Assignment 3 — DDL: 12:00, Thursday, Jun. 16 (BJT).

Q1: Consider the hash function H used for Bitcoin mining. Suppose this function has the property that its possible to find collisions. In other words, for any string s1, its possible to find another string s2 (even with certain patterns) such that H(s1) = H(s2) in about 10 hours. Show that this will lead to problems in Bitcoin security.

Q2: Suppose an adversary has found an algorithm to forge digital signatures used in Bitcoin.

That is, adversary can sign arbitrary message without having your signing key.

1) Assume you are constantly monitoring the blockchain. Can the adversary steal your Bitcoins without you being able to detect?

2) Come up with a strategy for the adversary to steal your Bitcoins so that there is no way for you to get them back (assuming you cannot forge signatures).

Q3: Bob has an idea to make Bitcoin more green and environmental friendly. Rather than wasting computational resources and electricity on solving a meaningless hash puzzle, why not solve a puzzle which is good for the society? Bob proposes that miners compete to solve hard problems in DNA sequencing. The person who mines the current block will also pick a DNA sequencing problem the next miner must solve in order to mine the next block. Is this secure?

Note: you don't need to understand what DNA sequencing is. Just think of them as some large computation scientists need to perform to understand human genes better.

Q4: Suppose that there are two forks in Bitcoin. Is it possible that both of them will be equally long and will continue to be equally long? Please explain your answer.

Q5: Suppose someone gives you an algorithm to solve the CDH problem: it takes as input g, g^a, g^b and output g^ab. Show how you can use this to break Elgamal encryption.

Q6: Consider auctions done using ElGamal Encryption. Alice is selling a Phone and has public key PK. Bob would like to Bid 100 dollars. He encrypts his bid under public key PK and sends it to Alice. Trudy is watching over the channel and sees the ciphertext. He doesn't know Bob's bid. But he would like to bid exactly double of Bob and win the auction in style. Show that this is possible in ElGamal encryption.

Class 5: proposal presentation

Every student needs to give a 3-4 min talk talk about the project problem, why it is interesting for you your plan for how you will work on the project what progress have you made so far

Project ideas:

1. proof of work vs proof of stake cryptocurrencies

2. Take any other cryptocurrencies and study that Like how Ripple works, how ETH works

3. Explore applications of digital signatures. For example, build an system for signing transcripts digitally

4. Build an encrypted chat application like WhatsApp or WeChat

5. Study a classical cipher like Enigma machine

Goal for this week: meet with your group decide a topic