Rob Johansen

u0531837

CS 4480 - Homework Assignment 7

P8

a. n = pq = 5*11 = 55
z = (p-1)(q-1) = (5-1)(11-1) = 40

b. Because 3 is less than 5 (n), and has no common factors with 40 (z).

c. d = 27 (because 3*27 = 81 mod 40 = 1)

d. $c = m^e \bmod n$
$c = 8^3 \bmod 55$
c = 512 mod 55
c = 17

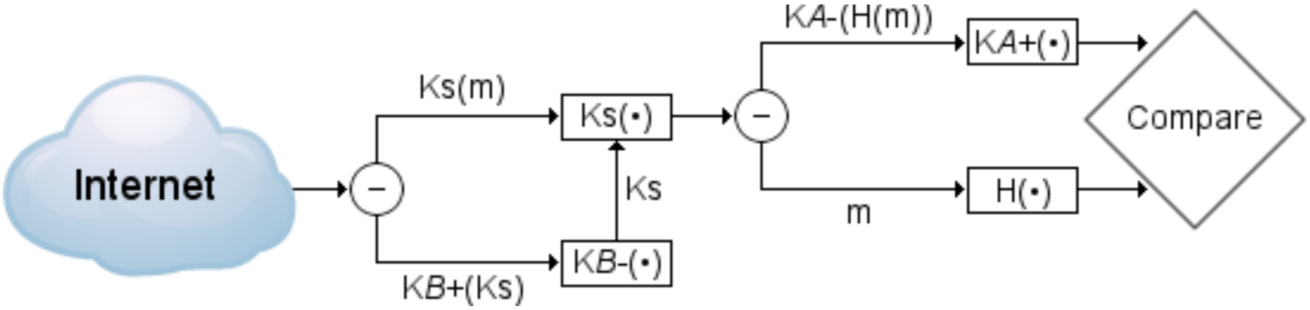
P15

Trudy could authenticate as Alice using the following technique:

1. Trudy sends the message "I am Alice" to Bob.
2. Bob chooses a nonce, R, and sends it to Trudy.
3. Trudy waits.
4. At some point, Bob sends the message "I am Bob" to Trudy.
5. Trudy sends Bob the *same* nonce, R, that he sent her in step 2.
6. Trudy continues to wait.
7. Bob encrypts the nonce using Alice and Bob's symmetric key and sends the encrypted nonce $K_{A-B}(R)$ to Trudy.
8. Trudy then simply sends Bob the *same* encrypted nonce, $K_{A-B}(R)$, that he just sent her in the previous step.
9. Trudy continues to wait.
10. Bob decrypts the nonce and verifies that it equals the nonce he sent. Trudy is now authenticated as Alice.

P17 (using Figure 8.21)

The following diagram illustrates the operations Bob must perform after receiving a message from Alice. He must decrypt the session key using his private key, then use the decrypted session key to decrypt the message, then decrypt the message digest using Alice's public key, then compute the hash and compare it with the one received from Alice:



P19

a. Packet 112 is sent by the client.

b. The server's IP address is 216.75.194.220. Its port is 443.

c. The acknowledgment number provided by the server is what the client will use as the sequence number of the next TCP segment it sends: 2785.

d. There are 3 SSL records in packet 112.

e. Neither. The Master Secret is independently computed by both client and server. The Encrypted Master Secret is only part of the "almost-SSL" protocol (see figure 8.25 on page 713 of the book).

NOTE: The level of detail posed by questions f, g, and h seems to be outside the scope of the book. I scrutinized section 8.6 repeatedly, but ultimately could not find the answers. As a result, I submitted a post in the discussion forum to which Kobus responded saying he would adjust the point allocation:

https://utah.instructure.com/courses/269722/discussion_topics/912883

P22

a. False

b. True

c. True

d. False

P25

Following is the filter table (access control list):

action	**source address**	**dest address**	**protocol**	**source port**	**dest port**	**flag bit**	**check conxion**
allow	222.22/16	outside of 222.22/16	TCP	>1023	23	any	
allow	outside of 222.22/16	222.22/16	TCP	23	>1023	ACK	X
allow	outside of 222.22/16	222.22.0.12	TCP	>1023	80	any	X
deny	all	all	all	all	all	all	

Following is the connection table, which contains three connections (all from inside to outside):

source address	**dest address**	**source port**	**dest port**
222.22.0.30	37.96.87.124	21176	23
222.22.0.31	198.1.205.23	6873	23
222.22.0.32	203.76.240.43	52812	23