B	256	BA	P = A
65	A	257	AB	C = empty
256	BA	258	BAA	

Encoder	Output	String	Table	
66	B	256	BA	P = A
65	A	257	AB	C = empty
256	BA	258	BAA	
257	AB	259	AABA	

encoder	outPut	string	Table	
66	B	256	BA	BABAB
65	A	257	AB	P: A
256	BA	258	BAA	C: A
257	AB	259	ABA	
65	A	260	AA	

encoder	outPut	string	Table	
66	B	256	BA	BABAA BA
65	A	257	AB	P: AA
256	BA	258	BAA	C: empty
257	AB	259	ABA	
65	A	260	AA	
260	AA			