# Problem Session CMPE-553 “Cryptography and Network Security” 21.05.2018

Chapter 9. RSA

9.2. Perform encryption and decryption using RSA algorithm for the following

a. p=3, q=11, e=7, M=5

b. p=5, q=11, e=3, M=9

c. p=7, q=11, e=17, M=8

d. p=17, q=31, e=11, M=7

e. p=17, q=31, e=7, M=2



9.3. In a public-key system using RSA, you intercept the ciphertext C=10 sent for a user whose public key is e=5, n=35. What is the plaintext M?

M=5

9.4. In an RSA system, the public key of a given user is e=31, n=3599. What is the private key of the user?

D=3031

Chapter 10. Key Management

10.1. Users A and B use the Diffie-Hellman key exchange technique a common prime q=71 and a primitive root a=7.

a. if user A has private key XA=5 what is A’s public key YA?

b. if user B has private key XB=12 what is A’s public key YB?



10.2. Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root a=2.

a. show that 2 is a primitive root of 11

b. if user A has public key YA=9, what is A’s private key XA?

c. If user B has public key YB=3, what is the shared secret key K?



10.4. In 1985, T. ElGamal announced a public-key scheme based on discrete logarithms, closely related to the Diffie-Hellman technique. As with Diffie-Hellman, the global elements of the ElGamal scheme are a prime number q and *a*,a primitive root of q. A user A selects a private key XA and calculates a public key YA as in Diffie-Hellman. User A encrypts a plaintext M<q intended for user B as follows:

1. Choose a random integer k such that 1<=k<q

2. Compute K=(YB)k(modq)

3. Encrypt M as the pair of integers (C1, C2) where

C1=ak(modq), C2=KM(modq)

User B recovers the plaintext as follows:

1. Compute K=(C1)XB(modq)
2. Compute M=(C2\*K-1)modq

Show that the system works; that is, show that the decryption process does recover the plaintext.



10.5. Consider an ElGamal scheme with a common prime q=71 and a primitive root a=7.

a. If B has public key YB=3 and A chooses the random integer k=2, what is the ciphertext of M=30?

b. If now A chooses a different value of k, so that the encoding of M=30 is C=(59, C2), what is the integer C2?

