CSC 437/539 Computer Security, Fall 2013
Module 2: Cryptographic Tools
Instructor: Dr. Natarajan Meghanathan

Question Bank

1) What is the difference between cryptanalytic attacks and brute force attacks on symmetric ciphers? How are they typically launched?

2) If the key size for a symmetric cipher is 128 bits, how long on average it would take to break the cipher using a brute force approach. Assume the computing capacity of the machine that does the cryptanalysis is 1000 decryptions per μs.

3) What are two key differences between block ciphers and stream ciphers based on their operating principles?

4) Briefly explain the working of the Triple DES algorithm that uses three keys, each of size 56 bits. Compare the cryptanalytic strength of this Triple DES algorithm compared to a block cipher algorithm that uses a key of size 168 bits.

5) Write the equations that characterize a round of the DES algorithm with respect to both encryption and decryption. Draw a flow diagram that illustrates the structure and working of a DES cycle.

6) How is the Cipher Block Chaining (CBC) method used to generate the message authentication code (MAC) for a plaintext? Explain briefly in words as well as with a diagram. Explain how any corruption in the plaintext (that is sent along with its MAC) can lead to the Avalanche Effect.

7) What is the idea behind the use of a pseudo random number generator in conjunction with a stream cipher, rather than just using one single secret key?

8) How can you do message authentication using one-way hash function and:

(i) Symmetric encryption
(ii) Public-key encryption
(iii) Without any encryption

Explain your answer either through a diagram or in words (in detail).

9) Explain the following properties of a hash function:

(i) One-way property
(ii) Weak-collision resistant
(iii) Strong-collision resistant

10) Briefly explain two other uses of secure hash functions other than their use for message and source authentication.

11) Under what scenarios you would use: (i) Public-key encryption and (ii) Symmetric key encryption.

12) Briefly explain how would use public-key encryption (do not use certificates) to transmit a message and guarantee:

(i) Confidentiality only
(ii) Integrity and Authentication only
(iii) All the three: Confidentiality, Integrity and Authentication

13) Briefly explain the Man-in-the-Middle attack and a cryptographic solution for it.

14) What are the constituents of a public-key certificate? What is the principle used to validate its authenticity?

15) Redo Question 12 (all the three scenarios) using public-key certificates.

16) How does the public-key certificate scheme work if the sender and receiver are not trusting the same CA? Explain with an example.

17) What are the three classes of public-key certificates and when/how are they used?

18) What is the idea behind a digital envelope? Explain with an example.

19) What are the different approaches for key distribution that you studied in this course? Briefly explain them.

20) Assume a message needs to be encrypted on the fly with a secret key that is randomly generated at the sender side. Explain how the sender can package the original message as well as its secret key so that the receiver can obtain them and be able to decrypt the message without any loss of confidentiality, integrity and authentication.

21) Explain the sequence of steps for the Needham-Schroeder protocol in words or through a flow diagram. Explain how it will work in case the KDC is not in the same trusted domain of the sender and the receiver.

22) How would you distribute the public keys (of other users) and a secret session key using an online public-key authority? Explain the sequence of steps using a diagram or in words.

23) Compute 5^{41} mod 9 using the right-to-left binary exponentiation algorithm.

24) Diffie-Hellman Key Exchange: Assume the secret integers used by Alice and Bob to be 15 and 29 respectively. The values of g and n are 13 and 45 respectively. What would be the secret key they will be agreeing with?

25) Explain how PGP provides the following (using words, in detail or through a diagram):

(i) Authentication
(ii) Confidentiality
(iii) Confidentiality and Authentication

26) Explain the sequence of steps that you would do to package a message under the S/MIME standard at the sender side as well as to unpack it at the receiver side.

27) Explain the use of nonce with an example, illustrating its purpose with respect to remote user authentication during key distribution.