Quiz #3

Security and Privacy
Sept. 27, 2018

Name: **Student Number:**

1. Using session keys to perform encryption/decryption of messages is to _______.

(A) better protect the interchange keys 32 (60%)
(B) make encryption and decryption faster 13 (25%)
(C) alternate the use of session and interchange keys 1 (2%)
(D) make key management easier 4 (8%)
(E) none of the above 3 (5%)

2. In secret key based key exchange protocols, the use of a random number in a message almost always serves the purpose of ______________________.

(A) naming the message 2 (4%)
(B) specifying the type of the message 0
(C) relating messages to each other so as to identify attacking messages 49 (92%)
(D) counting the number of messages during key exchange 2 (4%)
(E) none of the above 0

3. In public key based key exchange, the main challenge for establishing a session key is how to ___________________.

(A) protect the session key 10 (19%)
(B) protect the privacy key 6 (11%)
(C) generate the correct private-public key pair 6 (11%)
(D) deliver the correct public key 31 (59%)
(E) none of the above 0

4. In public key based key exchange, _____ key is used to encrypt the session key.

(A) sender's private 0
(B) sender's public 5 (9%)
(C) receiver's private 19 (36%)
(D) receiver's public 29 (55%)
(E) none of the above 0

5. A public key in a certificate is certified by a CA through encryption using _____.

(A) the public key of the CA 8 (15%)
(B) the private key of the CA 44 (83%)
(C) a shared secret key 0
(D) the private key that corresponds to the public key 0
(E) none of the above 1 (2%)

6. PKI (public key infrastructure) is a common mechanism for ____________.

(A) distributing public keys in the form of certificates 52 (98%)
(B) exchanging session keys 1 (2%)
(C) encrypting and decrypting messages 0
(D) protecting private keys 0
(E) none of the above 0

7. The purpose of a standard, such as X.509 for PKI, is to ___________.

(A) develop the best solution to solve a technical problem 1 (2%)

(B) demonstrate that there exists a solution to a problem 1 (2%)

(C) force developers to follow the same way of solving a problem 22 (41%)

(D) ensure the interoperability of solutions to the same problem 28 (53%)

(E) none of the above 1 (2%)

8. A user may not be able to immediately accept a certificate signed by a CA that is different from his/her own CA mainly because ____________.

(A) the two CAs would never communicate with each other 1 (2%)

(B) the user may not yet know the public key of the CA that signs the certificate 41 (78%)

(C) there is no way for the user to accept the certificate 1 (2%)

(D) the user cannot possibly accept a certificate issued by another CA 10 (18%)

(E) none of the above 0

9. Secret key based cryptography CANNOT provide digital signature because __.

(A) secret keys are only used for protecting the confidentiality of messages 6 (11%)

(B) digital signature doesn't require encryption 0

(C) digital signature doesn't involve any key 1 (2%)

(D) every secret key is shared by nature and is thus not unique 41 (78%)

(E) none of the above 5 (9%)

Honor list (in alphabetical order): 3 (6%)

王亦凱　徐天元　于天宇

Absentees (in alphabetical order): 1 (2%)

吴瑀