COMP6451 T1 2023
Assignment 1
Total Marks: 30
Due: 17:00 March 10, 2023

Submissions: Submit your solutions as a pdf or text file via the course moodle page. Your submission must be your individual work - UNSW rules concerning this will apply (see the Course Outline). Turnitin will be used to perform similarity checks. Use of ChatGPT and other generative AI tools for this assignment is prohibited. In general, these are short answer questions — aim to keep your answers brief but precise. Answer all parts, and show your working.

Question 1 (5 marks): (Cryptographic Hash Functions) Consider the following proposal for a hash function h. Let p be a large prime and let g be a generator mod p. Represent messages as sequences x= $x_1, x_2, \ldots x_n$ where the x_i are numbers mod p. We define the hash of such a message x by $h(x) = g^{x_1+x_2+\ldots+x_n} \mod p$.

1. (2 marks) Show that this hash function is good for use as a message digest for error correction purposes, in the sense that it has a high probability of detecting errors if messages x are transmitted in the form $(x, h(x))$, and a message (x, y) that is received is treated as correct if $h(x) = y$.

   In particular, for concreteness, suppose that the messages Alice will be sending are all of length two ($x = x_1, x_2$), and are generated uniformly at random.

   Suppose also that we know that communications channel that we are using contains occasional bursts of random noise (e.g., from sunspots on a radio channel) that may potentially damage every bit of the message $(x, h(x)$, including the hash. When Alice sends a message $(x, h(x))$, with probability p, the channel delivers the message to Bob exactly as transmitted. With probability $1 - p$, the channel delivers to Bob a message (y, z) selected uniformly at random, where $y = y_1, y_2$ and y_1, y_2, z are all numbers mod p. (The channel never delivers a message to Bob if Alice did not send a message.) Bob accepts a message (y, z) that he receives as a correct transmission of a message y from Alice if $h(y) = z$, and treats it as corrupted otherwise.

If Bob receives a message and hash (y, z) and accepts it as correct, what is the probability that y is not the message sent by Alice?

2. (3 marks) Which of the three properties of cryptographic hash functions (pre-image resistant, second pre-image resistant, and collision-free) are satisfied by the function h? Explain your answers. In case you say that the property is satisfied, give reasons to believe that it is. In case you say that the property is not satisfied, give a proof that that it is not satisfied (i.e., explain how an attacker could efficiently do what the property says cannot be done efficiently).

Question 2 (5 marks): **(Digital Signatures)** Suppose that h is a hash function taking long messages as input and producing 256 bit outputs and that M is a long message. Consider the following idea for constructing a signature scheme:

- A private signature key K_s is a pair of randomly generated sequences $x_1, ..., x_{256}$ and $y_1, ..., y_{256}$, both of length 256, where each value x_i and y_i is a 256 bit message.

- The corresponding public verification key K_v is the pair of sequences $h(x_1), ..., h(x_{256})$ and $h(y_1), ..., h(y_{256})$.

- To sign message M, where the hash $h(M)$ is the sequence of bits $b_1...b_{256}$, define $sign(M, Ks) = (M, z_1...z_{256})$ where $z_i = x_i$ if $b_i = 0$ and $z_i = y_i$ if $b_i = 1$.

1. Explain how you could verify this signature is correct: what does the verification function $V(K_v, (M, r_1 \dots r_{256}))$ do to check that $(M, r_1 \dots r_{256})$ is message M signed using the signature key corresponding to K_v?

2. Explain why this scheme is secure - why is it hard for an attacker to forge a signed document that passes the test? Clarify what assumptions on the hash function are needed for your argument.

3. Is it safe to use the same private key to sign more than one message? If not, explain what an attacker could do to attack a user who does this.

Question 3 (5 marks): **(Monetary Supply Laws)** One of the ways in which currencies (both standard and crypto-) differ is in their rules concerning how money is created. Different rules have different economic consequences and incentivize users and investors in potentially complex ways. One important economic metric is the *inflation rate*, which is the annual rate at which the cost of goods and services increases. As we have experienced in recent years, the factors impacting inflation are diverse and unpredictable, and may include pandemics, wars and catastrophic weather events. However, it is clear that one of the main reasons for the presently high inflation, and its consequences on people's lives, is the amount of new money that was created by central banks during the pandemic. Central bank doctrine in recent decades has been that deflation (decreasing cost of goods over time) is bad, because people tend to hoard money rather than spend, since they know they can buy the same goods cheaper later, and this causes unemployment as the economy grids to a halt. On the other hand, nobody likes high inflation when wages are fixed. Many central banks take the view that 2-3% inflation is socially optimal.

In this question, we focus on the *monetary inflation rate* r as a proxy[1] for price inflation. For a given period, this rate is defined as $r = (M' - M)/M$, where M is the amount of money in existence at the start of the period and M' is the amount of money in existence at the end of the period.

Cryptocurrencies use a number of rules to determine how much new money is created per block. In this question, we calculate the consequences for the monetary inflation rate. Let I_k be the amount of *new* money issued in the k-th block, so that I_0 is the amount of money issued in the genesis block of the cryptocurrency. Write M_k for the total amount of money that has been issued in the first k blocks. That is, $M_k = I_0 + \ldots + I_k$. Thus, the rate of inflation in the $k+1$-th block is $r_{k+1} = (M_{k+1} - M_k)/M_k$.

(a) **(A Bitcoin-like supply law, with halving)** Suppose that $I_0 = 2^N$, and

$$I_{k+1} = \begin{cases} I_k/2 & \text{if } I_k > 1 \\ 0 & \text{otherwise} \end{cases}$$

Write a closed form solution for M_k in terms of N, and use this to derive an expression for the rate of inflation r_{k+1} in the $k+1$-th block.

(b) **(An Ethereum1.0-like supply law)** Suppose $I_{k+1} = c$, where c is a constant. Write a closed form solution for M_k in terms of I_0, and use this to derive an expression for the rate of inflation r_{k+1} in the $k+1$-th block.

(c) In case (b), what happens to r_k in the limit, as $k \to \infty$?

(d) **(A supply law that pays interest to savers/stakers)** Suppose that in each period, a fraction S of the total amount of money is saved, and new money is created by paying interest at a fixed rate R to the savers. (The interests is a reward for making available the saved money for some

[1] In practice, population growth means that the cost of goods and services can be increasing due to increased competition for limited supply, even if the money supply is fixed.

socially productive purpose. In “proof of stake” cryptocurrencies, the savers are the stakers, and the socially productive purpose is the work done by them to secure the currency.) That is $I_{k+1} = M_k SR$. Write a closed form solution for M_k in terms of I_0, and use this to derive an expression for the rate of inflation r_{k+1} in the $k+1$-th block.

(e) In case (d), what happens to r_k in the limit, as $k \to \infty$?

(Hint: one of the lecture slides shows an approach to finding a closed form, not involving a summation, for $1 + x + x^2 + \ldots + x^n$.)

Question 4 (5 marks): **(Wallet Security)** The UNSW Forward Thinking Student Society decides to live up to its name by accepting annual fee payments from its members in Bitcoin. Since they are not in possession of a hard wallet, they decide to use a paper wallet, and Sophie, the Society Secretary, uses the following process:

- Sophie points her browser to a `https` secured webpage hosted by a reputable Bitcoin exchange, that provides paper wallet production functionality. (In order to attract potential customers to their site, the exchange offers this functionality openly, and does not require users to have an account with the exchange or to authenticate themselves in order to access the page.)
- Sophie's browser runs a Javascript function on the webpage that asks the user to move the mouse as a source of randomness.
- The page uses the randomness to generate and display a Bitcoin private key, public key and address.
- Sophie prints this page and puts it into her home safe.
- Sophie copies the public key and address, and closes the webpage.
- Sophie publishes the address on the Society's `https` secured webpage on CSE servers with the message “pay your annual subscriptions in Bitcoin to this address, then email us the transaction and output details so we can use the money”.

In no more than one page, discuss the security risks involved in this process, by describing at least 5 distinct attacks that an attacker might try to use to remotely (i.e., without breaking into anyone's house) steal the Society's money. For each, briefly describe (1) the identity and/or the type of attacker, and the information and capabilities that they have available to them, (2) the cost to the attacker in terms of money, difficulty, effort and/or computation time, and (3) what, if anything, Sophie can do to prevent the attack, or mininize the probability that the attack is successful.

Question 5 (5 marks): **(Bitcoin Script)** A national security agency has discovered that it can crack the cryptography being used by the enemy if it can solve the following puzzle for particular 256 bit values N_1, N_2:

> Find two 32 bit numbers x_1, x_2 such that
> $x_1 < x_2$ and $N_1 \leq h(x_2 - x_1) \leq N_2$.

where h is SHA-256. Solving the puzzle requires a very large and costly amount of computation, and to offload the cost, the agency comes up with a clever scheme. They pretend to be a philanthropist who is offering a 1 bitcoin donation to the first person who solves the puzzle. They hope that this will encourage many people around the world to use their desktop machines to search for a solution to the puzzle and submit the solution to the blockchain, where the agency will be able to read it. Describe precisely how they could do this with a Bitcoin transaction that will pay 1 bitcoin to anyone who solves the puzzle. Your answer should do the following:

- Give the locking script for this transaction.
- Give the unlocking script for the transaction.
- Show the sequence of stack values for a successful unlocking computation. Use abstract values such as x_1, $h(x_1)$ rather than actual numbers.
- Mary and Bob both get lucky, and independently solve the puzzle at exactly the same time. Discuss the factors involved in determining who gets the reward.

Hint: The complete set of Bitcoin Script opcodes is at

`https://en.bitcoin.it/wiki/Script`

You might find it helpful to use the Bitcoin Script simulator at

`https://siminchen.github.io/bitcoinIDE/build/editor.html`

to develop your solution. In your answers, use the opcode words rather than the corresponding numbers. Also follow the convention of omitting the value-pushing opcodes (that is, write just x instead of OP_DATA 1 x).

Question 6 (5 marks): **(Bitcoin Protocol & Applications)** Alice, Bob, Carroll and a thousand others live in a remote lithium mining community in the Australian outback. All the bank branches in the town have recently been closed, so the community decides to consider adopting Bitcoin as the currency for all payment transactions within the community. (Since Bitcoin is not widely adopted in the rest of the country, they will continue to use Australian dollars for transactions with the rest of the country.) You have been hired as a consultant to analyse the feasibility of this idea.

Some factors to be taken into consideration are the following:

- Lithium is now a hot commodity, so the community is relatively wealthy, and in particular, everyone has a smart-phone and a fancy computer at home. However, there is not adequate wealth for the purchase of additional computing infrastructure in the form of specialised equipment.

- The community is well served for internal communications by a wireless network, and everyone has a wireless modem at home. Local mobile calls are routed using the wireless network.
- Communications with the outside world are not good, however. There are no landlines connecting the community to the outside world (not even telephone lines or electricity cables), and the community network is connected to the internet only via a satellite communications link. The satellite serving the community has an orbit that enables the community network to connect to the rest of the internet only in the first of every four weeks. That is, the community has 1 week of connectivity, but then is disconnected from the internet for three weeks, before it gets its next week of connectivity, etc.

In no more than one page, taking into the account the factors above, the details of the Bitcoin protocol as well as economic considerations, write an analysis of how well (or not) the community's adoption of Bitcoin can be expected to function. Consider, in particular, a mode of use in which all community members run a Bitcoin full node at home. If any particular difficulties are likely to arise, explain what these are, and discuss economic, social and/or technical approaches for dealing with them. On the basis of this analysis, do you recommend that the community adopt Bitcoin?

– END –