Final Exam

Please read the following rules before starting.

Write your name on each sheet. Helps if the staple comes undone after you turn it in.

If you are uncertain about the details of a particular problem, make any reasonable assumptions that you feel are necessary to solve it. Be sure to write down your assumptions.

You are to neither give nor receive aid on this exam. You may not show or discuss this exam paper or your solution with anyone. Please sign and turn in this exam copy with your solution to acknowledge that you have followed these rules.

PRINT NAME : ____

IIT A# : ____

SIGNATURE :____

1. (3 pts) Digital signatures can prevent messages from being:

   A. Erased

   B. Forwarded

   C. Disclosed

   D. Repudiated

2. (3 pts) What is the justification for using a message digest in digital signatures?

   A. To indicate the encryption algorithm

   B. To confirm the identity of the sender

   C. To enable transmission in a digital format

   D. To detect any alteration of the message

3. (6 pts) Suppose that a server concatenates a unique 12-bit random number as salt value for every user's password and then stores the hashed password along with the salt value in a plaintext password file.

   (i) How much harder does adding the salt make it for an attacker who obtains the password file to crack Alice's password?

   A. Not much harder at all

   B. About twice as hard as it would be without salt

   C. About 2^{12}, which is 4096 times harder than it would be without the salt.

   D. Impossible

   (ii) How much harder does the addition of salt make it for an attacker who wants to carry out offline dictionary attacks on all user passwords?

   A. Not much harder at all

   B. About twice as hard as it would be without salt

   C. About 2^{12}, which is 4096 times harder than it would be without the salt.

   D. Impossible

4. (10 pts.) Circle T (true) or F (false) for each of the following statements below

   A. (T / F) Kerberos is susceptible to man-in-the-middle attacks

   B. (T / F) In Kerberos all servers share a secret with the authentication server

   C. (T / F) The purpose of the authenticator in Kerberos is to avoid replay attacks

   D. (T / F) In Kerberos the ticket granting server shares a secret with the authentication server.

   E. (T / F) During the process of registration every entity who wishes to obtain a certificate from the CA should provide a copy of their private keys to the CA.

5. (3 points) Suppose, Alice used CBC mode to encrypt her file. However, she forgot the Initializing Vector (IV) she used. If she has the ciphertext and the key, can she still decrypt the file?

   A. No, she cannot recover anything.
   B. She can recover everything except the very first block
   C. She can recover everything except the very first block and second block
   D. She can recover only the very last block

6. (3 pts) In order to know that a one-time pad provides confidentiality, which of these do we need to assume about the adversary?

   A. Has limited computational power
   B. Does not know anything about the key
   C. Attacker cannot modify the message
   D. Attacker can intercept the message

7. (3 pts) How can anti-disassembly techniques make software reverse engineering attacks more difficult?
   A. To confuse static view of code
   B. To confuse dynamic view of code
   C. Make code check itself to detect tampering
   D. Make code more difficult to understand

8. (3 pts) Suppose Alice has K_A as private key and K_{+A} as public key. Bob has K_B as private key and K_{+B} as public key. Which of the following messages will allow Alice to send m so Bob is ensured that it was generated by Alice and no one has breached its confidentiality. Here E_{KX} (m) denotes enciphering of m by the key K_X and || denotes concatenation.

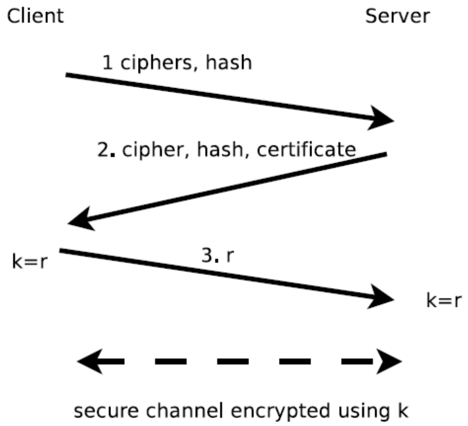
   A. E_{KA}(m) || E_{K+B} (m)

   B. E_{KB} (m) || E_{K+A}(m)

   C. E_{K+B} (E_{KA} (m))

   D. E_{KA} (E_{K+B} (m))

9. (6 pts) A communication channel is being established between a client and a server using a protocol similar to TLS as shown in the figure below. At first the client sends a hello message which includes the ciphers and hash methods it supports. Server replies with a message containing its chosen cipher and hash method, a certificate containing server's public key signed by a certificate authority's private key. The client verifies the certificate and then sends a randomly generated value r to be used as a session key.


Client
Server
1 ciphers, hash
2. cipher, hash, certificate
k=r
3. r
k=r
secure channel encrypted using k

   (i) How should the client securely send r to server? Here E_k(m) denotes enciphering of m by the key k

   A. Use a one time pad

   B. Send E_k(r) where k is a shared symmetric key

   C. Send E_{k+}(r) where k+ is server's public key

   D. Send E_{k-}(r) where k- is client's private key

(ii) Assuming that message 3 is appropriately protected. What could go wrong? (Choose all correct answers)

A. Man-in-the-Middle attacker can hijack session by replacing message 3

B. Man-in-the-Middle attacker can force client and server to settle on a weaker cipher by altering message 2

C. Eavesdropper could decrypt message 3 to learn k

D. Certificate can be altered which the client wouldn't be able to detect

10. (12 pts)

A. (4 pts) In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M? (Need to show work for partial credit)

B. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=11 and a generator g = 7. Note (a1 x a2) mod p = (a1 mod p) x (a2 mod p) (Need to show work for partial credit)

(4 pts) (i) If user A has private key X_a = 5, what is A's public key Y_a?

(4 pts) (ii) If B has a public key $Y_b = 3$, what is the secret key shared with A?

11. (6 pts) Consider a computer system with three users: Alice, Bob, and Donna. Alice owns the file “AlReport”, and Bob and Donna can read it. Donna can read and write Bob's file “BOReport”, but Alice can only read it. Only Donna can read and write her file “DOReport”. Assume that the owner of each of these files can execute it.

- Create the corresponding access control matrix.
  E.g. if a user has read/write/execution permission on a file, write as rwx
  if a user has read/write permission on a file, write as rw-
  if a user has read permission only on a file, write as r-
  if a user has no permission on a file, write as -

	AlReport	BOReport	DOReport
Alice			
Bob			
Donna			

- Donna gives Alice permission to read “DOReport”, and Alice removes Bob's ability to read “ALReport”. Show the new access control matrix.

	AlReport	BOReport	DOReport
Alice			
Bob			
Donna			

12. (12 pts) SMTP (Simple Mail Transport Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on TCP port number above 1023 for incoming connection requests. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

(4 pts) Your host in this example has IP address 172.16.1.1. Someone tries to send email from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume that a user on your host tries to send email to SMTP server on the remote system. Four typical packets for this scenario are as follows. Indicate on the Action and Rule column of the table below which packets are permitted or denied and which rule is used in each case.

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action	Rule
1	In	192.168.3.4	172.16.1.1	TCP	25		
2	Out	172.16.1.1	192.168.3.4	TCP	1234		
3	Out	172.16.1.1	192.168.3.4	TCP	25		
4	In	192.168.3.4	172.16.1.1	TCP	1357		

(4 pts) Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Typical packets are as follows:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Src Port
5	In	10.1.2.3	172.16.3.4	TCP	8080	5150
6	Out	172.16.3.4	10.1.2.3	TCP	5150	8080

Will the packet filer prevent the attack? Explain.

(4 pts) To provide more protection, the rule set from the preceding problem is modified as follows:

Apply this new rule set to the same six packets mentioned above. Indicate on the following table which packets are permitted or denied and which rule is used in each case.

Rule	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	Action
A	In	External	Internal	TCP	>1023	25	Permit
B	Out	Internal	External	TCP	25	>1023	Permit
C	Out	Internal	External	TCP	>1023	25	Permit
D	In	External	Internal	TCP	25	>1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

Packet	Action	Rule
1		
2		
3		
4		
5		
6		

13. (4 pts) Which is generally safer between a firewall with a `default deny' policy or a firewall with a `default allow' policy? Why?

14. (4 pts) How can an intrusion detection system actively respond to an attack?

15. (5 pts) Suppose a large news media named xyz.com installed a new DDOS defense system that looks at the source IP address on all incoming packets, and if it finds any IP address that accounts for more than 1% of traffic over the last hour, it installs an entry in the router that blocks all packets from that address for the next 24 hours. What can go wrong with this solution? Name three reason

16. (4 pts) What defenses are possible to prevent an organization's systems being used as intermediaries in an amplification attack?

17. (4 pts) How can you prevent SQL injection attack?

18. (4 pts) Give one example of a runtime and a compile time protection mechanism for buffer overflow?