Isaac Llewellyn
661582061

Homework # 2.b

Due October 15, 2018.

<u>Please show your work to get full credit.</u>

Q-1-) Users A and B use the *Diffie-Hellman* key exchange technique with a common prime q = 71 and a primitive root α = 7.

a) If user A has a private key X_A = 5, what is A's public key Y_A?
b) If user B has a private key X_B = 12, what is B's public key Y_B?
c) What is the shared secret key?

prime = 7`
priva = 5
privb = 12
puba = 7^5mod71 = 51
pubb =7^12mod71 = 4
Shared secret = 4^5mod71 =
30 = 51^12mod71

d) In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant (α^x mod q) for some public number α. What would happen if the participants sent each other (x^α mod q) instead?

In this case, each participant would be communicating using their secret number as their generator. This may not aways work as x will not always create full cyclic groups,

Q-2-) A network resource X is prepared to sign a message by appending the appropriate 64-bit hash code and encrypting that hash code with X's private key as described in class (also in the textbook, Page 330.

a) Describe the *Birthday Attack* where an attacker receives a valid signature for his fraudulent message?
a: The attacker would generate 2^64/2 fraudulent messages, and stores their respective hash values.
When the attacker finds a matching signature, the attacker can then send a fraudulent message containing that signature.
b) How much memory space does attacker need for an M-bit message?
b: 2^(m) bits to brute force every combination.
c) Assuming that attacker's computer can process 2^{20} hash/second, how long does it take at average to find pair of messages that have the same hash?
c; Assuming a message that has the same hash appears 50% of the way through;
(2^63)/(2^20) seconds, ~~ 287 years.
d) Answer (b) and (c) when 128-bit hash is used instead.
da: 2^128 bits.
db: Assuming a message that has the same hash
appears 50% of the way through;
(2^127)/(2^20) seconds, ~~ longer then the
universe has been around times 3..

Q-3-) Use *Trapdoor Oneway Function* with following secrets as described in lecture notes to encrypt plaintext P = '0101 0111'. Decrypt the resulting ciphertext to obtain the plaintext P back. Show each step to get full credit.

S = {5, 9, 21, 45, 103, 215, 450, 946}
a = 1019, p = 1999

Message = '0101 0111' = 87 in decimal
Calculate sequence based off S:

First, q = 1999, r = 1019

Public Keys = (Si * r) mod q
k1 = (5*1019)mod1999 = 1097
k2 = (9*1019)mod1999 = 1175
k3 = (21*1019)mod1999 = 1409
k3 = (45*1019)mod1999 = 1877
k4 = (103*1019)mod1999 = 1009
k5 = (215*1019)mod1999 = 1194
k6 = (450*1019)mod1999 = 779
k7 = (946*1019)mod1999 = 456
This sequence is our public key

Now we take each bit, and multiply to their respective key.
= 0 * 1097
+ 1 * 1175
+ 0 * 1409
+ 1 * 1877
+ 0 * 1009
+ 1 * 1194
+ 1 * 779
+ 1 * 456
= 5481

To decyrpt, we take the modular inverse of 1019mod1999, which is 1589, and multiply it by our value modulus q.
= (5481*1589)mod1999 = 1665 .
We then take the largest element we have in S and work down to 0 from 1665.
1665 - 946 = 720
720 - 450 = 270
270 - 215 = 55
55 - 45. = 10
10 - 9 = 1
1remainder.
The positions of the values we used are our 1 bits.
This corresponds to a binary string of '0101 0111',
which is equal to our original messaage