M12A1Solution CSS 211/ CS 459 Spring 2020 Covers: Chapter 12 of textbook

DATE ASSIGNED: April 21, 2020 DATE DUE: April 24, 2020 POINTS: 25

[A, 9 points ] Multiple Choice

[A1] Cryptology is the study of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (c)

(a) making codes (b) breaking codes (c) both making and breaking codes

[A2] Transposition involves rearranging the order of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) plaintext (b) ciphertext

[A3] The interceptor should not be able to predict what will happen to the ciphertext

by changing one character in the plaintext. This characteristic is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) confusion (b) diffusion

[A4] The cipher should spread the information from the plaintext over the entire ciphertext.

This principle is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) confusion (b) diffusion

[A5] DES and AES are \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ encryption algorithms. (a)

(a) symmetric (b)asymmetric

[A6] RSA is a(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ encryption algorithm. (b)

(a) symmetric (b)asymmetric

[A7] ECCs require \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ keys than the RSA algorithm requires, for equivalent security. (a)

(a) shorter (b) longer

[A8] A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of substitution is its regularity. (b)

(a) strength (b) weakness

[A9] Security resulting from using the DES algorithm is based on the secrecy of \_\_\_\_\_\_\_\_\_\_\_\_\_\_.(b)

(a) the DES algorithm (b) keys

[B, 16 points] For each of the following, state if it is TRUE or FALSE.

[B1] Substitution achieves diffusion. (F)

[B2] Transposition achieves confusion. (F)

[B3] Most people should make up their own encryption and decryption schemes. (F)

[B4] The DES and AES algorithms have been released for public scrutiny. (T)

[B5] The Digital Signature Standard (DSS) uses the RSA algorithm. (F)

[B6] ECCs are in the public domain and can be used in place of the RSA algorithm for Public Key

Cryptography. (T)

[B7] The NSA (National Security Agency) develops codes and ciphers for US military and diplomatic

uses. (T)

[B8] The one time pad is a provably unbreakable encryption scheme. (T)

[B9] Quantum cryptography is based on physics, not mathematics. (T)

[B10] The DES algorithm uses keys which are 256 bits long, of which 8 bits are dropped. (F)

[B11] The AES algorithm uses keys of length 64 bits. (F)

[B12] Cryptographic hash function are one-way functions. (T)

[B13] Cryptographic hash function produce obvious collisions. (F)

[B14] Two cryptographic primitives are: substitution, transposition. (T)

[B15] The MD5 algorithm has a maximum message size of 2 ^ 32 bits. (F)

[B16] The MD5 algorithm has a digest size of 128 bits. (T)