قائمة الاسئلة

امتحان نهاية الفصل الدراسي الأول - للعام الجامعي 1446 هـ - الموافق 2025/2024م-كلية الحاسوب وتكنولوجيا المعلومات :: مقدمة في التش

1) Which of the following is NOT a common use of block cipher?
   1) - S-box
   2) - F-function
   3) + One-way trap-door function
   4) - Confusion and diffusion
2) In an asymmetric-key cipher, the sender uses the ……. Key.
   1) - private
   2) + public
   3) - Secret key
   4) - Public and private
3) A ……. cipher replaces one character with another character.
   1) + substitution
   2) - transposition
   3) - public-key
   4) - permutation
4) A diffusion technique is result from applied the …….
   1) - F-function
   2) - transposition
   3) - public-key
   4) + permutation
5) A modern cipher is usually a complex ……. cipher made of a combination of different simple ciphers.
   1) + round
   2) - circle
   3) - square
   4) - keyless
6) DES is a(n) ……. method adopted by the U.S. government.
   1) - Public-key
   2) - asymmetric-key
   3) + symmetric-key
   4) - Public-key and single-key
7) DES uses a key generator to generate sixteen …… round keys.
   1) - 32-bit
   2) + 48-bit
   3) - 54-bit
   4) - 42-bit
8) ……. is a round cipher based on the Rijndael algorithm that uses a 128-bit block of data.
   1) - AEE
   2) - DES
   3) - AER
   4) + AES
9) ……. DES was designed to increase the size of the DES key.
   1) - Double
   2) + Triple
   3) - Quadruple
   4) - Key length
10) ECB and CBC are ……. ciphers.

1) - square
2) + block
3) - stream
4) - field

11) One commonly used public-key cryptography method algorithm that is the …… algorithm.
1) - AES
2) - RAS
3) - ECB
4) + RSA

12) The ……. method provides a one-time session key for two parties.
1) + Diffie-Hellman
2) - RSA
3) - DES
4) - AES

13) A sender S sends a message m to receiver R, which is digitally signed by S with its private key. In this scenario, one or more of the following security violations can take place. (I) S can launch a birthday attack to replace m with a fraudulent message.
(II) A third party attacker can launch a birthday attack to replace m with a fraudulent message.
(III) R can launch a birthday attack to replace m with a fraudulent message.
Which of the following are possible security violations.
1) - (I) and (II) only
2) + (I) only
3) - (II) only
4) - (II) and (III) only

14) In a RSA cryptosystem, a participant A uses two prime numbers p=13 and q=17 to generate her public and private keys. If the public key of A is 35, then the private key of A is ……
1) - 15
2) - 7
3) + 11
4) - 25

15) Ahmad digitally signs a message and sends it to Mohammad. Verification of the signature by Mohammad requires.
1) + Ahmad's Public Key
2) - Mohammad's Public Key
3) - Mohammad's Private Key
4) - Ahmad's Private Key

16) Suppose that everyone in a group of N people wants to communicate secretly with the N-1 others using symmetric key cryptographic system. The communication between any two persons should not be decode able by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is
1) - 2N
2) - N(N-1)
3) + N(N-1)/2
4) - (N-1)2 Depart

17) AES uses a _____ bit block size and a key size of …… bits.
1) - 128; 128 or 256
2) - 64; 128 or 192
3) - 256; 128, 192, or 256
4) + 128; 128, 192, or 256

18) Like DES, AES also uses Feistel Structure.
1) - True .
2) + False .
3) - Maybe
4) - Can’t say

19) Which algorithm among was chosen as the AES algorithm?
1) - MARS
2) - Blowfish
3) - RC6
4) + Rijndael

20) How many rounds does the AES-256 perform?
1) + 10
2) - 12
3) - 14
4) - 16

21) What is the expanded key size of AES-192?
1) - 44 words
2) - 60 words
3) + 52 words
4) - 36 words

22) Which of the 4 operations are false for each round in the AES algorithm?
(i) Substitute Bytes
(ii) Shift Columns
(iii) Mix Rows
(iv) XOR Round Key
1) - (i) only
2) + (ii), (iii) and (iv)
3) - (ii) and (iii)
4) - only (iv)

23) Which of the following is false for ECB mode of operation?
(i) The Plain text is broken into blocks of size 128 bytes
(ii) ii) Blocks can be swapped, repeated, replaced without recipient noticing
(iii) Good for short data
(iv) Encryption of each block is done separately using a randomly generated key for each block
1) - (i) only
2) - (ii) and (iii)
3) + (i) and (iv)
4) - (i), (ii) and (iv)

24) There is a dependency on the previous ‘s’ bits in every stage in CFB mode. Here ‘s’ can range from …….
1) - 8-16 bits
2) + 8-32 bits
3) - 4-16 bits
4) - 8-48 bits

25) Which of the following can be classified under advantages and disadvantages of OFB mode?
(i) Transmission errors
(ii) A bit error in a ciphertext segment
(iii) Cannot recover from lost ciphertext segments
(iv) Ciphertext or segment loss

1) + Advantages: None; Disadvantages: All
2) - Advantages: All; Disadvantages: None
3) - Advantages: (i); Disadvantages: (ii), (iii) and (iv)
4) - Advantages: (i); (ii) Disadvantages: (iii) (iv)

26) In OFB Transmission errors do not propagate: only the current ciphertext is affected, since keys are generated “locally”.
1) + True
2) - False
3) - May be
4) - Can't say

27) Which of the following modes does not implement chaining or “dependency on previous stage computations”?
1) + CTR, ECB
2) - CTR, CFB
3) - CFB, OFB
4) - ECB, OFB

28) A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE?
(i) Sender encrypts using receiver’s public key
(ii) Sender encrypts using his own public key
(iii) Receiver decrypts using sender’s public key
(iv) Receiver decrypts using his own private key
1) - (i) only
2) - (ii) and (iii)
3) + (i) and (iv)
4) - (i), (ii) and (iv)

29) Which block mode limits the maximum throughput of the algorithm to the reciprocal of the time for one execution?
1) - OFB
2) + CTR
3) - CBC
4) - ECB

30) Which mode requires the implementation of only the encryption algorithm?
1) - ECB
2) - CBC
3) + CTR
4) - OFB

31) Which of the following modes of operation does not involve feedback?
1) + ECB
2) - CBC
3) - CTR
4) - OFB

32) What is the general equation for elliptic curve systems?
1) - $y^3 + axy + by = x^4 + cx^2 + dx + e$
2) - $y^3 + ax + by = x^3 + cx^2 + dx + e$
3) - $y^2 + axy + by = x^3 + cx^2 + e$
4) + $y^2 + axy + by = x^3 + cx^2 + dx + e$

33) Example of a Monoalphabetic cryptosystem.
1) + Shift cipher and Substitution cipher

2) - Vigenere cipher
3) - permutation
4) - all false

34) Example of a Polyalphabetic cryptosystem.
1) - Shift cipher
2) - Substitution cipher
3) - Affine cipher
4) + Vigenere cipher

35) Let P = C = Z_{26} .K consists of all possible permutations of the 26 symbols 0, 1, . . . , 25. Then how many possible Substitution cipher is possible?
1) + (a) 26!
2) - (b) 2^{26}
3) - (c) 52
4) - (d) 26

36) If plaintext is equal to ciphertext then the encryption function is .....?
1) - (a) Identity function
2) + (b) Permutation
3) - (c) Shift function
4) - (d) None of these

37) The …… cryptosystem is used in some form in a number of standards including the digital signature standard (DSS) and the S/MIME email standard.
1) + ElGamal
2) - Elliptic Curve
3) - RSA
4) - Knapsack

38) In the RSA public key cryptosystem, the private and public keys are (e,n) and (d,n) respectively, where n=p*q and p and q are large primes. Besides, n is public and p and q are private. Let M be an integer such that 0< M <n and Φ(n) = (p-1)(q-1). Now consider the following equations:
(I) M^'= M^e mod n;M=□(M')□^d mod n
(II) ed≡1 mod n
(III) ed ≡ 1 mod Φ(n)
(IV) M^'= M^e mod Φ(n); M= □(M^')□^d mod Φ(n)
Which of the above equations correctly represent RSA cryptosystem?
1) - (I) and (II)
2) + (I) and (III)
3) - (II) and (IV)
4) - (III) and (IV)

39) …… is showing up in standardization efforts, including the IEEE P1363 Standard for Public-Key Cryptography.
1) - ElGamal
2) - RSA
3) - Knapsack
4) + Elliptic curve cryptography (ECC)

40) …… appears to offer equal security of RSA for a far smaller key size.
1) - ElGamal
2) + Elliptic curve cryptography (ECC)
3) - Knapsack
4) - DES