NATIONAL UNIVERSITY OF SINGAPORE

CS2107 – Introduction to Information Security

(AY2023/24 Semester 1)

Mid-Term Exam's *Answers*

Date: 11 Oct 2023 Time: 12:05 – 1:20PM

INSTRUCTIONS TO CANDIDATES

1. This question paper consists of **TWENTY-FIVE (25)** questions and comprises **SEVEN (7)** printed pages, including this page.
2. This mid-term exam has **25 marks**, and is worth **15%** of your final score.
3. Fill in your Student Number, Name, and Tutorial Group information on your **answer sheet** with a pen.
4. Answer **ALL** questions, and submit your **answer sheet**. You can keep this question paper.
5. Choose the best answer in each question and write down the corresponding letter choice on **your answer sheet**.
6. You may use pen or pencil to write your answers, but please erase cleanly and write legibly. Your answers may be unaccepted due to illegible handwriting.
7. If you think there is an ambiguity in a question, do make **your own best interpretation**. Please ask only administrative related questions, and not about the question's content.
8. This is an **OPEN BOOK** assessment.
9. You are allowed to use **NUS APPROVED CALCULATORS**. Yet, you should be able to work out the answers without using a calculator.

1. Which security requirement is directly violated by *data tampering/modification*?

a) Confidentiality
b) Integrity
c) Availability
d) Non-repudiation
e) Privacy

2. *Petya* is a family of ransomware discovered in 2016, which targets Microsoft Windows-based systems. It infects the hard drive's MBR to execute a payload that encrypts its file-system table, and prevents Windows from booting. It then asks the user to make a payment in Bitcoin in order to regain access to the system. From this attack description only, which security requirements are compromised w.r.t. user data within a victim system?

a) Confidentiality and non-repudiation
b) Integrity and availability
c) Authenticity and availability
d) Non-repudiation and availability
e) Integrity and non-repudiation

3. In the context of cybersecurity ecosystem in Singapore, what is *CSA Singapore* which annually reviews Singapore's cybersecurity situation?

a) Cyber Security Agency of Singapore
b) Computer Security Association of Singapore
c) Cyber Security Alliance of Singapore
d) Certification System Authority of Singapore
e) None of the above

4. Bob uses substitution cipher with 27 symbols in the alphabet like in our lecture. He, however, performs the cipher's encryption function **3 times** using **3 different** (substitution table) **keys**. That is, given a plaintext *X* and 3 different keys *S*1, *S*2 and *S*3, Bob encrypts to produce the ciphertext *C* as follows:

$$C = E_{S3}(E_{S2}(E_{S1}(X))).$$

Bob's decryption process is then performed 3 times using the 3 keys in reverse order. What's the ***actual*** **key space size** of Bob's modified substitution cipher?

a) 27
b) 27!
c) 3 × 27!
d) $(27!)^3$
e) $\log_3(27!)$

[***Note on the answer***: The composition of 2 substitution ciphers, i.e. a substitution cipher being successively carried out using 2 different keys, is still a substitution cipher with *a single* ***composed key***. By extending this argument, Bob's cipher is still a *single substitution cipher*. The actual key space size, as the attacker's work factor, therefore remains 27!]

5. ____________________________ performs its encryption on a binary bit or byte in a data stream, one at a time. It combines plaintext bits or bytes with a generated pseudorandom sequence. Its operation is fast, yet it has a low diffusion level.

a) DES (with CBC mode-of-operation)
b) AES (with CBC mode-of-operation)
c) RSA (with CBC mode-of-operation)
d) Stream cipher
e) One-time pad

6. Alice used AES in CTR mode-of-operation to encrypt two different plaintexts P_1 and P_2. Unfortunately, Alice selected the same IV value for encrypting the two plaintexts. What can Eve derive from observing the two corresponding IV-removed ciphertexts C_1 and C_2?

a) Alice can know the secret key of AES
b) Alice can know the pseudorandom sequences XOR-ed with the plaintexts
c) $\boldsymbol{C_1 \oplus C_2 = P_1 \oplus P_2}$
d) $C_1 = P_1 \oplus P_2$
e) $C_2 = P_1 \oplus P_2$

[***Note on the answers***: Since AES in CTR mode works as a stream cipher, option (c) is correct. By right, options (a) and (b) should have put “Eve” instead of “Alice”. However, with Alice being considered in these two options, both options become correct as well. All the three options are thus accepted due to the unintended typos.]

7. Alice needs to ensure confidentiality with a high diffusion level. Which cryptographic scheme below should she use?

a) AES in CBC mode-of-operation
b) AES in CTR mode-of-operation
c) SHA-256
d) HMAC
e) DSA

8. Which cryptographic scheme below is a symmetric-key based technique that can provide data-origin authenticity but *not* non-repudiation?

a) AES in CBC mode-of-operation
b) AES in CTR mode-of-operation
c) SHA-256
d) HMAC
e) DSA

9. Certain modes-of-operation can be **parallelized** so that two processors can complete a cryptographic operation in roughly half the time taken by a single processor.
Can **CTR mode-of-operation** be parallelized?

a) Yes for both encryption and decryption

b) Yes for encryption, no for decryption

c) No for encryption, yes for decryption

d) No for both encryption and decryption

e) Depends on the IV value selected

10. Consider the Padding Oracle attack like the one discussed in our lecture slides. For the given scenario of 8-byte block with 3 padding bytes added, the algorithm for outputting the value of x_5 is given. Now, you want to subsequently know **the value of x_4**.
How should you set the IV' and tell the output this time?
(***Note***: The numbers below are in hexadecimal.)

a) Set IV' = IV $\oplus$ 00 00 00 00 a 05 05 05, and output: 05 $\oplus$ a

b) Set IV' = IV $\oplus$ 00 00 00 a 06 06 06 06, and output: 06 $\oplus$ a

c) Set IV' = IV $\oplus$ 00 00 00 a 06 06 06 06, and output: 05 $\oplus$ a

d) Set IV' = IV $\oplus$ 00 00 00 a 08 08 08 08, and output: 08 $\oplus$ a

e) Set IV' = IV $\oplus$ 00 00 00 a 08 08 08 08, and output: 05 $\oplus$ a

[***Note on the answer***: There are typos in the given options. Option (c) should actually be: "Set IV' = IV $\oplus$ 00 00 00 a (x_5 $\oplus$ 05) 06 06 06, and output: 05 $\oplus$ a". I missed replacing the highlighted "06" in option (c) with "x_5 $\oplus$ 05". The same byte position in options (b), (d) and (e) could also be similarly replaced. Since there are no correct answers, this question is thus voided. Its carried 1 mark is given to everyone regardless of the answer given.]

11. The Padding Oracle attack as discussed in the class applies to the following conditions, ***except***:

a) The attacker has access to a padding oracle, which works as a weak form of decryption oracle

b) The oracle uses CBC mode-of-operation for decrypting queried ciphertexts

c) The attacker's ability to receive an error message from the oracle if the padding of a recovered/decrypted plaintext is incorrect

d) The attacker's ability to receive padding length information from the oracle

e) The attacker's ability in supplying modified IVs or ciphertext portions in its queries to the oracle

12. ______________________________ is carried out on an authentication system by trying all entries contained within a popular word list like rockyou.txt.

a) Brute-force/exhaustive password attack

b) Dictionary attack

c) Birthday attack

d) Side channel attack

e) Frequency analysis attack

13. Mirai attack works by enslaving IoT devices to form a massively connected network. The devices are then used to deluge target websites with requests, thus overloading the sites and effectively crashing them. Because these victim devices ________________________ and therefore become easy to hijack, Mirai could infect over 600,000 devices at its peak.

- **a) Have zero-day vulnerabilities**
- **b) Have known vulnerabilities**
- ***c) Have factory default usernames and passwords***
- d) Use broken cryptographic schemes
- e) Can be attacked using key-logger

[***Note on the answers***: As mentioned in our lecture notes, Mirai attacks took advantage of default credentials used in user devices. Hence, the best answer should be option (c). However, several security reports put that some past Mirai attacks were done by exploiting known and even zero-day vulnerabilities. Let me additionally accept options (a) and (b).]

14. Alice wants to select a **case insensitive alphanumeric** (A-Z, 0-9) password for an **online banking login page**. She wants to follow the recommendation in RFC 4086. Which is the shortest length that meets the security recommendation as discussed in the lecture?

- a) 5
- **b) 6**
- c) 7
- d) 8
- e) 12

[***Note on the answer***: **6 >** 29 / 5.17 = 5.6.]

15. The following measures are good practices that should be incorporated to protect **the password file** of an authentication system ***except***:

- a) The password file storing information derived from user passwords should not be accessible to non-root users
- b) User passwords should not be stored in clear, but they must be hashed first
- c) The hashing of a user password must also take a salt as input
- **d) A random system-wide salt can be used for all users in the authentication system**
- e) SHA-2 or SHA-3 can be used for the hashing operations

16. Which one is actually desirable or considered ideal in a biometrics system?

- a) A very high FMR (false match rate)
- b) A very high FNMR (false non-match rate)
- c) A very high FER (failure-to-enroll rate)
- d) A very high FTC (failure-to-capture rate)
- **e) None of the above**

17. ______________________ property ensures that a cryptographic hash function is hard to invert. In other words, given an element in the range of that hash function, it should be computationally infeasible to find the input that maps to that element.

a) Correctness
b) Efficiency
c) Pre-image resistance
d) Second pre-image resistance
e) Collision resistance

18. Suppose a hash function produces a 256-bit digest. Mallory wants to repeatedly generate message digests so that, with a probability of more than 0.5, she has two messages with the same digest. What is the ***minimum*** number of messages among the options below should Mallory hash in order to achieve her objective?

a) 2^{64}
b) 2^{128}
c) $\mathbf{2^{129}}$
d) 2^{256}
e) 2^{257}

19. Consider RSA where the modulus *n* is 143. What is the value of *Φ*(*n*)?

a) 11 and 13
b) 143
c) 132
d) 130
e) 120

20. Consider RSA where the modulus *n* is again 143. Suppose *e* is 7. Which among the following possible values should be *d*?

a) 20
b) 67
c) 103
d) 121
e) None of the above

21. Which statement below is the most appropriate regarding RSA public-key scheme?

a) *Φ*(*n*) must be made public since the public needs it for calculations
b) After deriving *Φ*(*n*), both prime factors *p* and *q* are still needed for calculations
c) Even with the knowledge of *Φ*(*n*), the attacker still cannot easily decrypt ciphertexts
d) The attacker cannot break RSA since there are no efficient algorithms to compute a modular exponentiation
e) The attacker cannot decrypt ciphertexts since deriving *Φ*(*n*) from *n* requires performing prime factorization

22. PKI is an arrangement that binds public keys with respective identities of entities (e.g. people and organizations). The binding is established through a process of registration and issuance of certificates conducted by ________________________.

a) A publicly available directory server

b) A Certificate Authority (CA)

c) Browser or OS developers like Google or Microsoft

d) ITU-T X.509

e) PKIX working group of IETF

23. Which statement regarding PKI below is ***incorrect***?

a) A certificate binds a subject entity with its stated public key

b) A certificate has only limited lifetime as specified by its issuing CA

c) A verifier must not accept a self-signed certificate even if it belongs to a root CA

d) There could be intermediate CAs in the certification chain of a certificate

e) A valid certificate in question still needs to be checked whether it has been revoked

24. Suppose one **root CA** trusted by a browser is compromised since the CA's private key became known by an attacker. Which action below can help prevent all browser users from being targeted by the attacker?

a) Check the validity of the compromised CA's certificate with its issuer CA

b) Check the validity of the compromised CA's certificate using CRL

c) Check the validity of the compromised CA's certificate using OCSP

d) Ensure that the padlock icon is always displayed when visiting HTTPS websites

e) Perform a browser update that removes the compromised root CA from the trusted root CA list

25. When a transfer of information objects between two separate processes is not supposed to be allowed by the applicable computer security policy, a/an _______________ is sometimes created by an attacker for the illegal transfer in order to bypass the policy and/or avoid detection.

a) Side channel

b) Covert channel

c) Mode-of-operation

d) Skimming

e) Birthday attack

**~~~ END OF PAPER ~~~**