In=16 Feb 8:45am; Out=06 Feb; Total Marks = 150

*You may partner with up to four others (**a group of max 5**) to submit a single write up in a single group. We encourage discussion with other students in class, even if they are not in your group. Each student must build a good understanding of all the questions even if they discuss and collaborate with others. Merely dividing the problems among group members and putting those together before submission will severely impact your learning, and we **strongly advice against it**. Furthermore, **blatant copying** from online or other resources is **forbidden**. If there are confusions or questions, post those on Piazza or see your TA or Instructor.*

Submission Instructions: *You must submit a PDF on LMS in the appropriate tab. This includes hand-written content (which you may scan and upload). There will be NO late days or extentions. Please write down the names and roll numbers on a front page. Make only one submission per group.*

Question 1 [2+4 marks]

a) Describe the workings of a 51% attack and list the conditions necessary for launching a 51% attack?

b) The Tesla Company has agreed to sell Electric Vehicles in Exchange for Ethereum. Can a 51% attack be used to purchase this Electric Vehicle for free? If yes, describe how you would do this. If no, explain why this is not possible.

Question 2 [3+3 marks]

a) Alice comes up with her own digital signature scheme. She writes a message and encrypts that message using her Private key. She then sends this message and the encrypted message both to Bob. Can Bob be sure that this message came from Alice?

b) Alice modifies this scheme. She writes a message and encrypts that message with her private key (as in the previous part). She then hashes the encrypted message and sends this hash along with the original message to Bob. Can Bob be sure that this message is from Alice?

Question 3 [4+4 marks] In class we learnt that a symmetric key is often used for communication *in-bulk* i.e. when there is a lot of data that must be transferred. This is done because symmetric keys operate a lot faster than assymetric keys.

a) Assume that Alice and Bob share a secret, symmetric key. Devise a scheme with which Alice can send a plain-text message to Bob and ensure that Bob can verify the authenticity of this message.
Assume that Alice and Bob must share a LOT of data and asymmetric keys are not viable.

b) Consider a scenario in which Alice wishes to relay to Bob the message "Give me 3.50$". A malicious actor, Kevin, duplicates this message and sends it twice to Bob. According to the scheme you devised in the previous part, what will the outcome be? Further, devise a scheme in which duplicated messages are rejected.

Question 4 [5 marks] There are multiple strategies to search for the 'nonce' value in Bitcoin mining. Suggest two strategies and explain which of the two you think is more strategic.

Question 5 [5 marks] Why is the nonce field included in the block header of Bitcoin when the number of possible rearrangements of transactions in a block (there are around 2500 transactions in a block) alone provides a monumentally huge space of $2500! \approx 10^{7411}$ while a nonce can have only 2^{32} values?

Question 6 [3+2+2+2+3 marks] Consider a hash function h(x) that is publicly known and defined as:

$$h(x) = (7x^3 + 5x^2 + 11x + 13) \mod 19$$

Alice has a private key method

$$Pri(m) = (11m^3 + 7m^2 - 5m + 3) \mod 19$$

and the corresponding public key method

$$Pub(c) = (-11c^3 - 7c^2 + 5c - 3) \mod 19$$

.

(a) Given the message (47, 2), is it from Alice?
(b) What are the possible values the signature can take in this hash function?
(c) What is the minimum value that the signature can take in this hash function?
(d) Can you find two different messages that produce the same signature using the hash function? If so, provide an example.
(e) How secure is this hash function? Can you find a collision or preimage attack on this hash function?

Question 7 [4 marks] What is the distinction between symmetric and asymmetric encryption that we studied in class?

Question 8 [4 marks] Why is it needed to create a fork? Who creates the fork? On what basis do they decide if a soft fork is created or a hard one?

Question 9 [5 marks] When a soft fork is invoked, why does it need majority of nodes to upgrade to ensure that a single chain emerges?

Question 10 [5 marks] In a generic blockchain, explain the five step process that allows a user transaction to become part of the ledger? Indicate the corresponding stages in data life cycle.

Question 11 [5 marks] In Bitcoin, each user's balance is represented using the hash of a public key. A user's name or identity is not stored on the blockchain. An adversary may still use the transaction history associated with a public key in order to arrive at the identity of a user. Give an example of how this is possible and devise two strategies which may be used to protect the anonimity of a user.

Question 12 [5 marks] Read up on "Shor's algorithm". Describe how the existence of this algorithm (and similar algorithms) is harmful for the long-term security of Bitcoin-like blockchain.

Question 13 [5+5+5+5 marks] Consider as simple encryption procedure using a public/private key pair. You have the public key as the integer p=7 and the "secret" private key as the integer s=3.
The method to encrypt an integer m is: $c = m^p \mod 33$
And the method to decrypt an encrypted integer is: $m = c^s \mod 33$
Assume that the input characters have the following numerical values:
$a/A = 0, b/B = 1, c/C = 2, ..., z/Z = 25.$

a) Encrypt the word 'SurpriseQuiz' and write down the sequence of numbers.

b) Decrypt the sequence "1 2 13 29 20 2 7 20 21 16 8 16 13 28". Write down the characters and what you think of them.

Now lets consider a hashing function $h(x) = \lfloor e^x + 100 \rfloor \mod 32$ where $x \in [0, 50]$.
As $h(x)$ is defined only for one input, we will modify it to take in lists of numbers such as "31 23 4 2 13". Now, $h(31\,23\,4\,2\,13)$ will be $h((31 + 23 + 4 + 2 + 13) \mod 50)$. The idea is that every number in the list makes a contribution. Suppose Alice has the public key $p = 7$ and private key $s = 3$. Data is sent in the form "$m^1 m^2 m^3 ... m^n$ sig" where the m^i are numbers from the message and "sig" is the private key encryption of the hash of the message.

c) Suppose Alice wants to transmit the word "SaveMe". What is the final message Alice transmits?

d) You receive a message "12 20 18 19 0 5 0 17 14 2 10 18 1 0 2 7 4 18 7 14 2 10 18 5". Is this message from Alice? Why or why not? If it is a message from Alice then write the message.

Question 14 [2+2+2+2 marks] Say Rose is using the public and private keys to sign and encrypt a message to Jack. She considers two options:

1) Sign the message and then encrypt the result
2) Encrypt the message and then sign the result

a) Which is the preferable strategy (considering she doesn't want to reveal her identity) and why?

b) Continuing from above part, which key will she use for each task (i.e. signing and encrypting the message)?

c) Continuing from part **a**, if Caledon steals Rose's private key. Will he able to decipher that this message was sent by Rose? Explain your answer.

d) Rose now wants to make a public announcement that could be authenticated by anyone on the internet. Which strategy should she use to accomplish this task. It can be from the above two strategies or one of your own. Explain your answer.

Question 15 [2+4+2 marks] Alice wants to send a message to Sara and she wants to ensure that Sara can verify that this message was sent by her. So Alice takes a hash of the message and encrypts it with her private key to generate a digital signature (signature = PrivKey(hash(m))). She then sends the message along with the signature to Sara. Alice uses the following function to compute the hash:

$hash(m) = (m + 4) \mod 24$

Alice wants to send a message (integer m) to Sara. So, she computes the hash of the message and encrypts it with her private key and sends the message and signature to Sara.

a) Upon receiving this message, how will Sara verify that the message was sent by Alice and that the message has not been tampered with. Explain your answer.

b) Jack is eavesdropping on the communication between Alice and Sara. Is it possible for him to modify the message in such a way that Sara cannot detect the tampering in the message? Explain your answer with an example.

c) Ideally we would want that the signature is invalidated when the message contents change. How can we make our technique more robust to detect even the slightest of changes in the original message? Explain your answer

Question 16 [3+3+3 marks] Alice devises a hash function.

a) The only *two* outputs for this hash function are 0 and 1. The output of this hash function is random looking and has the avalanche effect. Can this function have pre-image and collision resistance? Is this function cryptographically secure?

b) Alice modifies her hash function. The output of this function is still random looking and has the avalanche effect. However, it has two bits in the output, instead of one. Can this function have pre-image and collision resistance? Is this function cryptographically secure?

c) Alice continues to modify her hash function while the function's output is still random looking and has the avalanche effect. She increases the number of bits in the output. After how many bits will you consider this hash function cryptographically secure?

Question 17 [5 marks] Read up on "Grover's algorithm". Will the existence of this algorithm (and similar algorithms) effect cryptographic hash functions such as SHA256? What about symmetric key encryption such as AES-128?

Question 18 [20 marks] There are 10 people present in a room. Each of these people have 10 stones each. These people wish to trade these stones. HOWEVER, keeping actual, physical stones and trading them is cumbersome. Devise (in great detail) a scheme in which people can keep track of the number of stones each person has without the need of physical stones. Here are some questions you must ponder:

a. How will person A transfer an imaginary stone to person B?

b. How will person A determine how many stones person C has?

c. What are the capabilities necessary for each person in you scheme? For example, they should be able to make an announcement in the room or remember details about each person etc.

d. Can your scheme fail if a fraction of the users group together maliciously? If not, why not? If so, what is the size of this fraction and how will they destroy your scheme?

Question 19 [3+2 marks]

a) What is an "oracle" in the context of blockchain?

b) Recall the example of the Indian fertilizer in class. Which entity would be an oracle in that example?

Question 20 [5 marks] ChatGPT claims that digital signatures can be used for the purposes of non-repudiation. What is non-repudiation and is it necessary for a blockchain such as Bitcoin to function properly?