Security Exercises

These exercises are grouped into three parts. Part I contains routine exercises to help you understand the ideas directly presented in lectures. The exercises in Part II are designed to grow and deepen your understanding of principles that underpin electronic security. These exercises extend the lecture material and invite you to think about 'why' questions and about optimisations to what was lectured as well as alternatives to what was lectured. Part III are open-ended, stretching questions that you could tackle in your mini research project.

I hope you enjoy working through these questions, puzzles and research questions!

John Fawcett, July 2023

Part I

1. Which of these are good hash functions? Why (not)?
    a. H(x) = sin(x)
    b. H(x) = the value of y at the turning point of $y^2 + xy$
    c. H(x) = x^{13} MOD 221
2. If we had a database of thousands of usernames and hashed passwords, how could we try to recover any username/password combination if the hashed passwords are of the form…
    a. SHA3(plaintext)
    b. SHA3(N_8 || plaintext)
    c. How much longer will it take to crack (b) than (a)?
3. Figure out how to break the rock-paper-scissors game on the "final horror" slide.
4. Have a go at this Cambridge exam question:

Software and Security Engineering (RJA)

The public-key Needham-Schroeder protocol is as follows:

$$\begin{aligned} A &\longrightarrow B : \{NA, A\}_{KB} \\ B &\longrightarrow A : \{NA, NB\}_{KA} \\ A &\longrightarrow B : \{NB\}_{KB} \end{aligned}$$

(*a*) Explain the notation used and the purpose of the protocol. [4 marks]

(*b*) What is wrong with this as a protocol design and how might this flaw be fixed? [10 marks]

(*c*) What would we still have to check about an implementation? [6 marks]

5. Have a go at this second Cambridge exam question:

Security

The owner of a banking system which previously used manually distributed shared keys to compute MACs on transactions decides to use public key cryptography to distribute MAC keys in future. The proposed protocol is

$$A \to B : \{\{T_A, K_{AB}\}_{K_A^{-1}}\}_{K_B}$$

Explain the symbolism used in this description. [2 marks]

What is wrong with this protocol? [6 marks]

The protocol is changed to

$$A \to B : \{\{A, T_A, K_{AB}\}_{K_A^{-1}}\}_{K_B}$$

What attacks might there be on the system now? [12 marks]

6. Find out and explain how to build a good hash function from a block cipher using
    a. The Davies–Meyer construction
    b. The Merkle–Damgård construction

Part II

1. The IPv4 network protocol uses a 1's complement sum (OCS) to detect corruption. Implement a function that takes an array of integers as its input and returns the OCS.
    a. Given input 'v', prints an output, m, such that OCS(m) = v
    b. Given input 'm' will search for a different n, such that OCS(m)=OCS(n)
    c. Finds any two messages x and y that have the same OCS.
2. Try to implement the CRC-32 algorithm. Can you write three programs that…
    a. Given input 'v', prints an output, m, such that CRC32(m) = v
    b. Given input 'm' will search for a different n, such that CRC32(m)=CRC32(n)
    c. Finds any two messages x and y that have the same CRC32.
3. Cryptographically secure hash functions are related to encryption, which rely on similar mathematical tricks and mathematical analysis to prove their security. Find out and explain how each of the following uses of a block cipher work, and whether they are vulnerable:
    a. Electronic Code Book
    b. Output Feedback
    c. Cipher Feedback

Part III

1. I said that we can "use Physics to invent random junk". There are different ways to do this. Four possible mini-research projects might investigate how to do this based on:
    a. A radioactive sample and a geiger counter
    b. A very sensitive thermometer
    c. Quantum physics
    d. The timings of packets of data flowing through the Internet