UNIVERSITY OF OTAGO EXAMINATIONS 2024

SCHOOL OF COMPUTING

Paper COSC412

CRYPTOGRAPHY AND SECURITY

Semester 2

(TIME ALLOWED: THREE HOURS)

This examination comprises 4 pages.

Candidates should answer questions as follows:

Candidates should answer **all questions**.

The total number of marks available for this examination is 120.

Questions are worth various marks, and marks are shown this way: (5)

The following material is provided:

Nil.

Use of calculators:

Any model of calculator provided this is battery powered, silent, truly portable and free of communication capabilities.

Candidates are permitted copies of:

Nil.

TURN OVER

1. Basic cryptography

(a) Alice and Bob wish to communicate using a symmetric cryptosystem. What are the parts of such a system and how do they fit together? (4)

(b) If messages consist of a sequence of digits, and each digit is chosen from the usual range 0 through 9, how many different keys are available for a simple substitution cipher? Justify whether or not this is enough to rule out brute force attacks. (4)

(c) Contrast the difficulty in breaking a Vigenère cipher for an attacker that can perform a chosen plaintext attack versus an attacker performing a ciphertext-only attack. (4)

(d) The cryptography algorithms used within most commodity systems are assumed to be publicly known. Why is this the case? Does this public knowledge affect the security of the system? Where is all of the security focused, in practice? (4)

(e) Explain why asymmetric (public-key) cryptography is typically more convenient to use than symmetric key cryptography. Include an example that supports your answer. (4)

2. One time pads, pseudo-random generators and key agreement

(a) What is a "one time pad"? Why is it semantically secure? What is its primary disadvantage? (4)

(b) What is a pseudo-random generator? Include in your answer a description of general properties of the inputs and outputs of such a generator, G. (4)

(c) A pseudo-random generator is said to be secure if there is no efficient statistical test T that has significant advantage over G. What does that mean? (4)

(d) Chris has developed a pseudo-random generator G' that is 'strengthened' to ensuring that particular patterns in the output that might not look random, such as long sequences of 1-bits, are removed. Present how you would explain to Chris that this means that his generator is actually insecure. (4)

(e) Recall that we discussed Diffie-Hellmann key exchange between Alice and Bob including these steps:

- Alice and Bob agree on a large prime p and a primitive root g modulo p.
- Alice randomly chooses $2 \leq a \leq p - 2$ and sends $g^a \pmod{p}$ to Bob.

Finish the sequence of steps and explain how Alice and Bob can now compute a shared secret key k. If Eve is listening to the messages being exchanged, what is preventing her from discovering k? (4)

3. Block ciphers

(a) The explanation of a block cipher 'mode of operation' is often done using a diagram. Explain the purpose of each of four of the components often seen in such a diagram, illustrating the role of each of these components in the context of the cipher block chaining (CBC) mode of operation. (8)

(b) Consider the counter (CTR) block cipher mode of operation.

(i) Explain how the counter is used in the encryption process. (2)

(ii) If the nonce is repeated when encoding a subsequent message, what is the consequence for the security of the encryption? Justify your answer. (4)

(c) Give two examples of ways in which a block cipher using the CBC mode differs in behaviour from a stream cipher. (2)

(d) Explain how a block cipher can be used to produce a pseudorandom number generator. Include in your answer a description of the components of the block cipher that are used, and how they are combined to produce the pseudorandom output. (4)

4. HTTPS / TLS

(a) Recall that digital certificates used in HTTPS are a way to publish a public key, and demonstrate ownership of the corresponding private key. Explain how a user's computer with a fresh installation of Google Chrome can first connect to an internet banking website, and that the user can be confident they are not connecting to a fraudulent website. (6)

(b) The private keys used in HTTPS may be stolen if a server they are stored on suffers a security breach. Explain the dangerous consequences of such a theft. How can use of the stolen certificate be stopped? (4)

(c) Explain the purpose and function of the SSL/TLS handshake process in establishing a secure connection between a client and a server over HTTPS. Include the key steps involved and the role of digital certificates in this process. (6)

(d) Although checking certificates involves asymmetric cryptography, the actual data transfer in HTTPS uses symmetric cryptography. Explain two different benefits of this approach. (4)

5. **Kerberos**

(a) Illustrate and explain the interactions performed when a user uses Kerberos to authenticate to a remote server using the secure shell protocol (SSH). You can assume that the user does not yet have any valid Kerberos tickets. (8)

(b) If a user's service ticket is stolen, what are the potential consequences for the user and the system? Explain how Kerberos can be used to mitigate these risks. (4)

(c) Tickets can be renewable in Kerberos. This typically means the ticket has a short validity time, but a longer renewable time. The expired ticket can be presented to the Ticket Granting Server, and if the renewable time has not yet passed, a new ticket is issued. Contrast using a renewable ticket against requiring users to request a sequence of new service tickets. (4)

(d) Explain two downsides that arise from Kerberos using symmetric cryptography. (4)

6. **Decentralised web authorisation / blockchain**

(a) Say that you develop an application called SlideSlurp that automatically generates a slide deck from the slide content seen in a video presentation. SlideSlurp watches a user's YouTube account for new videos. Describe the sequence of steps within the OAuth2 'authorization code' workflow, and illustrate how it supports your application's needs. In your answer, identify each of the Resource Owner (RO), the Authorisation Server (AS), the Client (C) and the Resource Server (RS). (8)

(b) The 'authorization code' workflow assumes that the OAuth2 client is able to store secrets that the resource owner and other participants cannot access. In the implicit grant type, the client is not assumed to have this capability, e.g., because its software is directly observable by the resource owner. Explain the steps that can be skipped from the 'authorization code' workflow, and what this implies in terms of the security of the system. (4)

(c) In a public, permissionless blockchain such as bitcoin, can transactions ever be considered to be truly, persistently committed? Explain your answer. (4)

(d) Contrast the consensus algorithms used in a blockchain such as bitcoin against the consensus algorithms used within a data centre owned by a single organisation (e.g., supporting software such as a distributed database system). (4)