CSC 438/539 Systems and Software Security
Spring 2014
Instructor: Dr. Natarajan Meghanathan

Question Bank for Module 1 - Cryptography

1) Match the following security services to the mechanisms that are used to provide them:
Services: Confidentiality, Integrity, Entity Authentication, Message Authentication, Non-repudiation
Mechanisms: Encryption/Decryption, Digital Signature, Hashing, Notarization

2) Differentiate between Cryptography and Steganography. What are their pros and cons?

3) If an encryption algorithm uses 128 bits for the key, what is the average time it takes for a cryptanalyst to break the algorithm and determine the key using an exhaustive search on a supercomputer that crunches out 10^4 decryptions per second?

4) What is the difference between confusion and diffusion? Which kind of ciphers produce each of these and why?

5) Consider a ciphertext (in English) obtained using a classical cipher that is either entirely substitution or permutation-based. What technique and how would you use it to identify whether the ciphertext was obtained using a substitution or permutation-based cipher?

6) Explain why shorter messages (rather than larger messages) are more secure with substitution-based encryption algorithms?

7) Compare Caesar Cipher and Vigenere Cipher in the order of the magnitude of the confusion they create.

8) a) Given the plaintext "THIS IS A GOOD CLASS", determine the ciphertext by applying Caesar Cipher using the integer key 5.

b) Given the ciphertext "wi xkwo sc bkt", determine the plaintext by applying Caesar Cipher using the integer key 10.

9) Given the ciphertext "eua gtj o gxk muuj hajjoky", what would be the plaintext if the algorithm used is Caesar Cipher? Note you should proceed from a cryptanalyst point of view by considering various possibilities of monograms, digrams and trigrams. You should not take the brute-force approach. Show all your steps.

10) a) Use Vigenere Cipher to encrypt the plaintext "THIS IS NOT A VERY HARD COURSE" using the key string "SECURITY". Show your steps to arrive at the Ciphertext. Do not consider the blank spaces during encryption.
b) Use Vigenere Cipher to decrypt the ciphertext "llgwfckqwlcmxwhbeevbzvbr" using the key string "SECURITY". Show your steps to arrive at the plaintext

11) Consider the cryptanalysis of Book Cipher discussed in class. Let the ciphertext be "vafivxrsgflgtvsvlrg" and the key string be "IAMIEXISTTHATISCERT".
   a) Determine the plaintext
   b) In the plaintext that you obtained in (a), the probability that a given character in the plaintext is any one of A, T, N or I is more than 50%. Similarly, the probability that a given character in the given key string is any one of A, T, N or I is more than 50%. Construct a sub-table of the Vigenere table that lists the intersections between these four characters.
   c) Using the constructed table in (b) and the ciphertext given in the problem statement, try to predict the different possible characters in the plaintext. Compare the predicted plaintext characters with the plaintext obtained in (a). Determine the percentage correctness in the predictions.

12) a) Consider encrypting the plaintext "NOWADAYS IT DOES NOT COST TOO MUCH TO MAKE INTERNATIONAL PHONE CALLS" using columnar transposition. If the agreed upon key string is "PLANET", what would be the ciphertext. Show your transposition table. Use 'X' as the filler character to complete the table.
   b) Consider decrypting the ciphertext "NPARACXOYHOUUSELRKLCXHTSWQSSSUDESEX" obtained using the key string "ROBOT" and columnar transposition. The ciphertext character 'X' is used as a filler character in the transposition table. Show the transposition table and write down the plaintext.

13) For a cycle j in DES Encryption, if R_{j-1}, L_{j-1} and key K_j are the inputs, how would your represent the outputs L_j and R_j in terms of the inputs? Similarly for a cycle j in DES Decryption, how would you represent the outputs L_{j-1} and R_{j-1} in terms of the inputs L_j, R_j and key K_j.

14) Suppose the DES *f* function maps every 32-bit input R (regardless of the value of the input K) to 32-bit string of 1s. Given that the input to a round j is Lj-1 and Rj-1, determine what would DES compute after every two rounds and after every four rounds? [Hint: Use the XOR properties – $A \oplus A = 0$; $A \oplus 1 = A'$; $A \oplus 0 = A$]

15) Explain the Meet-in-the-Middle cryptanalysis attack possible on Double DES?

16) Why is the worst-case time complexity of executing a "Known Plaintext" attack on a 112-bit key Double DES is $O(2^{56})$ and not $O(2^{112})$? Explain.

17) 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.

18) Explain the following properties of a hash function:
    (i) One-way property
    (ii) Weak-collision resistant
    (iii) Strong-collision resistant

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

20) Compare and contrast symmetric encryption and asymmetric encryption with respect to the following:
    a. Number of keys
    b. Protection of key
    c. Best uses
    d. Key distribution
    e. Speed

21) RSA Algorithm: Let the encryption and decryption keys are both (11, 143) and (11, 143). Show the encryption and decryption for Plaintext 7.

22) Let (e, n) and (d, n) be the encryption and decryption keys of the RSA algorithm. How are they related to each other and what makes RSA difficult to break?

23) 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? Just show the work at either of the two sides.

24) Let K_{PUB-S}, K_{PRI-S} denote the public and private keys of Sender S. Similarly, let K_{PUB-R} and K_{PRI-R} be the public and private key of Receiver R. Let M be the secret message to be sent from S to R. Which of the following two transmissions would provide both confidentiality and message authentication and why? Which scheme would also be more vulnerable to cryptanalysis?
(i) E (K_{PUB-R} E(K_{PRI-S}, M))
(ii) E (K_{PRI-S} E(K_{PUB-R}, M))

25) Consider a message M. Using public-key encryption (along with any symmetric-key encryption, if needed), how would you send it from a source S to a destination D so that you can provide each of the following. Also, explain the order in which the receiver would unpack the message.
a) Confidentiality b) Integrity and Authentication c) All the three.

26) Briefly explain the Man-in-the-Middle attack and the use of a cryptographic solution to prevent it.

27) Consider the following structure of an encrypted message. Explain the sequence of steps that would be needed to decrypt the message.