QUEEN'S UNIVERSITY FINAL EXAMINATION
FACULTY OF ENGINEERING AND APPLIED SCIENCE
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

ELEC 473, 001 & Dr. Jianbing Ni
December 14, 2021

INSTRUCTIONS TO STUDENTS:
This examination is 3 HOURS in length.
There are 2 sections to this examination.
Please answer all questions in the exam

The following aids are allowed:
Casio FX-991 calculator

Put your student number on all pages of all exam papers
GOOD LUCK!

PLEASE NOTE:
Proctors are unable to respond to queries about the interpretation of exam questions.
Do your best to answer exam questions as written.

FULL NAME: _____

STUDENT ID: _____

Questions	Section I	Section II						Total
	1-30	Q1	Q2	Q3	Q4	Q5	Q6	
Points	1×30	10	15	10	13	10	12	100
Scores								

Answer Sheet of Section I

Questions	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Answers										
Questions	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20
Answers										
Questions	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30
Answers										

STUDENT ID:

Section I Multiple Choices - please mark the best answer (subtotal: 30 points).

1. RSA is designed by Rivest, Shamir, and Adleman in
A. 1975
B. 1976
C. 1977
D. 1978

2. Each block of a blockchain consists of which of the following?
A. A hash value of the previous block header
B. Timestamp
C. List of transactions
D. All of the above

3. Which of the following is not a block cipher operating mode?
A. ECB
B. CFB
C. GCM
D. OBF

4. Suppose a prime $p \equiv 3 \bmod 4$ and $a \in Z_p$. Which of the following is equivalent to a square root of a mod p?
A. $a^{p-1} \bmod p$
B. $a^{(p+1)/4} \bmod p$
C. $a^{(p+1)/2} \bmod p$
D. $a^{(p-1)/2} \bmod p$

5. Let C(K, M) denote a message authentication code function, produced for the message M and a shared key K. Let E(K, M) denote encryption of a message M with a key K, and let || denote the concatenation. If Alice sends to Bob the following information: $E(K_2, M) \,||\, C(K_1, E(K_2, M))$ where K_1 and K_2 are shared secret keys, it is
A. just message authentication
B. message authentication and confidentiality where authentication is tied to the plaintext
C. message authentication and confidentiality where authentication is tied to the ciphertext
D. message authentication and confidentiality where authentication is tied both to the plaintext and to the ciphertext

STUDENT ID:

6. TLS handshake protocol refers to
A. confirming that one of the many lines of communication between the sending client and receiving server is not already in use.
B. sending an electronic key attached to the message so that the receiving server can be unlocked as the message is coming in.
C. establishing a secure communication path between the message sender and receiver.
D. verifying that the message sender and message receiver have available communication channels that intersect in the middle.

7. How many bit-output is generated by MD5?
A. 128
B. 160
C. 256
D. 512

8. A sender must not be able to deny sending a message that was sent, it is known as
A. Message non-repudiation
B. Message integrity
C. Message confidentiality
D. Message sending

9. What is a blockchain?
A. A decentralized ledger on a peer-to-peer network
B. A type of cryptocurrency
C. An exchange
D. A centralized ledger

10. Which one of the following statements about hash function is incorrect?
A. If a hash function is strong collusion resistant, it must be second pre-image resistant.
B. If an adversary can solve the preimage problem of the hash function, he must be able to find a collusion.
C. If an adversary can find a collusion of the hash function, he must be able to solve the second pre-image problem.
D. If a hash function is weak collusion resistant, it must be second pre-image resistant.

11. Bitcoin is created by _____.
A. Saifedean Ammous
B. Satoshi Nakamoto
C. Vitalik Buterin
D. None of the above

12. Which one of the following statements about the TLS protocol is incorrect?
A. The alert protocol is used to convey TLS-related alerts to the peer entity.
B. TLS/SSL provides confidentiality, integrity, authentication, and availability for web security.
C. After the change cipher spec message, both the client and server use the newly negotiated cipher spec and keys to securely exchange the application data.
D. For TLS 1.2, the major version is 3, and the minor version is 3.

13. Which one of the following statements about the cipher suite:
TLS_ECDHE_RSA_with AES_256_GCM_SHA_384 is incorrect?
A. The ECDHE is used for key exchange.
B. RSA is used for public-key encryption
C. AES-256 is used for symmetric encryption
D. SHA-384 is the hash function

14. Which protocol provides authentication for packets at IP level?
A. AH
B. HTTPS
C. TLS/SSL
D. Kerberos

15. Which one of the following statements about the IPsec protocol is incorrect?
A. AH authenticates the IP payload but not the IP header in transport mode.
B. ESP encrypts and optionally authenticates the entire IP packet in transport mode.
C. AH header is inserted between the original IP header and a new outer IP header in tunnel mode.
D. ESP header is inserted after the original IP header and before the IP payload in transport mode.

STUDENT ID:

16. The maximum number of bitcoins that can be created is _____.
A. 11 million
B. 25 million
C. 21 million
D. 100 million

17. What is a node on the blockchain network?
A. A type of cryptocurrency
B. A blockchain
C. A computer/miner on a blockchain network
D. An exchange

18. What is the block cipher structure in DES?
A. Substitution-Permutation Network
B. Feistel Network
C. Rijndael
D. One-way Permutation

19. Give the following DES S-box, if the input is 100100, what is the output of the S-box?
A. 1110
B. 1101
C. 1000
D. 1001

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
01	0101	0100	0111	0110	0001	0000	0011	0010	1101	1100	1111	1110	1001	1000	1011	1010
10	1010	1011	1000	1001	1110	1111	1100	1101	0010	0011	0000	0001	0110	0111	0100	0101
11	1111	1110	1101	1100	1011	1010	1001	1000	0111	0110	0101	0100	0011	0010	0001	0000

20. Where is the bitcoin central server located?
A. Washington DC
B. Undisclosed Location
C. London
D. None of these

STUDENT ID:

21. What is the key length of AES?
A. 128 bits
B. 192 bits
C. 256 bits
D. All of the above

22. Which of the following attacks is passive attack?
A. Network traffic analysis
B. Replay attack
C. Denial of service
D. Message modification

23. Which of the following information is not public according to the Kerckhoffs' Law?
A. The encryption algorithm
B. The signing algorithm
C. The decryption algorithm
D. The secret keys

24. What of the following statements is incorrect?
A. The attacker has access to pairs of known plaintexts and their corresponding ciphertexts in known plaintext attacks.
B. The attacker has the ability to choose ciphertexts and to view their corresponding plaintexts in chosen plaintext attacks.
C. The attacker can choose what messages wants Alice to sign, and he knows both the messages and the corresponding signatures in chosen message attacks.
D. The attacker is given valid signatures for a variety of messages known by the attacker in known message attacks.

25. What is the period of m-sequence produced by the 100-stage LFSR?
A. 2^{100}
B. $2^{100}-1$
C. $2^{100}+1$
D. 2^{99}

26. Which of the following statements is incorrect?
A. If an adversary can address the RSA hard problem, it can factor the large integer n.
B. The large integer n factorization problem is equipment to the problem of computing φ(n) from n.
C. If an adversary can factor the large integer n, it can address the RSA hard problem.
D. The security of RSA is based on the hard problem of large number factorization.

27. Which of the following schemes can provide authenticity and integrity?
A. SHA-1
B. HMAC
C. 3DES
D. MD5

28. Which of the following statements is true?
A. Birthday attack attacks the strong collision resistance of hash function.
B. A hash function maps arbitrarily long strings to strings of variable length.
C. MD5 is a message authentication code.
D. If the attackers cannot use the exhaustive search attack to find the secret key, the MAC is secure.

29. Which of the following statements is false?
A. Session keys are used for symmetric-key encryption or MAC in sessions.
B. Two users can negotiate a session key over a public channel via a key agreement protocol.
C. A key distribution center chooses session keys and distributes them to users via an interactive session key distribution scheme.
D. The Diffie-Hellman key agreement protocol is insecure against meet-in-the-middle attacks.

30. Why can a message encrypted with the public key only be decrypted with the receiver's appropriate private key?
A. Not true, the message can also be decrypted with the public key.
B. A so called "trapdoor one-way function" is applied for the encryption.
C. The public key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate private key.
D. The encrypted message contains the function for decryption which identifies the private key.

STUDENT ID:

Section II (subtotal: 70 points).

Q1 (10 points).

a). In Bitcoin, why do the network nodes manage the blockchain?

b). How does Bitcoin mining work?

c). How does the Bitcoin ensure the anonymity of users?

d). What is the double spending problem with Bitcoin?

e). How does Bitcoin avoid double spending problem?

Q2 (15 points).

a). What are the functions offered by the TLS/SSL handshake protocol?
b). Describe the detailed processes of the TLS 1.2 handshake protocol (including 4 stages).

\

STUDENT ID:

Q3 (10 points). Define a toy hash function h: $(Z_2)^7 \rightarrow (Z_2)^4$ by the rule by $h(x) = xA$ where all operations are modulo 2 and

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Find all preimages of (0,1,0,1).

STUDENT ID:

Q4 (13 points). A common way to speed up RSA decryption incorporates the Chinese Remainder Theorem, as follows. Suppose that $d_k(y)=y^d \bmod n$ and $n=pq$. Define $d_p=d \bmod (p-1)$ and $d_q=d \bmod (q-1)$; and let $M_p=q^{-1} \bmod p$ and $M_q=p^{-1} \bmod q$. Then, consider the following algorithm:

Algorithm 1. CRT-Optimized RSA Decryption (n, d_p, d_q, M_p, M_q, y)
$x_p \leftarrow y^{dp} \bmod p$
$x_q \leftarrow y^{dq} \bmod q$
$x \leftarrow M_p q x_p + M_q p x_q \bmod n$
return (x)

The Algorithm 1 replaces an exponentiation modulo n by modular exponentiations modulo p and q. If p and q are l-bit integers and exponentiation modulo an l-bit integer takes time cl^3, then the time to perform the required exponentiation is reduced from $c(2l)^3$ to $2cl^3$, a saving of 75%. The final step, involving the Chinese Remainder Theorem, require $O(l^2)$ if d_p, d_q, M_p, and M_q have been pre-computed.

a). Prove that the value x returned by Algorithm 1 is, in fact, $y^d \bmod n$.

b). Given that p=15, q=23, and d=123, compute d_p, d_q, M_p, and M_q.

c). Given the above values of p, q, and d, decrypt the ciphertext y=17 using Algorithm 1.

STUDENT ID:

Q5 (10 points). Discuss whether the mutual authentication Protocol 1 is secure. If it is secure, give the security analysis; otherwise, present the attack and improve it to be secure. (Certificates are omitted from its description, but they are assumed to be included in the scheme in the usual way. $y = \mathbf{sig}_{Alice}(x)$ is Alice's signature of x, $\mathbf{ver}_{Alice}(x, y)$ is the verification of y on x using Alice's public key. $y = \mathbf{sig}_{Bob}(x)$ is Bob's signature of x, $\mathbf{ver}_{Bob}(x, y)$ is the verification of y on x using Bob's public key.)

Protocol 1: UNKNOWN PROTOCOL.

1. Bob chooses a random challenge, r_1, and he sends it to Alice.
2. Alice chooses a random challenge, r_2, she computes $y_1 = \mathbf{sig}_{Alice}(r_1)$, and she sends r_2 and y_1 to Bob.
3. Bob checks that $\mathbf{ver}_{Alice}(r_1, y_1) = true$; if so, then Bob "accepts"; otherwise, Bob "rejects." Bob also computes $y_2 = \mathbf{sig}_{Bob}(r_2)$ and he sends y_2 to Alice.
4. Alice checks that $\mathbf{ver}_{Bob}(r_2, y_2) = true$. If so, then Alice "accepts"; otherwise, Alice "rejects."

STUDENT ID:

Q6 (12 points). Here is a variation of the ElGamal Signature Scheme. The key is constructed in a similar manner as before: Alice chooses $\alpha \in Z_p^*$ to be a primitive element, $0 \le a \le p-2$ where $\gcd(a, p-1) = 1$, and $\beta = \alpha^a \bmod p$. The key $K = (\alpha, a, \beta)$, where α and β are the public key and a is the private key. Let $x \in Z_p$ be a message to be signed. Alice chooses $0 \le k \le p-2$ and computes the signature $\text{sig}(x) = (\gamma, \delta)$, where

$$\gamma = \alpha^k \bmod p,$$

and

$$\delta = (x - k\gamma)a^{-1} \bmod (p-1).$$

Answer the following questions concerning this modified scheme.

a). Describe how a signature (γ, δ) on a message x would be verified using Alice's public key.

b). Suppose that two people (say Alice and Bob) using this variation of the ElGamal Signature Scheme happen to use the same k-value to sign two messages. Additionally, we assume that Alice and Bob employ the same values of p and α. Alice has $\beta_1 = \alpha^{a_1} \bmod p$ and Bob has $\beta_2 = \alpha^{a_2} \bmod p$, where $|a_1 - a_2| \le c$, for some small constant $c \le 1000000$. Alice has created a signature (γ, δ_1) on a message x_1, and Bob has created a signature (γ, δ_2) on a message x_2. Then it is almost always possible for an adversary to easily compute Alice's and Bob's secret keys (a_1 and a_2, respectively), without solving the corresponding instances of the Discrete Logarithm problem.

Describe how an adversary can first compute $c = a_1 - a_2$ and then compute Alice's and Bob's secret keys (a_1 and a_2, respectively). Note that if c is small in absolute value, it is feasible to compute c from $\alpha^c \bmod p$.