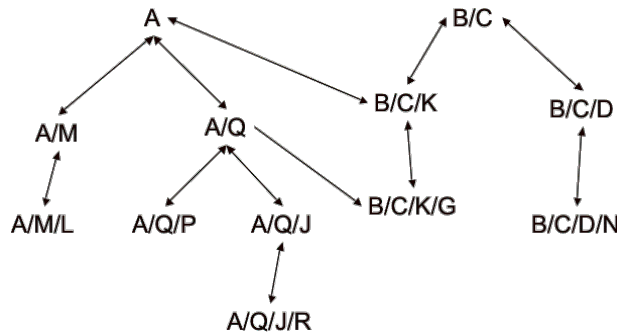


Name: _____

pp. 1

- Consider a constrained-name, bottom-up PKI, given by the picture below (all the links are bi-directional, except for the one from A/Q to $B/C/K/G$. Remember that the validation algorithm from β to γ proceeds as follows. First, it tries to find whether there is a (down, up, or cross)-link from β to any ancestor of γ . If not, the algorithm recurses on an ancestor of β .



Answer each of the following questions:

- List all ancestors of $A/Q/J/R$:

Answer: $A/Q/J/R, A/Q/J, A/Q, A$.

- List all nodes whose certificates are accepted by $A/Q/P$.

Answer: $A/Q, A/Q/J, A/Q/J/R, B/C/K/G, A, A/M, B/C/K, A/M/L$.

- Why the certificate for B/C cannot be accepted by A/Q ?

Answer: Because neither A/Q nor any ancestor of A/Q has a cross-link to B/C or to an ancestor of B/C .

- List all nodes whose certificates are accepted by $B/C/K/G$.

Answer: All nodes in this tree have certificates that are accepted by $B/C/K/G$. To see this, note that A , the ancestor of

Name: _____

pp. 2

all nodes starting with A , is certified by $B/C/K$, which is an ancestor of $B/C/K/G$. Moreover, all other nodes are descendants of B/C , which is an ancestor of $B/C/K/G$.

- d. Show the certification paths from $B/C/K/G$ to A/Q , from $A/Q/J$ to $B/C/K$, from $B/C/D/N$ to $B/C/K$, and and from B/C to A .

Answer: $B/C/K/G \rightarrow B/C/K \rightarrow A \rightarrow A/Q$.

$A/Q/J \rightarrow A/Q \rightarrow A \rightarrow B/C/K$.

$B/C/D/N \rightarrow B/C/D \rightarrow B/C \rightarrow B/C/K$.

Does not exist. B/C has no cross-links to A (or a parent of A), and no parent.

2. Answer the following questions about the Kerberos system.

- a. Suppose Alice must use an untrusted workstation to access Kerberos services. Alice enters her password at the workstation, obtaining a ticket-granting-ticket. After some time after Alice has signed in, the workstation is compromised and an intruder scans the machine memory contents. Will the intruder be able to find out what is Alice's password? Explain. Will the intruder be able to impersonate Alice for a while? explain.

Answer: The intruder will NOT recover Alice's password because the Kerberos client does not save the password after authentication. The intruder WILL be able to impersonate Alice because he can steal her TGT (ticket-granting-ticket), session key, and any valid tickets.

- b. Suppose the KDC disk crashes. The system administrator quickly substitutes the hard drive, restores the KDC database from a secure storage device, and reboots the KDC, all within half an hour. Will users that had logged in before the incident have to obtain new TGTs (ticket-granting-tickets) immediately as the server re-boots to continue to use Kerberized services? Explain.

Answer: No. Kerberos' KDC is a stateless server. The TGT tickets continue to be valid until their timestamps expire.

Name: _____

pp. 3

3. Answer with true or false, or chose the right answer among the choices.
NO NEED TO JUSTIFY YOUR ANSWERS.

a. If Alice and Bob both want to use DSA but do not wish to share the same (effective) secret key, is it correct for them to use the same prime modulus p , but generate different private exponent and public keys?

Answer: YES.

b. If Alice wishes to economize in generating good random numbers, can she re-use the “one-time” public key to sign more than one message using DSA?

Answer: NO.

c. The security of the DSA system requires that it be difficult to compute discrete logs { factor large numbers, compute discrete logs}.

d. The semantic security of the Elgamal encryption scheme against chosen plaintext { chosen plaintext, chosen ciphertext} attacks follows from the fact that the decisional Diffie-Hellman (DDH) { decisional Diffie-Hellman (DDH), Euclidean GCD} problem is hard.

4. In this question, we will use the TCP-IP model of a network as consisting of five data-path layers: Application layer, transport layer, network layer, data-link layer, and physical layer.

a. Explain why SSH, an application layer protocol, reveals more information for purposes of traffic analysis than IPSEC, a network/transport layer protocol.

Answer: All the control data of the TCP protocol (which identifies the type of application (SSH, for instance) is at a lower layer than SSH. As such, it encapsulates the SSH packets, and is visible in the clear during network transmission of SSH packets. On the other hand, IPSEC being a network layer protocol, it protects all headers and control information except those of the IP layer. However, the IP layer (being at the network level) only identifies the network nodes (i.e., source and destination machines) and not the type of application being protected.

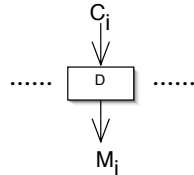
- b. Fill in the blanks: A protocol data unit (PDU) has two parts, a control/header section and a message contents/payload section. An attack that uses the information contained in the first section is called a traffic analysis attack, while an attack that seeks to reveal the contents of the second threatens the confidentiality of the communication.
- c. Describe at least two practical differences between link-to-link and end-to-end network security measures. For each difference, explain the advantages and disadvantages that it entails.
5. Kerberos' third message (from Alice to Bob) consists in sending the ticket from the Kerberos KDC and an encrypted timestamp $C = K_{AB}\{T\}$, where K_{AB} is the session key. The fact that T is the current time is the only thing stopping an adversary from re-playing the message later. Consider an attacker that wants to re-use this message. He computes the difference $X = T \oplus T'$ between the time encrypted in C (he knows that because it is the time when C was sent) and a future time T' . He wishes to xor X somewhere with the encrypted ticket containing the timestamp, hoping that it will make the ticket valid for Bob at time T' .

Consider each mode of encryption separately: ECB, CBC, CFB and OFB. Would some of them permit this attack while others prevent it? Consider separately the cases where the encrypted timestamp is the last encrypted block and where there is a block after the timestamp encrypting something recognizable by Bob. (Refer to the pictures of decryption under ECB, CBC, CFB, and OFB below.)

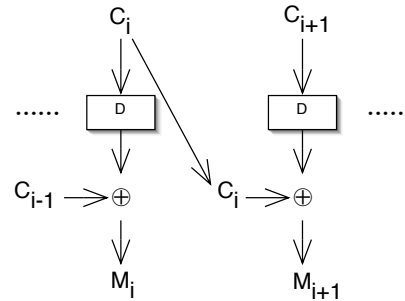
Decryption algorithms for various encryption modes:

Name: _____

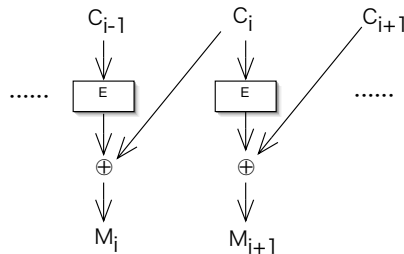
pp. 5



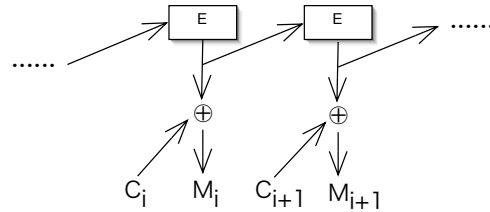
ECB decryption



CBC decryption



CFB decryption



OFB decryption

Answer: (1) Decryption in ECB mode uses the block cipher decryption function, which is like a random function. So decrypting the timestamp XORed with anything will result in a mangled decryption which will not make sense as a timestamp. So ECB is not vulnerable to this attack.

(2) Decryption in CBC also uses the decryption function. So if the attacker XORs T with the same block that encrypts the timestamp, it will be mangled in decryption. However, if the timestamp is the last block and there is a block before it, xoring into that block results in the timestamp becoming valid at the later time. This may be a detectable attack though, because the block before the timestamp will decrypt to garbage, so it is possible that Bob will recognize the attack.

(3) Decryption in CFB does not use the decryption function. If the timestamp is in the last block, XORing with X will make it valid at the future time T' , and nothing else will change so the attack is successful. On the other hand, if the timestamp is not the last block,

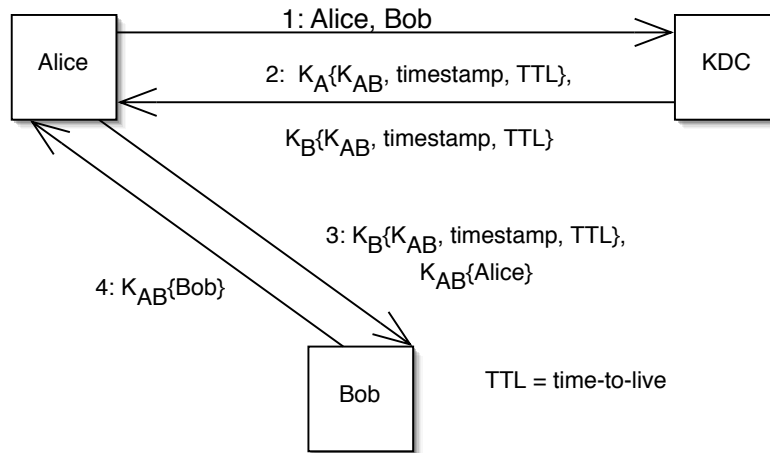
the block following the timestamping will be mangled and the attack will be detected.

(4) Decryption in OFB also does not use the decryption function. Moreover, because there is no chaining, the attack is always successful, no matter where the timestamp is positioned (as first, middle, or last block).

6. Fill in the blanks: In an attacker recovers the shared secret key, it is called a total break, while if he succeeds only in decrypting a few messages, it is a breach of confidentiality of the communication. If the attacker has only access to encrypted data for analysis, this is called a ciphertext-only attack, while if he knows some messages and their corresponding encryption, it is called a known-plaintext attack.
7. Fill in the blanks:
 - a. A session key should be random, and used for a limited number of messages/ communications, while a long-term key can be used for authentication and to establish other keys.
 - b. The initialization vector (IV) permits a sender to send the same message twice, encrypted under the same key, and have the fact remain undetected to an eavesdropper. In CBC mode, this quantity can be sent in the clear as the first block of the transmission.
 - c. Nonces/IV should never be repeated. In some cases they can be substituted by a timestamp; in other cases, they should be unpredictable values. Authentication protocols use these to prevent re-play attacks.
8. Consider the following protocol, which has as goals the establishment of a common key and mutual authentication of two parties. The protocol employs a key distribution center, and has four messages (as Kerberos). However, this protocol is quite insecure, being vulnerable to several attacks. Describe a possible attack that would compromise the security of this protocol, and how to fix the vulnerability. (Here you only have to prevent the exact attacks you describe, not to fix the protocol such that it is completely secure.)

Name: _____

pp. 7



Answer: First attack: Notice that the ticket to Bob in message (2) does not include Alice's name. If Mallory is also a system user with privileges to service Bob, she can ask for a ticket to Bob. It receives a ticket, and learns the common key K_{MB} . Then, it sends the message to service Bob claiming to be Alice. Since it can compute $K_{MB}\{\text{Alice}\}$, Bob will agree to share key K_{MB} with Mallory (thinking her to be Alice), and will grant the appropriate services. For instance, if Bob is a file server, Mallory will get all Alice's files encrypted for her (Mallory).

Prevention: To solve this problem, the name of user should be added to the ticket to the server in message (2).

Second attack: The ticket to Alice in message (2) does not include Bob's name. Let's assume that the attacker controls Alice's gateway and can intercept and change all of Alice's communication. This is not a far-fetched scenario. For instance, Alice could be connecting to some open wireless network at an airport and/or hotel lobby. The attacker could have put a fake access point, and forward the traffic to a real one (perhaps after modifying Alice's messages). Suppose also that the attacker has compromised some server "Mr. Slow" in the system, and knows the key to that service. (May be a low-importance server that is not monitored very carefully.) Then, when Alice asks for a ticket to server Bob (an important server, say the mail server), Mallory substitutes that for a request from Alice to Mr. Slow. The KDC generates tickets, and a session key K_{AS} , and returns these to Alice via

Mallory. Alice then tries to connect to server Bob, and gets the right answer $K_{AS}\{Bob\}$ from Mallory. Alice believes she is communicating to Bob using key K_{AS} . She notices no new mail (Mallory cannot communicate to Bob to get the mail, so she pretends there is no new mail), and proceeds to respond to the old mail, including some sensitive information. Mallory learns the contents of all the messages Alice is trying to send.

Prevention: To solve this problem, the name of the server should be included in the ticket to the user in message (2).

9. Compute the Elgamal encryption of message $m = 4 \pmod{23}$, where $g = 2 \pmod{23}$ and the public key of the receiver is $3 \pmod{23}$. Use random value $r = 5$.

Answer: The encryption is $(g^r, my^r) \pmod{23}$, so substituting the values we get $(2^5, 4 \cdot 3^5) \pmod{23}$. $2^5 = 32 = 9 \pmod{23}$, and $3^5 = 13 \pmod{23}$. Finally $4 \cdot 13 = 6 \pmod{23}$. So the ciphertext is:

$$(9, 6) \pmod{23}.$$