Extended Euclidean Algorithm

$\gcd(17, 72) = 1$

$1 = d \cdot 17 + x \cdot 72$

$72 = 17 \cdot 6 + r$

$17 \cdot 4 + 16$

$17 = 16 \cdot 1 + 1$

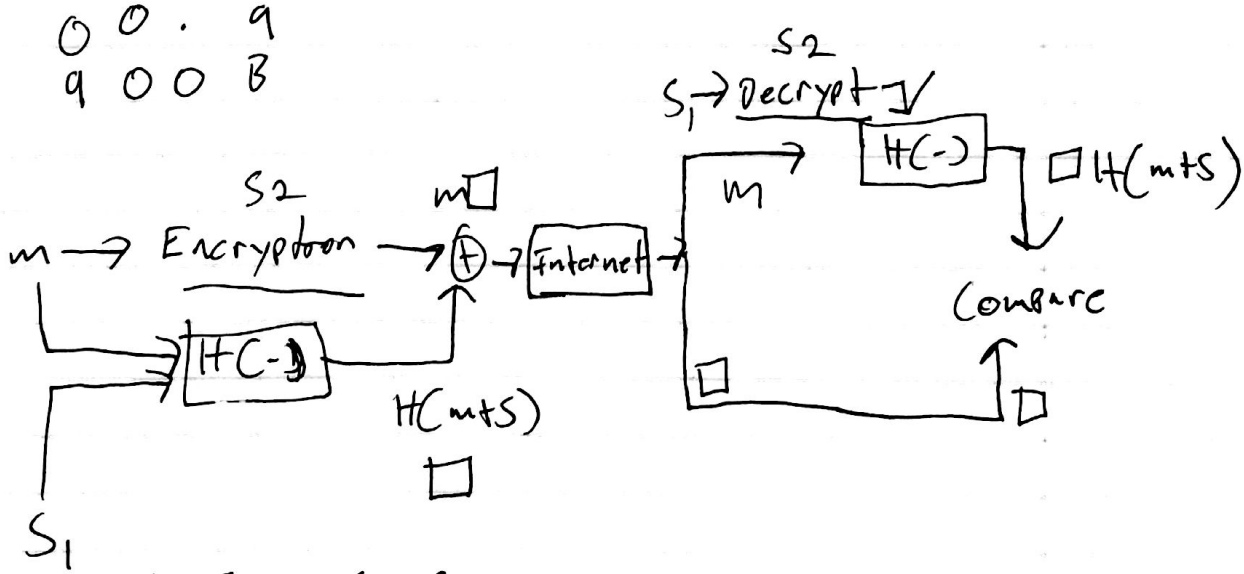
$16 = 1 \cdot 16 + 0$

Ch 8 P11, 12, 13, 15

P11

I	B	U	I
0	0	.	9
9	0	0	B

P12



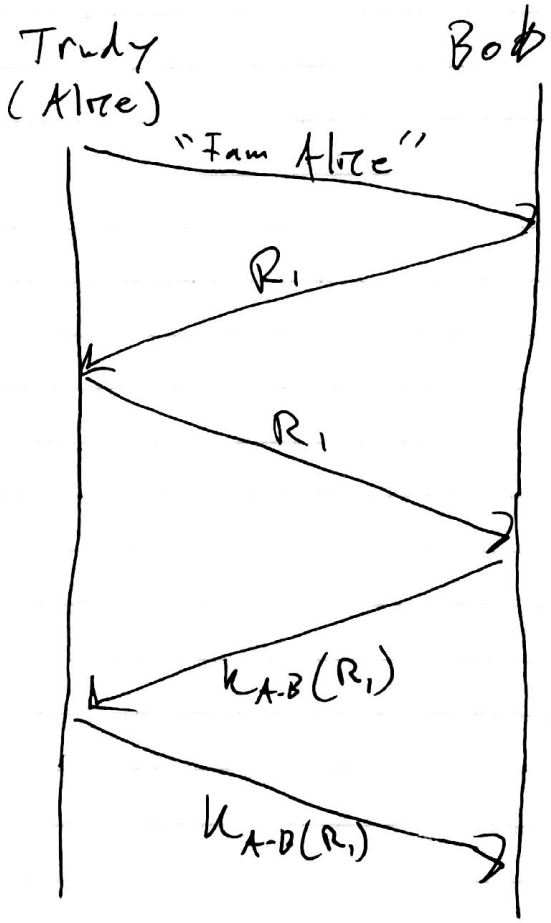
m = message
S_1 = Auth code
S_2 = Encryption code

Q13

Hash blocks and give key on fully trusted site

Then when it's done downloading, it checks the hash and if it doesn't match, it gets thrown out.

Q15



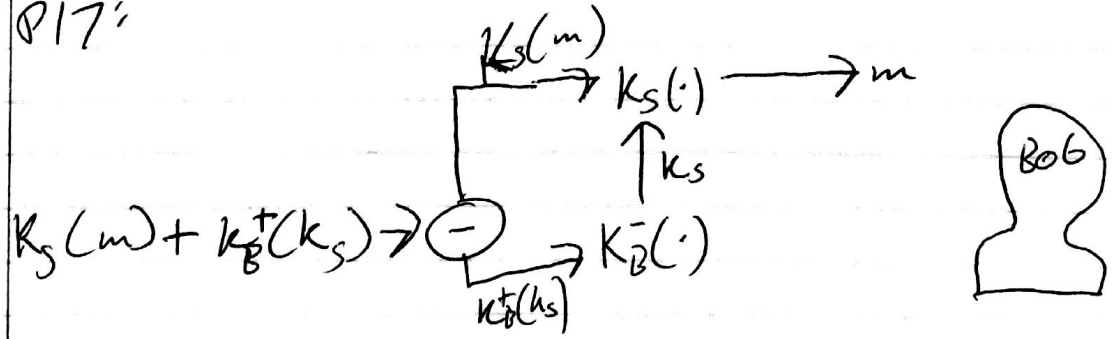
Networking

P16:

a)

b) Trudy could intercept Alice's encryted nonce response and passed it off to Bob, thus appearing to be Alice to Bob.

P17:



P19)

a) Packet 112 is sent by the client

b) Server IP: 216.75.194.220 port#: 443

c) 114

d) 1

e) ~~Neither~~ Yes

f)

P20) To do a deletion attack you'd need to guarentee that the resulting checksum will have the same value after deletion.

P21) Probably, but to set the right sequence number you'd have to be using wireshark almost in the same room.