Lab 13

1) how would Alice send the message?

Alice should encrypt the message m1 using Bob's Public key $P_u(b)$

$E_{-}\{P_u(b)\}(m1)$

then Alice sends an encrypted message. Bob receives the message. Bob needs to decrypt using his private key

$D_{-}\{Pr(B)\}(E_{-}\{P_u(B)\})(m1)$.

Decrypt key encrypted key message

2) Let us denote the message Alice sent as M_3. how would bob decipher the message?

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

$D_{-}\{Pr(B)\}(E_{-}\{P_u(B)\})(m1)$.

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.

Alice makes a digest of message using a hash function $H(m2)$. Alice would have to encrypt the message using her private key

$E_{-}\{Pr(A)\}(H(m2))$

Alice attaches digest to the encrypted message.

$M2 \,||\, E_{-}\{Pr(A)\}(H(m2))$

Alice can now send the message.

4) how would bob verify the message was from Alice:

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

$D_{-}\{P_u(A)\}\, E_{-}\{Pr(A)\}(H(m2))$.

Bob creates digest of the message using Alice's hash $H(m2)$

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

Q3)

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: Decompresses 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 BaBaaBaaa

encoder	output	string	Table
66	B	256	BA

BA

P = A

C = empty

encoder	output	string	Table
~~66~~			
66	B	256	BA
65	A	257	AB

BABA

P = B

C = empty

encoder	output	string	Table
66	B	256	BA
65	A	257	AB
256	BA	258	BAA

BABAA

P = A

C = empty

encoder	output	string	Table
66	B	256	BA
65	A	257	AB
256	BA	258	BAA
257	AB	259	ABA

BABAABAA

P = A

C = empty

encoder	output	string	Table
66	B	256	BA
65	A	257	AB
256	BA	258	BAA
257	AB	259	ABA
65	A	260	AA

BABAAB

P=A
C=A

encoder	output	string	Table
66	B	256	BA
65	A	257	AB
256	BA	258	BAA
257	AB	259	ABA
65	A	260	AA
260	AA		

BABAABA

P= AA
C= empty.