CS5342 Network Security – Mid-term Spring 2023 (part 1)

Name: _____ Seat #: _____
Section (01 or D01): _____
R#:_____
Total credits: 30

1. (14 points) Multiple Choice, check all listed assertions that appear to be correct

(1) In message confidentiality, the transmitted message must make sense to only intended
A. receiver C. modular
B. sender D. translator

(2) In asymmetric cryptography, _____ key is used to sign a message, and _____ key is used to decrypt a ciphertext.
A. public, private C. private, private
B. private, public D. public, public

(3) A secure blockchain system can achieve multiple security requirements, which include _____.
A. Integrity C. Accountability
B. Availability D. Only A and B

(4) What operations can achieve diffusion and confusion in cryptography systems.
A. Substitution (S) C. Hybrid approach consisting of S and T
B. Transposition (T) D. Feistel cipher structure

(5) Which of the followings is a block cipher?
A. ECC (Elliptic-curve cryptography) C. AES
B. 3DES with two keys D. RC4

(6) Random Numbers have the following properties
A. Uniformity C. Unchangeable
B. Independence D. Unpredictable

(7) Public-key cryptography can provide_____.
A. Easy key distribution C. Digital Signature
B. Encryption D. None of the mentioned

	Q1	Q2	Q3	Q4	Q5	Q6	Q7
answers							

2. (7 points) False (F) or True (T)

(1) Public-key cryptography is much slower than symmetric-key cryptography.

(2) AES encryption fixes message size (plaintext) but uses different secret key lengths to guarantee levels of security.

(3) A common approach to communicating securely and quickly is first using symmetric-key cryptography to send a key, then using public-key cryptography to send message.

(4) In the stream cipher, a stream key can always be re-used since producing unlimited keys is unrealistic.

(5) RSA encryption without padding is secure since padding could cause side channel attack.

(6) We can trade-off between security and efficiency (i.e. cost & speed) when designing a commercially used cryptographic system. Security can be sacrificed to some extent.

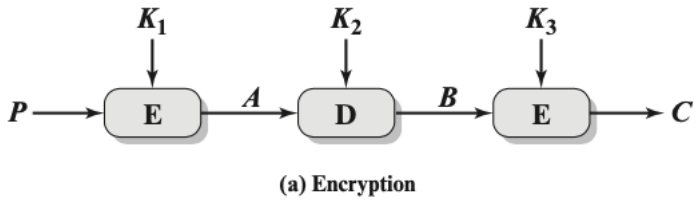
(7) If an attacker learns the internal state of an HMAC-based pRNG they can predict future outputs.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7
answers							

CS5342 Network Security – Mid-term Spring 2023 (part 2)

Name: _____ Seat #: _____
Section (01 or D01): _____
R#:_____
Total credits: 30

3. (3 points) Figure 1 shows the Triple DES encryption process. P is plaintext. C is ciphertext.



(a) Encryption

Figure 1

(1) Write the **decryption** equation

4. (4 points) Consider a very simple symmetric block encryption algorithm in which 64-bits blocks of plaintext are encrypted using a 192-bit key. Encryption is defined as

$$C = [(P \oplus K_1) \boxplus K_0] \oplus K_2$$

Where C = ciphertext, K = secret key, K_0 = leftmost 64 bits of K, K_2 = rightmost 64 bits of K, K = $K_0 || K_1 || K_2$ (from left to right), $\oplus$ = bitwise exclusive OR, and $\boxplus$ is addition mod 2^{64}, Show the decryption equation. That is show the equation for P as a function of C, K_0 and K_1.

5. (2 points) Write RSA encryption and decryption algorithms. Suppose the public key {d, n}, and private key {e,n} are given.

Encryption:

Decryption:

6. Bonus (2 points). In your assigned review paper 2, what network security problem was addressed?