**Final Exam Review**

***Review and Preparation Instructions***

80% of contents are from Chapter 9, 10, 11, 12, 13, 14 and 15

20 % of contents are comprehensive

Do the concepts and algorithms given below

Read text and then review via ppt

Finish assignments and submit to get partial credits if not done yet

***Exam Instructions:***

*3 hours test conducted in BB*

*click save button after each problem in BB*

*open book and notes*

*each student get his/her own set of problems, generated by the system*

*Exam format – True/False, Multiple Choices, and calculation and reasoning*

**Part I: review Concepts**

*Note: also review concepts given in the mid-term review sheet*

*Note it is no way a complete list of concepts*

1. Asymmetrical cryptographic algorithms
2. Public key
3. Private key
4. Public key cryptosystem
5. RSA
6. One way function
7. Hash
8. Cryptographic hash
9. Key Exchange
10. Digital Signature
11. Diffie-Hellman key exchange
12. Man in the middle attack
13. MD4
14. SHA
15. Collision
16. Message authentication
17. MAC
18. KDC
19. Master key
20. Nonce
21. Public key certificate
22. Key management
23. Key distribution
24. X.509 Certificate
25. Kerberos
26. Mutual authentication
27. Identity management
28. Registration authority
29. Time stamp
30. Verifier

**Part II: Calculation and reasoning**

1. In the RSA scheme, the steps are
   1. Select prime number p and q such that p is not equal to q
   2. define n as the product of the two numbers, that is, n = pq
   3. calculate φ(n) = (p – 1)(q – 1)
   4. select integer e such that φ(n) and e are relatively prime
   5. find d such at de = 1 mod φ(n), where de is the product of d and e
   6. for any given plain-text, the cipher-text is C = M mod n
   7. for any cipher-text C, the plain-text is M = C mod n

Performing encryption and decryption using RSA algorithm for

1. p=11, q=13, e = 11, M=7 and
2. p = 17, q=31. E=7, M=2
3. The purpose of Diffie-Hellman key exchange algorithm is to enable two users to exchange a key securely that can be used for subsequent encryption of message.

For example, if Alice and Bob agree on a public prime *p* and primitive root *g* modulo *p*, the algorithm tells

* 1. Alice chooses a random value **x and** sends **gx mod p** to Bob
  2. Bob chooses a random value **y** and sends **gy mod p** to Alice
  3. Alice computes **gyx mod p as (gymod p)x mod p** to get the shared secret
  4. Bob computes **gxy mod p** as **(gxmod p)y mod p** to get the same secret

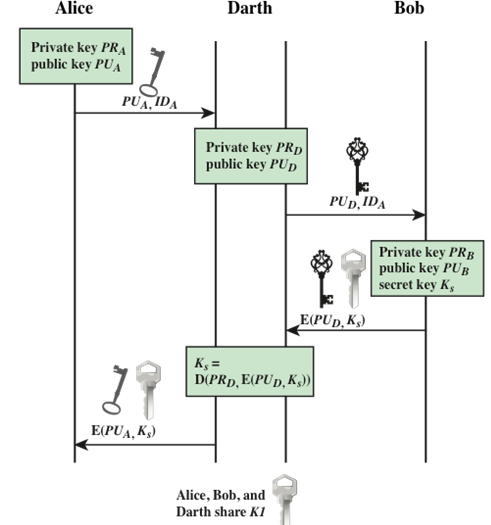
Performing Diffie-Hellman key exchange, q=71, a = 7.

If user A has private key Xa = 5 what is A’s public key?

If user B has private key Xb = 12,

What is B’s public key? What is the shared secret key?

1. Describe man in the middle attach in the following scenario.



1. Describe the public key distribution sequence

