CSC 541 Cryptography and Network Security
Instructor: Dr. Natarajan Meghanathan, Fall 2015

Sample Questions

Module 0: Introduction

1) Distinguish between passive attacks and active attacks. What are the various forms of these two attacks? Briefly explain.

2) Distinguish between cryptography and steganography and explain the tradeoff.

3) Define the following terms:
a) Non-repudiation
b) Message authentication
c) Digital signature
d) Hashing
e) Notarization

Module 1: Classical Symmetric Ciphers

1) 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?
2) What is the difference between a "Known-Plaintext" attack and a "Chosen-Plaintext" attack? Which one is more easy and beneficial from a cryptanalyst point of view and why? Justify your answer.
3) Explain why shorter messages are more secure with substitution-based encryption algorithms?
4) Rank the following four substitution ciphers in the order of the magnitude of confusion they create. Justify your answer.

(a) Caesar Cipher
(b) Vigenere Cipher
(c) Vernam Cipher
(d) Monalphabetic Cipher

5) 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.

6) 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.

7) 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

8) 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.

9) 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.

10) How would you test a piece of ciphertext to determine quickly if it was likely the result of a simple substitution or permutation?

11) Even though the Monoalphabetic Cipher has a search space of 26! keys under a brute-force attack, explain why it is highly vulnerable to cryptanalytic attacks?

12) Consider a one-time pad version of the Vigenere Cipher that uses a key comprising of a stream of random numbers between 0 and 25 (inclusive). For example, if the key stream is 5 21 3 …, then the first letter of the plaintext is encrypted with a shift of 5 letters, the second with a shift of 21 letters, the third with a shift of 3 letters and so on.

a) Encrypt the plaintext "SEND MORE MONEY" using the key stream

9 0 1 8 9 7 23 14 15 21 11 2 23

b) Decrypt the ciphertext obtained in (a) using an appropriate key stream so that the plaintext obtained is "CASH NOT NEEDED"

13) Compare and contrast stream ciphers and block ciphers with respect to the following:

a. Speed of transformation
b. Error propagation
c. Diffusion
d. Susceptibility to malicious insertions/ modifications

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

15) Explain how the Cipher Block Chaining method can be used to check for the "integrity" of the data.

16) What are the limitations of the Cipher Block Chaining method?

Module 2: Advanced Symmetric Ciphers
Instructor: Dr. Natarajan Meghanathan

Data Encryption Standard (DES)

1) Explain the Meet-in-the-Middle cryptanalysis attack possible on Double DES and discuss its worst-case time complexity?
2) 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.
3) Illustrate the sequence of encryption and decryption conducted in Triple DES.
4) What are "semi-weak" keys in the context of DES?
5) Explain the scenarios under which you would refer to a key as a "weak" key in the context of DES.
6) What is the weakness of DES with respect to ones-complement?
7) 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. Also, draw a high-level diagram illustrating a DES cycle, showing the substitution and permutation boxes involved.
8) Derive the 32-bit output for the 48-bit input using the S-Box table given in the lecture slides:

48-bit input

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	1	1	0	1	0	0	1	1	1	1	0	0	1	0	1	0	1	0	1	0	0	0	1

25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
1	1	0	1	1	1	0	0	0	1	0	0	1	0	1	0	0	1	1	1	0	0	0	1

	6-bit input	Row value	Column value	S-box result	4-bit output
S-Box S1					
S-Box S2					
S-Box S3					
S-Box S4					
S-Box S5					
S-Box S6					
S-Box S7					
S-Box S8					

32-bit output

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

9) Consider the 48-bit input given in Question 1. Invert the leftmost bit of each of the eight 6-bit input blocks. By "invert", what I mean is that if the leftmost bit is a 0, change it to 1 and if the leftmost bit is a 1, change it to 0.
a) Determine the 4-bit output from each of the eight S-boxes and find your 32-bit output.

b) Determine what fraction of your 32-bit output is different from the 32-bit output obtained in Question 1.

10) Use the bit-wise complement property of DES to prove that the key search space for 56-bit key-based DES in a chosen plaintext attack is $O(2^{55})$ and not $O(2^{56})$.

11) 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 – $A \oplus A = 0$; $A \oplus 1 = A'$; $A \oplus 0 = A$]

Advanced Encryption Standard (AES)

1) Determine the expanded key length (in terms of the number of words) for AES when we use key of length: (a) 128-bits, (b) 192-bits and (c) 256-bits.

2) Given the following state array (in hex.) for an AES encryption round, perform the Sub Bytes step followed by the Shift Rows Step and write the output array (in hex.)

41	5a	6b	7c
9c	3d	4a	90
12	23	5e	4b
3c	2a	4d	2f

3) Use the output array of Q2 as the input array for an AES decryption round to perform the Inverse Shift Rows step followed by the Inverse Sub Bytes step and write the resulting state array.

4) Show the steps to determine the third value of the product vector of the AES Mix Columns step of the following column vector of a state array

$$\begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix}$$

5) Show the steps to determine the first value of the product vector of the AES Inverse Mix Columns step of the following column vector of a state array

$$\begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix}$$

6) Perform addition and multiplication of (5a) and (b3) using the $GF(2^8)$ arithmetic.

7) Explain the differences between DES and AES with respect to input processing, encryption and decryption, and avalanche effect.

Module 3: Number Theory and RSA Public Key Encryption

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

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

3) 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.

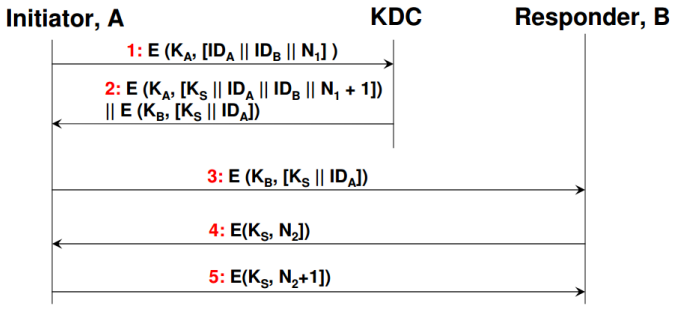
4) RSA Algorithm: Let p = 23 and q = 29. Your encryption key *e* has to be at least 10 such that *e* is relatively prime to (p-1)*(q-1).
a) Find the encryption and decryption keys.
b) Show the encryption for plaintext 18.
c) Show the decryption for ciphertext 16.

5) 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?

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

Module 4: Key Distribution and Management

1) Consider the Needham Schroeder Protocol. Answer the following:



a) How does the initiator A authenticate that it is receiving the session key from the KDC? Explain.
b) What are the two ways the responder B is getting convinced that the session initiator is A?
c) Can the initiator decrypt message (3) forwarded to the responder? Why or why not?

2) Find the primitive root of prime integer 29. The candidates are: {7, 10, 11}.

3) Diffie-Hellman Key Exchange: Let n = 31.
a) Find a suitable value for the parameter g.
b) Select suitable values for the private keys for users Alice (a) and Bob (b). Compute the intermediate key value sent by Alice to Bob and the intermediate key value sent by Bob to Alice.
c) Compute the final secret key arrived at by Bob based on the intermediate key value received from Alice.
d) Compute the final secret key arrived at by Alice based on the intermediate key value received from Bob.
e) Show the global view computation of the secret key.

4) Explain the Man-in-the-Middle attack on Diffie-Hellman Key exchange. Explain how the Station-to-Station protocol fixes the vulnerability leading to the attack.

5) What are the components of a public-key certificate? How is the notion of "trust" used in the context of a public-key certificate?

6) What are the different classes of public-key certificates? Explain with an example for each class.

7) Assume users A and B are in the same network and both of them trust a certificate authority CA. Let the public-key certificate obtained by user A from the CA be represented simply as PUB-CERT-A and this public-key certificate should be seen only by user B and not visible to anybody else. Explain how you would send a message M from user A to user B for each of the following cases:

a) User B needs to make sure the message came from user A and not anybody else.
b) User B needs to make sure that the integrity of the message was maintained during transmission.
c) User B needs to make sure both (a) and (b) simultaneously.

8) Assume users A and B in two different networks. User A owns a public-key certificate (PUB-CERT-A) that is digitally signed by a certificate authority (CA-1) whose public-key certificate (PUB-CERT-CA-1) is digitally signed by another certificate authority (CA-2). User A trusts CA-1 and User B trusts CA-2.

(a) Explain how you would send a message M from user A to user B such that it provides integrity, confidentiality and authentication.
(b) What would be the sequence of steps executed by receiver B to extract the message M?

Module 5: Data Integrity

1) Briefly explain the two key properties expected of a cryptographic hash function. Can the parity bit scheme be used as a cryptographic hash function? Why or why not?

2) If parity bit is used as the hashing scheme, explain why there is a 50% chance for being able to detect any error during transmission?

3) Consider communication channels that could be (a) prone to error during transmission or (b) reliable. Let there be two hashing algorithms H1 and H2 that produce hash value of size 32 bits and 64 bits respectively. Which of the two hashing algorithms would you prefer to use for each of the two channels? Justify your answer.

4) Consider a hashing algorithm H that generates purely random hash values of size 8 bits for any message. What is the probability for the hash function to generate the same hash value for two different messages?

5) Compute the 16-bit checksum for message: CAPITAL**.**
(ASCII chart in HEX would be provided during exam)

6) Consider a message of size 10,456 bytes and its hash value is computed using SHA-256.
(a) Draw the message generation diagram (similar to the SHA-512 provided in handout).
(b) Determine the number of blocks, the number of bits of the message in the last block as well as the size of the padding 100000…0 needed for the last block.

7) Assume you can only use a hash function H and a symmetric-key encryption algorithm that takes a secret key K. Show how would you transmit a message M from user A to user B so that the following are guaranteed: (a) Message Authentication and Integrity (b) Confidentiality (c) Message Authentication, Integrity and Confidentiality.

8) Assume you can only use a hash function H and a secret key S. Show how would you transmit a message M from user A to user B so that both message authentication and integrity are guaranteed. You should not use any encryption.

9) Assume you can only use a hash function H and public-key encryption algorithm. Show how would you transmit a message M from user A to user B so that the following are guaranteed: (a) Message Authentication and Integrity (b) Confidentiality (c) Message Authentication, Integrity and Confidentiality.

10) Assume you can use a hash function H, public-key encryption algorithm as well as a symmetric-key encryption algorithm for which the secret key K has to be generated on the fly (generated by the sender at the time of sending a message). Show how would you transmit a message M from user A to user B so that the following are guaranteed: (a) Confidentiality; (b) Message Authentication, Integrity and Confidentiality.

11) Explain how hashing is used to store and validate user passwords by operating systems as well as used for intrusion detection by anti-virus scanners?

12) Briefly explain the functioning of a Bloom Filter? Why is that there could be some false positives, but no false negatives?

13) Consider a bloom filter hash table of size 8 bits, filled as shown below.

0	1	2	3	4	5	6	7
0	1	0	0	1	0	1	0

Find the probability of obtaining a false positive if the number of hash functions used is: (i) 2 and (ii) 3. Assume each function gives a distinct hash value (in the range 0...7) for a particular word (i.e., the hash value generated by two different hash functions for the same word is different).

14) Consider the following performance curve expected of a Bloom Filter and the two regions marked A and B: (a) Why is that the probability of false positives increases with increase in the number of hash functions in region A and (b) Why is that the probability of false positives decreases with increase in the number of hash functions in region B?

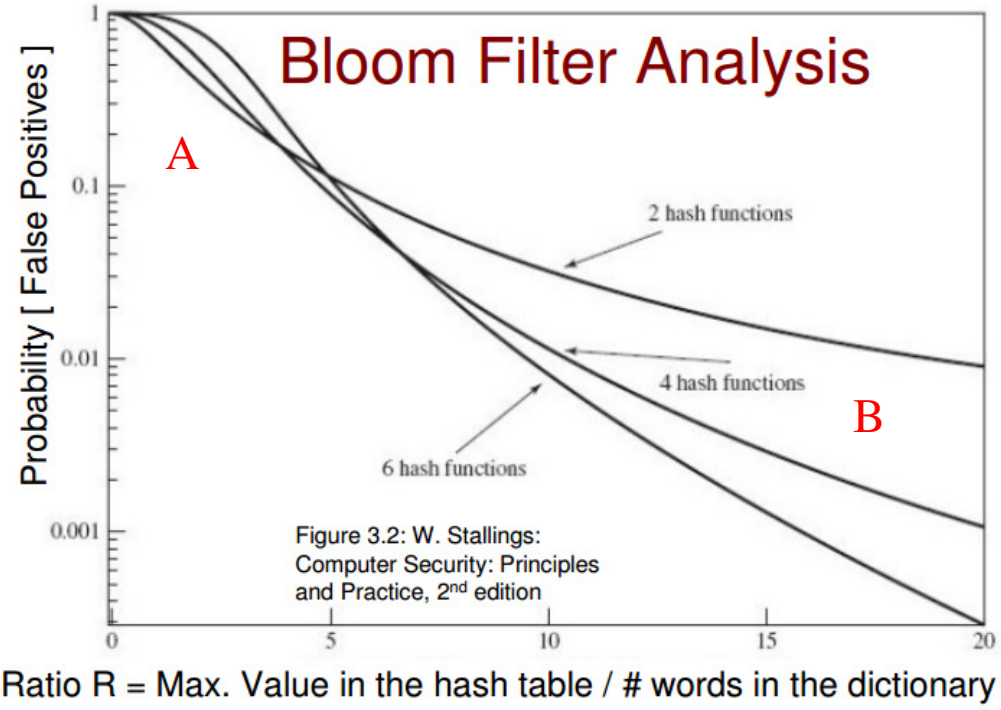


Figure 3.2: W. Stallings: Computer Security: Principles and Practice, 2nd edition

Module 6: Web Security

1) What is the impact of DNS cache poisoning on web security? Explain with an example.

2) What are the characteristics of the two types of active code models for execution at the client side? Which one do you recommend and why? Explain.

3) What are the two types of XSS attacks? Explain their basic principle as well as the difference between the two attacks.

4) Briefly explain using an example [you need not explain with the actual code for php; however use the java script code as and when needed to explain the idea], how can the following attacks be conducted:
    a. Persistent XSS attack
    b. Non-persistent XSS attack
    c. Standalone XSRF attack
    d. XSRF attack in coordination with a persistent XSS attack

5) What could be the strategy of an attacker to make his scripting code look less obvious while launching an XSS attack?

6) What is the primary difference between XSS and XSRF attacks?

7) What is the implicit advantage in using the POST method, rather than the GET method, of data retrieval in web pages?

8) Explain the three potential solutions that were discussed in class to combat XSRF attacks.

9) Briefly explain the idea behind using the CAPTCHA kind of challenge-response authentication in websites. What is its use?

10) What are the different strategies (mention at least three in each case) one can adopt to protect against XSRF attacks: (i) as a user, (ii) as a developer.

Module 7: TCP/IP Stack and Addressing Schemes: An Overview

1) Identify whether the following belongs to class A, B, C, private or multicast addresses? If they belong to a class A, B, C address - identify whether they are network address, unicast address or broadcast address.

a) 132.14.56.0
b) 90.255.255.255
c) 172.17.45.1
d) 225.6.2.1
e) 195.34.2.0
f) 154.134.12.255

2) What is the maximum number of class A, class B and class C networks possible? Similarly, what is the maximum number of hosts per class A, class B and class C network? Make sure you consider all the special IP addresses that would eat up the address space before deciding the maximum number of networks and the maximum number of hosts per network.

3) What is the difference between a direct broadcast IP address and a limited broadcast IP address?

4) What is a private IP address? Can it be used as the destination IP address to directly route a packet over the Internet? Why or why not? Justify your answer.

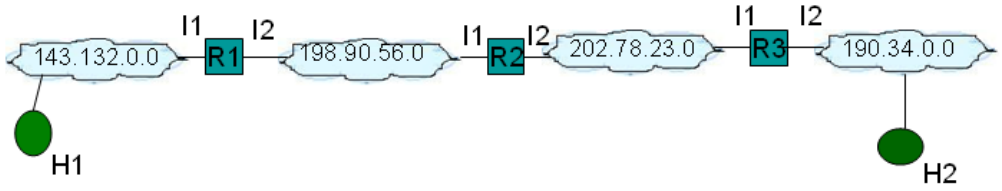
5) Define the following: (a) Datagram (b) Segment (c) Frame (d) Maximum Transmission Unit

6) What is the implicit security feature behind the "Time to Live" field in the IP header.

7) When we fragment a datagram, what headers are repeated in each fragment and what header(s) go with just one fragment? Justify your answer.

8) Give three examples of ICMP error control options and briefly explain them.

9) Consider the following internetwork:



Host/ Router	IP address	Hardware address
H1	143.132.0.1	34:12:45:AB:CD:EF
Interface 1 of R1	143.132.90.2	38:45:A9:E2:B5:C3
Interface 2 of R1	198.90.56.1	4C:9A:3B:54:DF:12
Interface 1 of R2	198.90.56.2	24:3B:1C:4A:52:CD
Interface 2 of R2	202.78.23.1	9C:12:AB:89:CF:33
Interface 1 of R3	202.78.23.2	BC:32:11:A2:45:23
Interface 2 of R3	190.34.0.1	28:12:AB:45:69:12
H2	190.34.0.2	30:90:CD:EF:AB:43

Indicate the contents (Port numbers, IP addresses, Hardware addresses) of the TCP, IP and the Frame headers as the data passes from a process (port number 1025) running at host H1 (IP address: 143.132.0.1) to a process (port number 2045) running at host H2 (IP address: 190.34.0.2). You need to show the contents at each of the hosts H1, H2 and the routers R1, R2, R3.

Contents of the frame leaving H1 and entering R1

Source H/W	Dest H/W	Source IP	Dest IP	Source Port	Dest Port	
						DATA

Contents of the frame leaving R1 and entering R2

Source H/W	Dest H/W	Source IP	Dest IP	Source Port	Dest Port	
						DATA

Contents of the frame leaving R2 and entering R3

Source H/W	Dest H/W	Source IP	Dest IP	Source Port	Dest Port	
						DATA

Contents of the frame leaving R3 and entering H2

Source H/W	Dest H/W	Source IP	Dest IP	Source Port	Dest Port	
						DATA