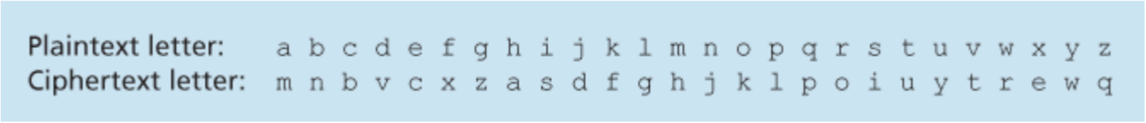
Homework assignment 5, CIS 427, Fall 2022

Firm Submission Due: 11:59 PM, 12/5/2022.

1. (15 points)
   Using the monoalphabetic cipher below, decode the message "rmij'u uamu xyj."



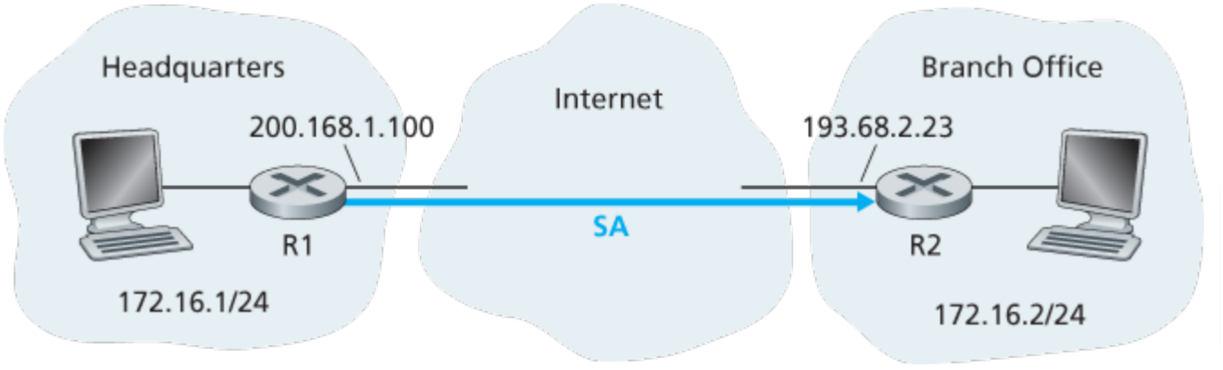
Plaintext letter:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext letter:	m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

2. (15 points)
   Can you "decrypt" a hash of a message to get the original message? Explain your answer.

3. (15 points)
   Suppose N people want to communicate with each of $N – 1$ other people using symmetric key encryption. All communication between any two people, i and j, is visible to all other people in this group of N, and no other person in this group should be able to decode their communication. How many keys are required in the system as a whole? Now suppose that public key encryption is used. How many keys are required in this case?

4. (20 points)
   Suppose Alice wants to communicate with Bob using symmetric key cryptography using a session key K*s*. We learned how public-key cryptography can be used to distribute the session key from Alice to Bob. In this problem, we explore how the session key can be distributed—without public key cryptography—using a key distribution center (KDC). The KDC is a server that shares a unique secret symmetric key with each registered user. For Alice and Bob, denote these keys by $K_{A\text{-}KDC}$ and $K_{B\text{-}KDC}$. Design a scheme that uses the KDC to distribute K*s* to Alice and Bob. Your scheme should use three messages to distribute the session key: a message from Alice to the KDC; a message from the KDC to Alice; and finally a message from Alice to Bob. The first message is $K_{A\text{-}KDC}$ (A, B). Using the notation, $K_{A\text{-}KDC}$, $K_{B\text{-}KDC}$, K*s*, A, and B, what are the 2nd and 3rd messages? Explain your answer.

5. The following T/F questions pertain to the graph below (15 points)



   1) When a host in 172.16.1/24 sends a datagram to a host in 172.16.2/24, the router R1 will change the source and destination address of the IP datagram.

2) Suppose a host in 172.16.1/24 initiates a TCP connection to a Web server in 172.16.2/24. The routers between R1 and R2 can see PORT number=80 in the TCP headers.

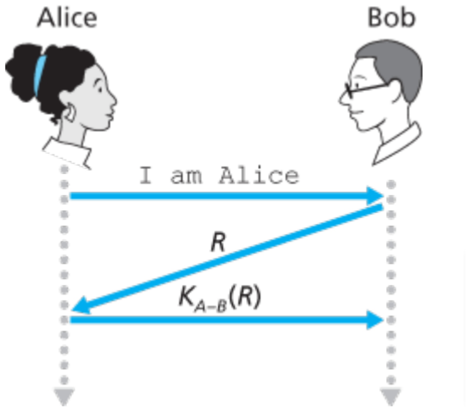
3) Consider sending a TCP segment from a host in 172.16.1/24 to a host in 172.16.2/24. Suppose the acknowledgment for this segment gets lost, so that TCP resends the segment. Because IPsec uses sequence numbers, R1 will not resend the TCP segment.

6. (20 points)

Consider an authentication protocol where Alice authenticates herself to Bob. We use K_{A-B} to denote the symmetric secret key shared by Alice and Bob. Assume Alice and Bob can add more rounds of communications but they can only use the symmetric secret key.

1) Give a new authentication protocol, in which while Alice is authenticating herself to Bob, Bob will also authenticate himself to Alice.

2) Show how to perform a man-in-the-middle attack on the new authentication protocol (i.e., Trudy, pretending to be Alice, can now authenticate herself to Bob as Alice and to Alice as Bob).


Alice
Bob
I am Alice
R
$K_{A-B}(R)$