Overview: Question 1 [7 Marks]
These are short-answer questions. Please answer in 2-4 lines and not in paragraphs. ***Explain your reasoning behind the answer.*** *Yes/no answers will not fetch you marks.*

a) If P=NP, one-time pads will not be secure any more. True or False. Justify.

b) Ceaser cipher (monoalphabetic) is vulnerable to chosen plain-text attack. True or false? Justify.

c) In RSA, for n=35 and e=7, what is d?

d) In which cipher block mode is decryption faster than encryption. Why?

e) In a system with N entities, what is the minimum number of keys required if communication among these entities must be kept secret from intruders *apart* from these N entities? Which type/model of cryptography achieves this?

f) In SSL, what is the advantage of session resume over creating a new session?

g) In class, we saw how to authenticate the server to the client in SSL. How can mutual authentication happen within the same framework?

Question 2: Block Cipher [3 Marks]

Let $m_1, m_2, \ldots, m_t$ be a sequence of t plaintext blocks. Hacker Hakim is bored with the modes he saw in class and wants to invent one of his own. He defines a sequence of $t + 2$ ciphertext blocks $c_0, c_1, c_2, \ldots, c_t, c_{t+1}$ which satisfies the equation $\mathrm{c}_i = E_k(c_{i-1} \oplus m_i \oplus c_{i+1})$, for $i = 1, \ldots, t$.

a) Hakim was having trouble figuring out how to compute the c_i's because of the circular dependencies. Please help him by showing how to compute c_{i+1} from c_{i-1}, c_i, and m_i, where $1 \leq i \leq t$. How should he choose $c0$ and $c1$?

b) Describe how to reconstruct $m_1, \ldots, m_t$ given $c_0, \ldots, c_{t+1}$.

Question 3: Cryptography Building Blocks [6 Marks]

Suppose A wants to send a message M to B. A wants to ensure integrity and authenticity (not confidentiality) of the message. Which of the following options meet this objective? Justify. You can ignore freshness concerns (i.e. replay attacks). The terminology is same as followed in class.

a) A sends $E_{B,pu}$ (M) to B

b) A sends { M, $E_{A,pr}$(M) } to B

c) A sends { M, $E_{B,pu}$(k), MAC_k(M) } to B; k is a newly chosen symmetric key

d) A sends { M, $E_{B,pu}$(k), MAC_k(M), $E_{A,pr}$(k) } to B; k is a newly chosen symmetric key

Suppose now A wants to ensure confidentiality in addition to integrity and authenticity of the message. Which of the following options meet this objective? You can ignore freshness concerns (i.e. replay attacks).

a) $E_{B,pu}(M)$, $E_{A,pr}(B,pu)$

b) $E_{B,pu}(M)$, $E_{A,pr}(M)$

c) $E_{B,pu}(E_{A,pr}(M))$

e) $E_{B,pu}(k)$, $E_k(M)$, $E_{B,pu}(E_{A,pr}(k))$, k is a newly chosen symmetric key

Question 4: Passwords [4 Marks]
LinkedIn experienced a major data breach in June 2012 where 6.5 million email-addresses and passwords were compromised. Unsalted password hashes were supposedly the culprit.
In unsalted version, the database maintained records containing two fields [user-email, hash(password)]. In salted version, it maintains three fields [user-email, salt, hash(password|salt)].

a) Suppose an attacker got hold of the database records and his main goal is to break *your* password via a dictionary attack. Does the lack of salting in LinkedIn's scheme make this goal substantially easier? Justify. A dictionary attack is based on trying all the strings in a pre-arranged listing, typically popular passwords, often derived from a list of words such as in a dictionary.

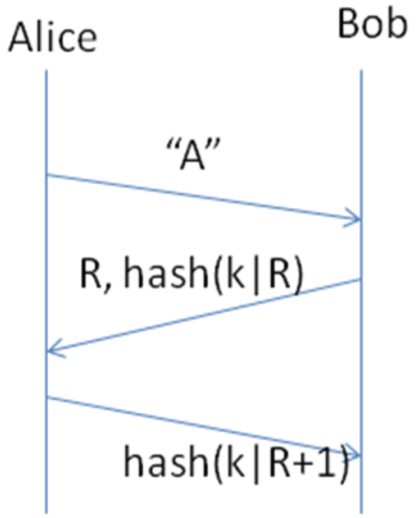
b) Suppose the attacker's goal is to break at least half of the passwords in the database via a dictionary attack. Does the lack of salting in this scheme make this goal substantially easier? Justify.

c) Suppose you are contacted by the attacker and given a set of password hashes (that's it, no user-email, no salt). Assuming the hash function is known, is there a measurement you could make in order to infer if the hashes are likely salted or not? Explain how.

d) It turns out that that roughly 20% of LinkedIn users with Yahoo Mail e-mail addresses used the same password at LinkedIn as Yahoo. You learn that, unlike LinkedIn, Yahoo salts its passwords. Should Yahoo be concerned about the LinkedIn breach or not?

Question 5: Authentication [4 Marks]

Alice and Bob wish to achieve mutual authentication based on symmetric cryptography using the the below protocol. What are the possible flaws in this protocol? Also propose how to fix the possible flaws with minimal modifications to the protocol. Justify how the modification fixes the flaw.



Question 6: More Authentication [6 Marks]

Alice and Bob wish to exchange messages with each other (bi-directional traffic) and have agreed upon a sequence K_1, K_2, . . . of shared secret keys. Each key K_i consists of a pair (a_i,b_i) so that the MAC of message M computed with key K_i is $MAC(K_i,M) = a_iM + b_i$ (mod p), where p is a publicly known large prime. Given the nature of the function, they know that each K_i should not be used to MAC more than one message.

Alice and Bob agree on the following protocol for managing their use of keys and for exchanging messages. Both parties keep track of the index t that was most recently used by either themselves or their counterparty. Thus, when Alice sends a message M, she increments her t by one and then MAC's M with key K_t. The message she sends has the format: ("Alice", "Bob", M, t, MAC (K_t, M)).

When Bob receives this message, he checks that the MAC is correctly computed for the given value of t. If it is not correct for that value of t, he ignores the message altogether. If the MAC is correct for that value of t, Bob accepts the message and sets his local value of t to be equal to the t of the received message. The same procedures are followed symmetrically (with roles switched) when Bob sends to Alice. Note, each party only maintains a single local variable t.

Marks will be based on clarity and thoroughness of the solution. So, be clear in your head before writing down the answer. Be precise and to the point.

a) Why should K_i not be used to MAC more than one message?

b) Identify as many vulnerabilities as you can in the above protocol design. You may assume that the messages sent on the channel can be controlled by an adversary i.e it can insert, delete, modify, or replay messages on the channel.

c) Propose a revised protocol that doesn’t suffer from these problems.