Quiz #2

Security and Privacy
Sept. 20, 2018

Name: **Student Number**:

1. Which of the following statements CANNOT be correct?

(A) Cryptographic algorithms should remain open. 0
(B) Cryptographic algorithms cannot be kept secret. 6 (12%)
(C) Cryptographic keys must be well protected. 0
(D) Cryptographic keys cannot be shared. 44 (86%)
(E) None of the above. 1 (2%)

2. Transposition is one type of basic cipher operations for symmetric cryptography in which characters in the plain texts are _______________.

(A) encrypted one by one 0
(B) encrypted as a single unit 0
(C) exchanged in terms of their positions 51 (100%)
(D) replaced or dropped 0
(E) none of the above 0

3. Caesar cipher is a substitution cipher that can be broken by _____________.

(A) permuting characters 2 (4%)
(B) replacing every character with every other following the same rule 48 (94%)
(C) deciphering each and every character at a time 1 (2%)
(D) randomly guessing the original plain text 0
(E) none of the above 0

4. Running DES in the CBC mode would make it harder to break DES mainly because CBC mode ____________________.

(A) uses a different and stronger encryption algorithm 1 (2%)
(B) applies a different and longer key to perform encryption 4 (8%)
(C) makes cipher blocks interwind with each other 44 (86%)
(D) takes longer time to complete the encryption 2 (4%)
(E) none of the above 0

5. The purpose of the Diffie-Hellman key exchange algorithm is to ____________.

(A) generate a public key from a private key 0
(B) establish a shared secret key between two communicating parties 51 (100%)
(C) propose a method to protect the privacy key 0
(D) none of the above 0

6. It is said that RSA public key encryption was developed based on earlier work by Diffie and Hellman due primarily to the fact that the former inherited the following concepts from the latter.

(A) Public key. 8 (16%)
(B) Private key. 0
(C) The way in which encryption and decryption are performed. 5 (10%)
(D) All of the above are true. 38 (74%)

7. Public key-based encryption is not efficient mainly because ______________.

(A) it takes long time to generate the public and private key pair 16 (32%)

(B) encryption involves time-consuming computation 34 (66%)

(C) encryption algorithm is very complex in structure 1 (2%)

(D) such an encryption algorithm has not yet been developed 0

(E) none of the above 0

8. For message authentication using public key cryptography, encryption is applied to a message digest instead of the message itself because ___________.

(A) encrypting the message is not necessary 0

(B) encrypting the message can be time-consuming 0

(C) generating and encrypting the message digest is generally much faster than encrypting the message 4 (8%)

(D) all of the above 46 (90%)

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

Honor list (in alphabetical order): 18 (35%)

Bartkowski 蔡亦华 曹燕飞 冯泽琛 龚令华 **Gwizdz**

Labuzek 赖苡立 **Moylan** **Raman** 苏立梓 孙力 王亦凯

吴敬恒 吴亦锟 杨丽婷 姚健菁 张馨以

Absentees: 4 (7%)

白厚源 黄琚 温碧聪 吴瑀