CSC 439-01/539-02 Advanced Information Security
Spring 2013

Sample Questions for Module 1 – Number Theory and Public-key Cryptography

1) What cryptographic techniques/ algorithms are typically used to provide: (i) Confidentiality, (ii) Integrity, (iii) Non-repudiation, and (iv) Authentication?

2) Compute 7^{69} mod 8 using the Right-to-Left binary algorithm. Determine the number of multiplications made.

3) Find the multiplicative inverse of 83 modulo 65 using the Extended Euclid algorithm.

4) RSA Algorithm: Let p = 13 and q = 17. Your encryption key *e* has to be at least 10 such that *e* is relatively prime to (p-1)*(q-1).
a) Find the encryption and decryption keys.
b) Show the encryption for plaintext 8.
c) Show the decryption for ciphertext 6.

5) RSA Algorithm: Let p = 23 and q = 29. Your encryption key *e* has to be at least 10 such that *e* is relatively prime to (p-1)*(q-1).
a) Find the encryption and decryption keys.
b) Show the encryption for plaintext 18.
c) Show the decryption for ciphertext 16.

6) Diffie-Hellman Key Exchange: Alice and Bob have to agree on a secret key. They start with by agreeing on the field size 45 and the integer g to be 10. Alice generates the secret integer a 5 and Bob generates the secret integer 7. What would be the secret key thy will be agreeing with.

7) Explain how would you distribute a secret key between two users using public-key encryption so that both confidentiality and integrity can be obtained?

8) Considering encrypting a message in the following two orders sent from sender S to receiver R. Discuss whether each of these two provide both confidentiality, integrity and authentication. Justify.

(i) Epub-key-R (Epri-key-S (M))
(ii) Epri-key-S (Epub-key-R (M))

9) In an organization comprising of 100 users, what would be the maximum number of keys needed in the case of symmetric encryption and in the case of public-key encryption?

10) List and explain at least three major differences between symmetric encryption and public-key encryption.