Crypto quiz 1031

Quiz for Public Key

姓名

程锦科

学号

18010100078

1. The Federal Government wants to be able to issue advisories to the general public while ensuring that no one will be able to tamper with their messages or spoof a fake advisory. Which of the following is the best cryptographic approach to address this problem?

● A、Use a digital signature scheme, with the public key known to everyone, to sign each advisory when it is released.

○ B、Use a public-key encryption scheme, with the public key known to everyone, and decrypt each advisory when it is released.

○ C、Use multiple message authentication codes, with each member of the public being given a unique key, and generate one tag per key each time an advisory is released.

○ D、Use a message authentication code, with the key known to everyone, to generate a tag for each advisory when it is released.

2. The president and vice president of a company want to communicate while ensuring integrity of their communication. Which of the following is the best cryptographic approach to address this problem?

○ A、Use a CPA-secure private-key encryption scheme, with the key shared between them, and encrypt each message they send.

○ B、Use a digital signature scheme, with the public key known to everyone, and sign each message they send.

○ C、Use a message authentication code, with the key made public, and generate a tag for each message they send.

● D、Use a message authentication code, with the key shared between them, and generate a tag for each message they send.

3. Assume the "plain" RSA signature scheme, with public key (N=55,e=3). Which of the following verifies correctly as the signature on the message m=17?

○ A、7

○ B、43

○ C、4

● D、8

4. Assume "plain RSA" encryption is used with public key (N=33,e=3). What is the encryption of the message m=2?

○ A、32

○ B、7

● C、8

○ D、2

5. Assume the "plain" RSA signature scheme with public key (N,e=3). For which of the following messages is it always possible to forge a signature without seeing any prior signatures or factoring N? (Assume N>1000, and N relatively prime to each of the messages that follow.)

○ A、37

● B、27

○ C、47

○ D、2

6. Assume El Gamal encryption, where the group being used is Z^*_47 with generator 5. (This group has order 46, which is not prime. But El Gamal encryption can be defined in any cyclic group.) Assume the public key contains h=10. Say an attacker sees a ciphertext (41, 18) that is the encryption of some unknown message m. Which of the following is an encryption of [5m mod47]?

○ A、(17, 18)

● B、(41, 43)

○ C、(1, 5)

○ D、 (41, 5)

7. Which of the following is true in the public-key setting, but NOT true in the private-key setting?

○ A、It is possible to achieve perfect secrecy. x ✓

○ B、A deterministic encryption scheme cannot be CPA-secure. ✓ ✓

● C、Allowing the attacker to have access to an encryption oracle makes no difference when defining security. ✓ x

○ D、 (Under standard assumptions) there exist schemes that are CPA-secure, but are not CCA-secure.

8. Consider the SSL/TLS handshake protocol as described on slide of the SSL/TLS lecture. Say the encryption of pmk were changed from using a CCA-secure public-key encryption scheme to using a CPA-secure public-key encryption scheme. Which of the following attacks would this change potentially enable?

○ A、A passive eavesdropper can now learn pmk. In combination with NC and NB, this allows the attacker to recover mk.

● B、An attacker can eavesdrop on an execution of the protocol to learn the ciphertext c. Then, it can impersonate the client, send modified versions of c to the server, and learn pmk by using information about whether the server returns an error or not in response to these ciphertexts.

○ C、An attacker can impersonate the server by sending its own public key pk∗ to the client. By doing so, it can convince the client to encrypt pmk again, but this time using a public key for which the attacker can decrypt.

○ D、 A passive eavesdropper can now learn NC and NB. In combination with other known information, this allows the attacker to recover mk.

9. In this and the next question, assume the Schnorr identification protocol is run in the subgroup of Z∗23 generated by 2. (This subgroup has order 11.) Say the prover's private key is x=7. What is the prover's public key?

13

10. (This is a continuation of the previous question.) Say the prover runs an execution of the Schnorr identification protocol with a verifier. The prover chooses r=4 and sends A=16. The verifier sends challenge 3. What response does the prover send?

3

提交

举报