Instructions:

1. *Use the Answer Sheet. Remember to fill in your id. Submit only the Answer Sheet.*
2. *Total 25 MCQ and 7 pages.*
3. *The numberings of the sub-questions continue from previous question so that they correspond to the numbering in the Answer Sheet.*
4. *If you think that there is ambiguity in the question, make your own interpretation.*
5. *Only ask administrative questions. Do not raise questions about the content.*
6. *You can use iPad, tablets, calculator, or laptop. No communication to outside allowed, for e.g., not allowed to search Internet. No phone. Keep your phone in pocket or in the bag.*

I. 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. Mirai works by enslaving IoT devices to form a massively connected network. The devices are then used to deluge websites with requests, overloading the sites and effectively taking them offline. Because these devices _____ and are easy to infect, Mirai has been found spreading to at least 500,000 devices.

   A. have weak default passwords
   B. use SHA1
   C. have zero-day vulnerabilities
   D. accept self-signed certificates
   E. use expired certificates

2. In cryptography, a digital certificate is an electronic document used to prove the ownership of a _____ .

   A. Private key
   B. Public key
   C. Identity
   D. Signature
   E. Certificate Authority

3. A _____is an arrangement that binds public keys with respective identities of entities (like persons and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA).

   A. PKI
   B. trusted repository
   C. Chain of trust
   D. Self-signed Certificate
   E. secure broadcast channel

4. After more than 500 fake DigiNotar certificates were found, major web browser makers reacted by blacklisting all DigiNotar certificates. The scale of the incident was used by some organizations to call for a deeper reform of HTTPS in order to remove the weakest link _____.

   A. that the underlying cryptographic primitives are not provably secure.
   B. that a single compromised CA can affect that many users.
   C. that human errors are inevitable.
   D. that simple programming errors could bring down all security mechanisms.
   E. that the underlying cryptographic primitives can be broken by quantum computer.

5. Several techniques for _____have been developed. However, some are more effective than others. Perhaps the most common method seen today is eye blinking detection. This seems reasonable; after all, a photo cannot blink.

   A. biometric authentication
   B. face recognition
   C. face detection
   D. multi-factor authentication
   E. liveness detection

6. _____is basic knowledge in cybersecurity, but it very often violated. For example, it is almost impossible to buy digital lock with known cryptographic algorithms and protocols. As a result, most digital locks use weak crypto.

   A. Strong Authentication
   B. Security by obscurity
   C. Kerckhoff's principle
   D. Multi-factor authentication
   E. Attack model

7. A _____requires two inputs: a message and a secret key known only to the originator of the message and its intended recipient(s). This allows the recipient of the message to verify the integrity of the message and authenticate the message's sender.

   A. digest
   B. signature
   C. mac
   D. certificate
   E. encryption

8. The disadvantage of _____ is a lack of diffusion. Because it encrypts identical plaintext blocks into identical ciphertext blocks, it does not hide data patterns well.

   A. ECB mode
   B. CBC mode
   C. CTR mode
   D. GCM mode
   E. block cipher

9. The following was obtained from a website on signature.

   "*The digital signature creator's private key is used to encrypt the hash. The encrypted hash -- along with other meta information, such as the hashing algorithm -- is the digital signature*."

   The description follows a way that the CS2107's lecturer doesn't like, and he kept mentioned it during lecture. What is that?

   A. The description does not give the attack model properly. It doesn't state the goal and capability of the attacker.
   B. RSA-based signature schemes encrypt the hash, but there are many other signature schemes that do not involve encryption. The method of encryption works with RSA encryption but not necessary with others.
   C. Following Kerckhoff's principle, all algorithms must be made public. So, we shouldn't treat it as part of the secret.
   D. Meta information must also be hashed instead of being directly encrypted. Signature is for authenticity and not confidentiality. There is no reason to encrypt meta information such as the hashing algorithm.
   E. The lecturer is too fussy.

II. A request of a particular service is associated with a 20-bits request ID. This request ID is included in the server's response. For e.g.

Client → Server: "*Hello. My request ID is 162. Detail of my request is so-and-so*."
Server → Client: "*Hello. Regarding your request ID 162, the result is so-and-so*."

After the Client receives a response from the Server, the Client matches the request ID among the sent requests. If not found, the Client simply ignores the response. If the Client receives two responses with the same request ID, the one that arrives late will be ignored.

Suppose an attacker can trick its victim (who is the client in the above) to send out a large number ***m*** of requests at the same time, where the request IDs are randomly generated and are unique among the ***m*** requests. When the client receives a response, it will match it with the ***m*** requests based on the request ID. Although the attacker can trick the victim, the attacker is unable to know the request ID. The attacker can also forge responses that arrive faster than the legitimate responses. *The attacker can forge **q** responses.* The attack is successful if the device accepts at least one forged response.

10. When ***m***=1, and ***q***=1, what is the probability that the attack is successful?

A. 2^{-20} B. 1/10
C. 2^{-10} D. 1
E. 1/20

11. Suppose ***m***=1. Among the choices for ***q*** below, which is the smallest so that there is a good chance (specifically, probability greater than 0.1) of successful attack?

A. 1 B. 2^6
C. 2^9 D. 2^{10}
E. 2^{20}

12. Suppose ***m***=2^{11}. Among the choices for ***q*** below, which is the smallest so that there is a good chance (specifically, probability greater than 0.1) of successful attack?

A. 2^5 B. 2^6
C. 2^{10} D. 2^{11}
E. 2^{20}

III. (Padding Oracle)

13. Suppose a padded two-block message is:
(1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4,1,1), (0,0,0,0, 0,0,0,0, 0,0,0,0, 0,0,0,0)
What is the original unpadded message?

A. (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4,1,1), (0,0,0,0, 0,0,0,0, 0,0,0,0, 0,0,0,0)
B. (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4,1,1)
C. (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4,1)
D. (1,1,1,1, 2,1,1,1, 3,1,1,1, 4,4)
E. empty string

Suppose the attacker knows that a 16-byte plaintext is the string (hexadecimal representation):

($\boldsymbol{b}_1$, $\boldsymbol{b}_2$, $\boldsymbol{b}_3$, $\boldsymbol{b}_4$, $\boldsymbol{b}_5$,0,0,0, 0,0,0,0, 2, 2, 2, 2)

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

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

so that the oracle outputs "Correctly padded" iff $\boldsymbol{b}_5 = 1$.

14. For the above method to work, what is the value of a_{10}?
A. 02 B. 0A
C. 0B D. 0C
E. any of the above will work.

15. For the above method to work, what is the value of a_{16}?
A. 0A B. 0B
C. 0C D. 0E
E. any of the above will work.

16. For the above method to work, what is the value of a_5?
A. 0A B. 0B
C. 0C D. 0D
E. any of the above will work.

17. For the above method to work, what is the value of a_1?
A. 02 B. 0B
C. 0C D. 0D
E. any of the above will work.

IV. (RSA)

18. Consider RSA where the modulo ~~module~~ n=77. What is the value of $\varphi(n)$? (recap that $\varphi(n) = (p-1)(q-1)$ where p, q are the prime factors)
    A. 11, 7 B. 77
    C. 18 D. 60
    E. 49

19. Suppose n=77 and the encryption key e=7, what is the decryption key?
    A. 3 B. 5
    C. 11 D. 32
    E. 43

20. Suppose n=77, the encryption key e=7, and the plaintext is 2. What is the ciphertext?
    A. 3 B. 20
    C. 27 D. 51
    E. 128

21. Which statement below on $\varphi(n)$ is the most appropriate?
    A. $\varphi(n)$ must be made public since the public needs it for calculation.
    B. Although not necessary, $\varphi(n)$ can be made public.
    C. $\varphi(n)$ must not be made public, otherwise security will be compromised.
    D. It is believed that even with the knowledge of $\varphi(n)$, attacker still cannot break RSA. However, there is no formal proof. So, it is typically not made public.

V. (Hash, Mac and Signature) Recap that given a message ***m*** and a key ***k,*** the CBC-mac is computed by carrying out CBC encryption with the IV fixed as the string of all 0's, and the final mac is the last block of the encryption.

22. Bob wants to design a new mac. Instead of keeping only the last block as mac, he keeps all the blocks. Essentially, the mac is the ciphertext of ***m*** where the IV is fixed as zeros. Which of the following statements is most appropriate?

    A. The method gives a secure mac. We do not use this method because the mac size is large.
    B. The method gives a secure mac. However, it leaks information of the plaintext because the IV is always fixed at 0.
    C. The method is not secure. Suppose the attacker knows the mac of a 2-block message ***m***. The attacker can forge the valid mac of a 1-blcok message which is the first block of ***m.***
    D. The method is not secure. Since there are multiple blocks in the mac, the attacker can conduct birthday attack with significantly fewer operations.

23. Consider this hash function:

$$H(m) = SHA3(m) \oplus SHA3(m \oplus \mathbf{1})$$

where **1** is a string of one's and it has the same length as *m*. Essentially, the operation ($m \oplus \mathbf{1}$) flips all the bits in *m*. To illustrate, $1011 \oplus 1111 = 0100$. Which of the following statements is most appropriate?

A. Since SHA3 is collision resistant, so the function H'(m) = SHA3 ($m \oplus \mathbf{1}$) is also collision resistant. The xor of two collision functions is still collision resistant, and thus H() is a collision resistant hash.
B. Since H() is the xor of two functions, running time of birthday attack can be reduces by another square root factor.
C. H() is not collision resistant. For any message *m*, its digest is the same as the digest of ($m \oplus \mathbf{1}$).
D. There is a *m* and *m'* such that H(*m*) = H(*m'*) and m≠m'. Hence it is not collision resistant.

24. We need a cryptographic secure hash function. Among the followings, which one should we use?

A. A hash function which is resistant to collision attack.
B. A hash function which is resistant to one-way attack.
C. A hash function which is resistant to 2nd pre-image attack.
D. A hash function which is resistant to forgery.

25. Consider the VLC example in Lecture 3 which demonstrate the applications of unkeyed hash. In the example, the attacker wants to change the file and yet the user still believes that he/she has downloaded the correct file. Among the following, which is the most precise description of the attack?

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

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