Instructions:

1. *Use the Answer Sheet. Remember to fill in your id. Use 2B pencil. Submit only the Answer Sheet.*
2. *Total 25 MCQ and 7 pages.*
3. *Note that the numberings of the questions are consecutive starting from 1, even when some questions are logically grouped.*
4. *Only ask administrative questions. If you think that there is ambiguity in the questions, make your own interpretation. We will resolve the ambiguity later.*
5. *You can use iPad, tablets, calculator, or laptop. No communication with human allowed. No phone. Keep your phone in pocket or in the bag. No taking of photo.*
6. *We assume that carrying out 2^{64} primitive cryptographic operations (e.g. hash, one-block AES operation, multiplication of two large integers) is feasible, whereas it is infeasible for 2^{128} operations.*

(General) Some of the following statements are modifications of phrases extracted from the public domain or other documents. They may not use the same notations in our lecture. Nonetheless, from the context, the meaning is clear. Choose the most suitable answer.

1. *Website defacement* is an attack that changes the visual appearance of a website. This attack compromises the _____ of the site.

   A. availability B. integrity
   C. confidentiality D. accountability E. creditability

2. Many systems are open source. With respect to security, we can say that these systems are practicing _____.

   A. accountability B. confidentiality
   C. Kerckhoff's principle D. security by obscurity
   E. crowd sourcing

3. Signature uses PKC whereas mac uses symmetric key. Hence, signature can ensure ____ while mac can't.

   A. authenticity B. non-repudiation
   C. confidentiality D. efficiency
   E. availability

4. GPS spoofing, also known as GPS simulation, refers to the practice of manipulating or tricking a GPS receiver by broadcasting false GPS signals. Essentially, it misleads the GPS receiver into believing it is located somewhere it is not, resulting in the device providing inaccurate location data. This best demonstrates an attack on _____.

   A. confidentiality B. integrity
   C. availability D. reliability E. accountability

5. Which of the following statements on zero-day vulnerability is likely wrong?

   A. Many zero-day vulnerabilities are already documented in the CVE. The difficulty is in patching them and thus difficult to mitigate.
   B. A zero-vulnerability is typically discovered by the attacker before the developer, and thus there is no patch when the attack is launched.
   C. Zero-day vulnerabilities are difficult to find, but some could be simple mistakes that are overlooked for a long period of time.
   D. Zero-day vulnerabilities could be due to implementation bugs, design flaws or even configuration mistakes.

6. A company published the NRIC number (this is a 7-digit id system in Singapore) of the lucky draw winners. This led to many complaints in the social media as it violated the winners' privacy. In the second round, instead of publishing the NRIC, the company published the hashed values using SHA3. So, the participants can still check their status, and yet hiding information of their NRIC. This led to another round of heated discussion in social media. What do you think?

   A. Due to collision, the digests would leak some information of the NRIC but not all. So not totally meaningless.
   B. This additional step was meaningless. One could exhaustively hash all possible NRIC and invert the hashed values.
   C. This was an example on the tradeoff of security and usability. The additional step would make it less usable during checking but improve security.
   D. The company should encrypt the NRIC using its RSA private key and publish the ciphertext. The participant could use the company public key to decrypt and check.
   E. This was meaningless. SHA3 would produce random digests. Even the participants could not check.

7. Certain mode of operations can be parallelized so that two processors can complete the operation in roughly half the time taken by a single processor. Can CBC mode be parallelized?

   A. Yes for encryption. No for decryption.
   B. No for encryption. Yes for decryption.
   C. Yes for both encryption and decryption.
   D. No for both encryption and decryption.
   E. Depend on the choice of IV.

8. Refer to the previous question. Can CTR mode be parallelized?

   A. Yes for encryption. No for decryption.
   B. No for encryption. Yes for decryption.
   C. Yes for both encryption and decryption.
   D. No for both encryption and decryption.
   E. Depend on the choice of IV.

(Padding Oracle) All the followings are encrypted using CBC mode and each block consists of 16 (sixteen) bytes. Numbers written in the form x00 are in hexadecimal format. E.g. x0A represents the value 10 (ten).

9. Suppose a padded two-block message is:
   (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4,1,1), (1,2,3,4, 5,6,7,8, 9,0,1,3, 3,3,3,3)
   What is the original unpadded message?

   A. (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4,1,1), (1,2,3,4, 5,6,7,8, 9,0,1,3, 3)
   B. (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4,1,1), (1,2,3,4, 5,6,7,8, 9,0,1,3)
   C. (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4,1,1), (1,2,3,4, 5,6,7,8, 9,0,1)
   D. (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4,1), (1,2,3,4, 5,6,7,8, 9,0,1,3, 3)
   E. (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4), (1,2,3,4, 5,6,7,8, 9,0,1)

10. Consider a situation where the plaintext consists of only 1 block. Let the IV and the ciphertext be

    $\mathbf{v} = (v_1, v_2, v_3, \ldots, v_{16})$
    $\mathbf{c} = (c_1, c_2, c_3, \ldots, c_{16})$

    The padding oracle returns "correctly padded" when on input ($\mathbf{v}$, $\mathbf{c}$). On input

    ($(v_1, v_2, v_3, \ldots,$ x03 xor $v_{15}, v_{16})$, $\mathbf{c}$),

    the padding oracle returns "wrongly padded". What is the most specific implication?

    A. The number of padded bytes is at most 2.
    B. The number of padded bytes is at least 2.
    C. The number of padded bytes is strictly less than 2.
    D. The number of padded bytes is strictly more than 2.
    E. The number of padded bytes is not 2.

Suppose the attacker knew that a 16-byte plaintext was a string (hexadecimal representation) of the following form:

($\boldsymbol{b}_1$, $\boldsymbol{b}_2$, $\boldsymbol{b}_3$, $\boldsymbol{b}_4$, $\boldsymbol{b}_5$, $\boldsymbol{b}_6$, $\boldsymbol{b}_7$, $\boldsymbol{b}_8$, $\boldsymbol{b}_9$, $\boldsymbol{b}_{10}$, x00, x00, x02, x02, x02, x02)

The attacker did not know the value of the $\boldsymbol{b}_i$'s. Let $\boldsymbol{v}$ be the one-block IV and $\boldsymbol{c}$ be the one-block ciphertext of the above plaintext. The attacker knew $\boldsymbol{v}$ and $\boldsymbol{c}$. Next, the attacker sent a query ($\boldsymbol{w}$, $\boldsymbol{c}$) to the padding oracle where:

$\boldsymbol{w} = \boldsymbol{v} \oplus (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$

The oracle returned "correctly padded". From this output, the attacker inferred that $\boldsymbol{b}_{10}$ must be 0, and $\mathbf{b}_9$ must be 0. The attacker also inferred that no conclusion can be made on $\mathbf{b}_8$. The attacker was right.

11. Based on the information above, what was the value of a_{16}?
    A. x02 B. x04
    C. x08 D. x0A
    E. any of the above is possible.

12. What was the value of a_{10}?
    A. x02 B. x04
    C. x08 D. x0A
    E. any of the above is possible.

13. What was the value of a_9?
    A. x02 B. x04
    C. x08 D. x0A
    E. any of the above is possible.

14. What was the value of a_8?
    A. x02 B. x04
    C. x08 D. x0A
    E. any of the above is possible.

(RSA)

15. Consider RSA with the modulo n=35. What is the value of $\varphi(n)$?
    A. 7, 5 B. 35
    C. 24 D. 12 E. 10

16. Suppose n=35 and the encryption key e=5, what is the decryption key?
    A. 1 B. 3
    C. 5 D. 7 E. -1

17. Suppose *n*=35, the encryption key *e*=5, and the plaintext is 3. How the is ciphertext computed?
    A. 5^3 mod 35
    B. 5^3 mod $\varphi(n)$
    C. $3^5 + 5^3$
    D. 3^5 mod $\varphi(n)$
    E. 3^5 mod 35

18. Which of the following statements on the RSA's primes ***p***, ***q*** is wrong?
    A. The primes ***p***, ***q*** must not be revealed to the public.
    B. Both ***p*** and ***q*** must be large, say at least 1000 bits.
    C. One of the primes must be large, say at least of 1000 bits, and the value of both primes must be larger than 65536. It is not necessary to have both primes to be large.
    D. Both ***p*** and ***q*** should be randomly chosen primes.
    E. Given a 2048-bit number, under current computing power, it is feasible to determine whether it is a prime number.

(Hash, Mac, Signature)

19. A lucky draw announced the winners by publishing the last 4 decimal digits of the participants' NRIC numbers (NRIC is a 7-digit id in Singapore, e.g. 8012345). The total number of winners was **W**, and there were **N** non-winners. Hence, there were a total of (**W**+**N**) participants. Let us assume that the NRIC numbers were randomly assigned. Suppose **N**=3,000. Among the followings, what was the smallest possible **W** so that the probability that a non-winner's last 4 digits being published was high (i.e. greater than 0.5)?

    A. 10
    B. 20
    C. 30
    D. 40
    E. 50

20. Alice wrote a program that, when on input a JPEG image **x**, would output another JPEG image **y** with the same digest, i.e H(**x**)=H(**y**) where H() was some hash function. This program successfully carried out an attack on the hash function H(). What was this attack?

    A. Collision attack.
    B. 2nd pre-image attack.
    C. One-way attack.
    D. Birthday attack.
    E. Known plaintext attack.

21. Here is a MAC (message authentication code) scheme. Given a message *x* and the secret key ***k***, the mac is the ciphertext

    t = Encrypt (***k***, H(***x***)),

    where Encrypt() is some symmetric key encryption and H() is some hash function. During verification, given a mac t_0 and the message x_0, the verifier simply decrypts t_0 and compares it with the digest of x_0.

    The security of the mac depends on the design of Encrypt() and H(). Suppose a particular construction is not secure. Which of the following approaches is likely wrong in showing that the mac is not secure.

    A. First show that H() is not pre-image resistant. Next, show that when given a valid mac ***t*** and a message ***x***, the attacker can invert and find another ***t'*** such that (***x***, ***t'***) is a valid mac.
    B. First show that H() is not pre-image resistant. Next, show that when given a valid mac ***t*** and a message ***x***, the attacker can invert and find another ***x'*** such that (***x'***, ***t***) is a valid mac.
    C. First show that Encrypt() is a stream cipher. Next, argue that if Encrypt() is a stream cipher, then the mac will not be secure.
    D. First find a collision of H(), say **x** and **x'**. Next, argue that if attacker knows the valid mac for **x**, then the attacker can derive the mac for **x'**.

22. A mysterious person painted a 256-bit string ***d*** on a public wall. It was artistically painted and was treated as a graffiti masterpiece. A few years later, Alice claimed that she was the artist. She also announced an 8-byte ASCII string ***m=***"`AN8%{@1z`" where SHA3(***m***) = ***d***. Do you accept Alice's claim?

    A. Alice might not be the artist. A person, who was not the artist, could exhaustively search for an 8-byte string whose digest matched ***d***.
    B. Alice might not be the artist. There are many hash functions, each with many different versions. A person, who was not the artist, could try all possible combinations to find such a match.
    C. Alice might not be the artist. A person, who was not the artist, could employ birthday attack on ***d*** to find the ***m***.
    D. Alice likely was the artist. Because SHA3() is one-way, it was unlikely for anyone to infer ***m*** from ***d***. Thus, only the person who created ***m*** could paint ***d***. The fact that Alice knew ***m*** implied that she was involved in the process.
    E. Alice likely was the artist. A randomly chosen 8-byte sequence is unlikely to be all ASCII characters. The fact that Alice could produce a ***m*** consisting of all ASCII characters implied that she was involved in the process.

23. The question is the same as the previous question, except that, in this question, the length of ***d*** is 128 bits. Do you accept Alice's claim?

    A. Same as the previous question.
    B. Same as the previous question.
    C. Same as the previous question.
    D. Same as the previous question.
    E. Same as the previous question.

24. The question is the same as the previous question, except that, here, the length of ***d*** is 256 bits and ***m=***"`Alice@SG`". Do you accept Alice's claim?

    A. Same as the previous question.
    B. Same as the previous question.
    C. Same as the previous question.
    D. Same as the previous question.
    E. Alice likely was the artist. It is unlikely that a randomly chosen message matches her name. The fact that the message contained her name implied that she was involved in the process.

25. Bob employed the following H() based on the 256-bit SHA3.

$$H(\boldsymbol{m}) = L_{128}(\text{SHA3}(\boldsymbol{m})) \text{ xor } T_{128}(\text{SHA3}(\boldsymbol{m}))$$

where $L_{100}(\boldsymbol{x})$ is the leading 128 bits, and $T_{100}(\boldsymbol{x})$ is the trailing 128 bits of ***x***. Bob realized that H() is not cryptographic secure and gave a proof. Which of the following statements is a valid proof?

    A. There are many digests where the leading 128 bits are the same as their trailing 128 bits. All these lead to digest of all zeros and thus are examples of collisions.
    B. There are many messages where the leading 128 bits are the same as their trailing 128 bits. All these messages have the same digest and thus we can easily find a collision.
    C. The length of each digest is only 128. Hence, it is feasible to carry out birthday attack to find collisions.
    D. Choose m_1 ="0" and m_2 ="1". Both have the same digest and thus we have a collision.
    E. By Pigeonhole principles, there are many collisions. Thus, the above is not collision resistant.

---------- END of Paper ----------