# COMP3334 Computer Systems Security

Semester 2, 2023/2024, Section 2

April 2, 2024

Student ID: ________________ Student Name: ________________________________________

# Quiz 2A

## README

This is a closed-book exam. Complete your ID and name above first. When instructed, open the booklet and answer the multiple choice questions by **circling** the right answer (there is only one possible correct answer per question). Continue by answering questions in the spaces provided. If you run out of room for an answer, it is most likely getting too long. As a reminder, plagiarism is a serious offence. If you are caught cheating, you will receive a zero for this quiz. If you finish the quiz and there is less than 10 minutes remaining, stay until the end.

Total: 16 points worth 8% of the course weight. Total pages: 4

Allowed time: 30 minutes

## **Multiple Choice Questions** (single correct answer) [6 pts]

1. What differentiates a self-signed certificate from a root CA certificate? (1 pt)

   A. A self-signed certificate can issue certificates to other entities, whereas a root CA certificate cannot

   B. The root CA certificate is not self-signed

   C. Self-signed certificates are automatically trusted by web browsers and operating systems

   [✓ D.] The root CA certificate is trusted by devices and browsers

2. Which of the following is NOT an application of public-key cryptography? (1 pt)

   A. Digital signature

   B. Decryption

   [✓ C.] Key derivation

   D. Key exchange

3. Among the following, what is a typical key size for elliptic curve cryptography? (1 pt)

   A. 15,360 bits

   B. 1024 bits

   [✓ C.] 256 bits

   D. 128 bits

4. What is the primary function of TLS (Transport Layer Security)? (1 pt)

   A. To speed up website loading times

   [✓ B.] To secure communications over the internet

   C. To authenticate user access to web services

   D. To preserve anonymity of users on the web

5. What is the security of the Diffie–Hellman algorithm based on? (1 pt)

   [✓ A.] Discrete Logarithm Problem

   B. Man-in-the-middle attacks

   C. Trapdoor one-way functions

   D. Factorization

6. Which of the following is NOT a digital signature algorithm? (1 pt)

   A. RSA

   [✓ B.] DH

   C. ECDSA

   D. EdDSA

(turn to next page)

## **Short Answer Questions** [10 pts]

7. In public-key encryption, which key is used to *decrypt* the ciphertext? (1 pt)

   Private key

8. In TLS 1.3, according to the simplified handshake we discussed in class, what is the purpose of the ClientHello and ServerHello messages? (1 pt)

   Perform a Diffie-Hellman key exchange (send each other's public key) + agree on a ciphersuite.

9. Write the command line to run a brute-force attack with hashcat against SHA1 hashes (hash type 100) stored in `hashes.txt`. Passwords are only composed of seven random lowercase letters. (1 pt)

   ```
   hashcat -m 100 -a 3 hashes.txt ?l?l?l?l?l?l?l
   ```

10. If Alice's private key is $a$, Bob's private key is $b$, and $p$ and $g$ are the public parameters of the system (a large prime and a primitive root mod $p$, respectively), what is the shared secret obtained by both parties at the end of the Diffie–Hellman key exchange algorithm? (1 pt)

    $g^{ab} \bmod p$

11. What is a X.509 digital certificate? (1 pt)

    Data structure that binds a public key to an identity, by means of a digital signature generated by a trusted third party (or Certification Authority (CA)).

12. According to our discussion of the course assignment, give one reason why the Lan Manager (LM) hashing algorithm has been deprecated for hashing passwords in Windows. (1 pt)

    All possible passwords can be brute-forced within a short period of time on current hardware.

(turn to next page)

13. Based on your reading of the textbook *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin* (2nd ed.) by Van Oorschot, P. C. (2021), Chapter 2: "Cryptographic Building Blocks," what main advantage does elliptic curve cryptography (ECC) offer compared to integer factorization cryptography (IFC) and finite field cryptography (FFC)? (2 pts)

ECC is easier to compute (computational efficiency), faster

ECC has smaller keys

14. Explain the danger of not authenticating keys for communications that are encrypted using public-key cryptography. (2 pts)

Man-in-the-middle attacker can swap someone's public key for his own, then get encrypted communications to himself so he can decrypt the communication.