PART TWO (MCQ): Choose the correct answer, and then fill the table with the chosen letter (30 Marks)

Q	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ANS															
Q	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
ANS															

1) _____ Assures that data and programs are changed only in a specified and authorized manner. (CLO 2.3)
a) Data integrity b) Data confidentiality c) Data availability d) Data authenticity

2) A loss of _____ is the unauthorized disclosure of information. (CLO 2.3)
a) Integrity b) Confidentiality c) Nonrepudiation d) Authenticity

3) _____ prevents either sender or receiver from denying a transmitted message (CLO 2.3)
a) Integrity b) Confidentiality c) Nonrepudiation d) Authenticity

4) gcd (8, 2) = _____ (CLO 1.1)
a) 1 b) 2 c) 3 d) 4

5) The number of positive integers less than n and relatively prime to n is known as _____. (CLO 2.3)
a) CRT b) Miller-Rabin c) Euler's totient function d) Fermat's theorem

6) If gcd (a, n) = 1, the value of ($a^{\Phi(n)+1} \bmod n$) is _____. (CLO 2.2)
a) a^{-1} b) n c) 1 d) a

7) In symmetric cryptography, which of the following MUST be true? (CLO 2.1)
a) Encryption and decryption take the same amount of time
b) Different algorithms are used for encryption and decryption
c) Cryptographic operations are one-way, and not reversible
d) The same key is used for encryption and decryption

8) The Caesar cipher is an example of _____ cipher. (CLO 2.1)
a) Transposition b) Product cipher c) Public key d) Substitution

9) The _____ cipher is based on the use of a 5 x 5 matrix of letters constructed using a keyword. Plaintext is encrypted two letters at a time using this matrix. (CLO 1.1)
a) Vigenere b) Playfair c) Caesar d) One-time pad

10) DES encrypts data in (CLO 1.1)
a) 64-bits blocks using a 64-bit key
b) 64-bits blocks using a 56-bit key
c) 32-bits blocks using a 56-bit key
d) 32-bits blocks using a 32-bit key

11) In each round i of encryption of the Feistel Structure, the round function F is applied to (CLO 2.2)
a) Right half of data then taking the exclusive or with the left half
b) Left half of data then taking the exclusive or with the right half
c) Left and right halves of data then taking the exclusive of the results
d) Original key then taking the exclusive of the result with the left half

12) The Data Encryption Standard (DES) is an example of _____ cipher. (CLO 2.1)
a) Transposition b) stream c) Public key d) block

13) Which of the following statements is NOT correct regarding '*seed*' and its requirements in context of cryptography applications? (CLO 2.2)
a) The seed serves as input to the PRNG.
b) The seed must be a random or pseudorandom number.
c) It is not recommended to generate the seed by a TRNG.
d) The seed must be secure and unpredictable.

14) Most of the recently developed _____ are based on the use of feedback shift registers (FSRs). (CLO 1.1)
a) Caesar Ciphers b) Entropy Sources
c) Block Ciphers d) Stream Ciphers

15) _____ is a variable key size stream cipher with byte-oriented operations that is based on the use of random permutation. (CLO 2.1)
a) Feistel Cipher b) RC4
c) Hash function d) DES

16) Which of the following is NOT an algorithm of public-key cryptosystems? (CLO 2.1)
a) RSA b) Diffie-Hellman
c) Elliptic curve d) DES

17) In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'? (CLO 2.2)
a) p and q should be divisible by Φ(n) b) p and q should be co-prime
c) p and q should be prime d) p/q should give no remainder

18) The security of RSA cryptosystem relies on the difficulty of _____. (CLO 2.4)
a) Discrete logarithms b) Factoring large number
c) Exponentiation d) S-box calculations

19) Discrete logarithm problem guarantees the security of _____ algorithm. (CLO 2.4)
a) RSA b) DES c) Miller-Rabin d) Diffie-Hellman

20) The _____ algorithm provides practical method for public exchange of session key for two parties. (CLO 2.3)
a) RSA b) DES c) El-Gamal d) Diffie-Hellman

21) The key exchange protocol that does Not authenticate its participants is vulnerable to a _____ attack. (CLO 2.4)
a) Mathematical b) Timing c) Chosen ciphertext d) Man-in-the-middl

22) A _____ accepts a variable length block of data as input and produces a fixed size value h = H(M). (CLO 1.1)
a) Hash resistance b) Hash value c) Hash function d) Hash code

23) The hash functions are mainly used for _____ applications. (CLO 2.3)
a) Data integrity b) Data compression
c) Data collision resistance d) Mapping messages

24) SHA-1 produces a hash value of _____ bits. (CLO 1.1)
a) 224 b) 160 c) 384 d) 256

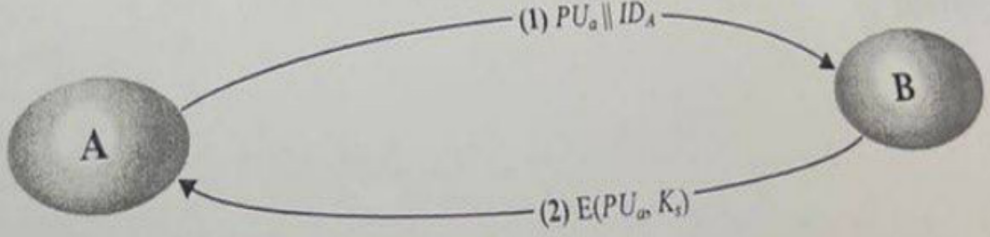
25) For digital signature scheme, the type of attack in which the adversary determines the user's private key is known as _____. (CLO 2.4)
a) Total break b) Universal forgery c) Existential forgery d) Selective forgery

26) Which one of the following is Not correct regarding digital signature? (CLO 2.4)
a) Used to authenticate message contents b) Can be verified by third party.
c) Used to verify the sender of the message. d) Can be verified using sender private key.

27) To verify the signature, the verification algorithm receives _____ as inputs. (CLO 2.3)
a) The message hash, the signature, and sender's public key.
b) The message hash and the signature.
c) The message hash, the signature, and sender's private key.
d) The message hash, the sender's private key, and sender's public key.

28) Which of the following key is used only once or at most is very short-lived. (CLO 2.1)
a) Ephemeral key b) Sequence key c) Master key d) Stream key

29) The protocol depicted in the following figure that uses a public-key encryption to establish a session key is insecure against _____ attack. (CLO 2.2)
a) Mathematical b) Timing c) Chosen ciphertext d) Man-in-the-middle



30) A ___ is shared by the KDC and an end system or user and used to encrypt the ___. (CLO 2.1)
a) Master key, session key b) Session key, master key
c) Master key, message d) Session key, message

With best w