TEAM NUMBER:

NAME(S):

INDIVIDUAL/GROUP PLEDGE SIGNATURES:

CS/ECE 4457 Assignment 11 (Security)

Instructions:

- Due date/time:
  - Individual submission: Copy into your team box folder only at the start of class on Nov. 28
  - Team submission: Nov. 28 end of class; Submit completed paper copy
- Pledge:
  - Group Pledge: *On our honor as students, we have neither given nor received aid on this assignment.* (Sign above).
  - We affirm that we have only accessed course notes posted on the Course materials Web site, the textbook, and textbook Companion Web site. We have not accessed any other materials from the Web, and have not conducted Web searches with the specific intent of finding answers to these particular questions. We have not consulted answer keys. (Sign above).
  - Total number of points: 14 points

Problem 1. (2 points)

Using the RSA public key cryptosystem, if $p = 5$, $q = 11$, and public key, $e = 3$, find a private key, d that qualifies. Next, compute the cipher text corresponding to the plaintext message *hoos*. Assume that letters are represented by numeric values as follows: a = 1, b = 2, etc. [e.g., 'h' equals 8]. Encrypt *hoos* one letter at a time and give the corresponding decimal numeric values for the ciphertext.

Problem 2. (2 points)

Consider a highly simplified Diffie-Hellman exchange in which $n = 23$ and $g = 5$. Suppose that user A chooses the random number $x = 3$ and user B chooses the number $y = 7$. Find the symmetric key created between users A and B. [Hint: Compute $g^x mod(n)$ as a first step.]

For Grading Purposes:

1:	2:	3:	4:	5:	6:

Problem 3. (2 points)

Assume that Alice only trusts the root certification authority in the PKI structure shown in Fig. 1, and that she already has the public key of this root CA. Bob has obtained a certificate from certificate authority CA5.

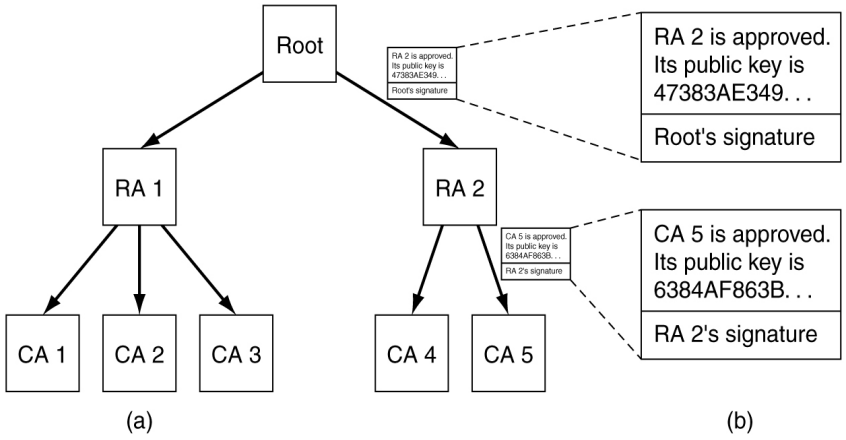


Fig. 1 Public-Key Infrastructure (PKI)

Answer the following:

a. Which entity's key is used to generate the signature contained in Bob's certificate? What type of key is used to generate the signature?

b. After Alice receives Bob's certificate from Bob, how many additional certificates does Alice need to obtain before she can trust Bob's public key? Who is the subject in each of these certificates?

Problem 4. (2 points)

Fig. 2 shows the packet filtering rules programmed in a firewall. Show whether the firewall permits or denies transit for each of the incoming datagrams, P1, P2, P3, P4, under two different orders of the firewall rules, by completing Table 1. In the order, R1, R3, R2, the first rule applied is R1, next R3, and finally R2. Use the same interpretation for the order R3, R1, R2.

Rule	Source address	Destination address	Action
R1	111.11/16	128.143.22/24	permit
R2	111.11.11/24	128.143/16	deny
R3	0.0.0.0/0	0.0.0.0/0	deny

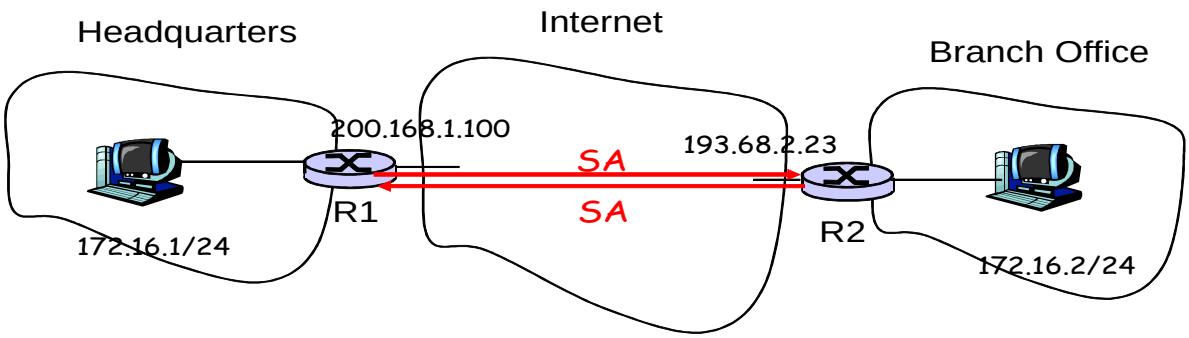
Fig. 2 Packet filtering rules programmed in a firewall

Table 1: Action performed by the firewall on incoming datagrams

Datagram	Source IP address	Destination IP address	Action under R1, R3, R2 (permit or deny)	Action under R3, R1, R2 (permit or deny)
P1	111.11.11.1	128.143.6.6		
P2	111.11.11.1	128.143.22.2		
P3	111.11.6.6	128.143.22.2		
P4	111.11.6.6	128.143.6.6		

Problem 5. (4 points)

Two (simplex) security associations (SA) are set up between R1 and R2 as shown in the figure below and are required to be applied to all datagrams sent/received in the corresponding directions between the branch office and headquarters of a company to provide confidentiality, authentication and integrity. The security policy databases at routers R1 and R2 indicate that these SAs are to be used only for datagrams between the headquarters and branch office.



True or False?

a. When a host in 172.16.1/24 sends a datagram to an Amazon.com server, the router R1 will encrypt the datagram using IPsec.

b. When a host in 172.16.1/24 sends a datagram to a host in 172.16.2/24, the router R1 will place this datagram into the payload of another IP datagram before transmitting it onto its interface to the Internet.

c. Suppose a host in 172.16.2/24 initiates a TCP connection to a Web server in 172.16.1/24. As part of this connection, all datagrams sent by R1 will have protocol number 50 in the outermost IPv4 header field.

d. What follows the ESP trailer in a datagram from R1 to R2?

e. In a datagram from a host 172.16.1.5 at Headquarters to a host in the Branch Office, what visible IP address is carried in the source address field of the datagram that arrive at Router R2?

f. What IP address does the receiving host at the Branch office see as the source address when it receives the decrypted datagram from part (e)?

g. What header, and what field in that header, allows Router R2 to determine what security operations and corresponding algorithms to apply to the received IPsec datagram from part (e)?

h. Assume that a new router R3 is added to the branch office, and an IPsec association is established between R1 and R3. Is the SA used between R1 and R3 the same as the SA used between R1 and R2?

Problem 6. (2 points)

Suppose Alice wants to communicate with Bob using symmetric key cryptography with a session key K_S. We learned how public-key cryptography can be used to distribute a session key from Alice to Bob. In this problem, we explore how a session key can be distributed without public key cryptography. This solution uses a key distribution center (KDC). The KDC is a server that shares a unique secret symmetric key with each registered user. Key K_{A-KDC} is a symmetric key shared between Alice (A) and the KDC, and key K_{B-KDC} is a symmetric key shared between Bob (B) and the KDC. The KDC selects a session key K_S upon receiving a request from a user.

The purpose of this problem is to understand how the KDC is used to obtain a session key K_S for secure communications between Alice and Bob. Draw a figure. Use three messages to distribute the session key: (i) a message from Alice to the KDC; (ii) a message from KDC to Alice; and (iii) a message from Alice to Bob.

The first message is $K_{A-KDC}(A, B)$, which means that a message consisting of identifiers A for Alice and B for Bob is encrypted with the key K_{A-KDC}. The KDC decrypts this message and interprets the message to mean that A wants a session key to communicate securely with B. Use the following symbols: K_{A-KDC}, K_{B-KDC}, K_S, A, and B. Express the second and third messages in the notation used for the first message, i.e., key followed by the contents of the message in parenthesis. Use commas to separate the parameters of the message.

a. What is the second message?

b. What is the third message?