CNS SHORT TYPE QUESTION:-

1. In brute force attack, on average half of all possible keys must be tried to achieve success.
a) True
b) False
View Answer
Answer: a
Explanation: In brute force attack the attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained.
2. If the sender and receiver use different keys, the system is referred to as conventional cipher system.
a) True
b) False
View Answer
Answer: b
Explanation: Such a system is called asymmetric, two-key, or public-key cipher system.
3. Divide (HAPPY)26 by (SAD)26. We get quotient –
a) KD
b) LD
c) JC
d) MC
View Answer
Answer: a
Explanation: Dividing (HAPPY)26 by (SAD)26 gives us KD with a remainder MLP.
4. Dividing (11001001) by (100111) gives remainder –
a) 11
b) 111
c) 101
d) 110
View Answer
Answer: d
Explanation: Dividing (11001001) by (100111) gives us (110).
5. pi in terms of base 26 is
a) C.DRS
b) D.SQR
c) D.DRS
d) D.DSS
View Answer
Answer: c
Explanation: On converting using base conversions we get 3.1415926 as D.DRS.
6. The time required to convert a k-bit integer to its representation in the base 10 in terms of big-O notation is
a) O(log2 n)
b) O(log n)
c) O(log2 2n)
d) O(2log n)
View Answer

Answer: a
Explanation: Let n be a k-bit integer in binary. The conversion algorithm is as follows. Divide 10 = (1010) into n. The remainder – which will be one of the integers 0, 1, 10, 11, 100, 101, 110, 11 1, 1000, or 1001 – will be the ones digit d0. Now replace n by the quotient and repeat the process, dividing that quotient by (1010), using the remainder as d1 and the quotient as the next number into which to divide (1010). This process must be repeated a number of times equal to the number of decimal digits in n, which is [log n/log 10] +1 = O(k).
We have O(k) divisions, each requiring O(4k) operations (dividing a number with at most k bits by the 4 bit number (1010)). But O(4k) is the same as O(k) (constant factors don't matter in the big-0 notation, so we conclude that the total number of bit operations is O(k). O(k) = 0(k2). If we want to express this in terms of n rather than k, then since k = O(1og n), we can write
Time(convert n to decimal) = 0(log2n).
7. In base 26, multiplication of YES by NO gives –
a) THWOE
b) MPAHT
c) MPJNS
d) THWAE
View Answer
Answer: c
Explanation: Convert the alphabets into their respective values in base 26 and proceed with base 26 multiplications.
8. Division of (131B6C3) base 16 by (IA2F) base 16 yeilds –
a) 1AD
b) DAD
c) BAD
d) 9AD
View Answer
Answer: d
Explanation: Base 16 division to be followed where A-F stand for 10-15.
9. An encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available.
a) True
b) False
View Answer
Answer: a
Explanation: The above statement is the definition for unconditionally secure cipher systems.
10. The estimated computations required to crack a password of 6 characters from the 26 letter alphabet is-
a) 308915776
b) 11881376
c) 456976
d) 8031810176
View Answer
Answer: a
Explanation: The required answer is 26^6 = 308915776.
11. Reduce the following big-O natations:
O[ $ax^7 + 3x^3 + \sin(x)$] =

a) O[$ax^7$].
b) O[sin(x)].
c) O[$x^7$].
d) O[$x^7 + x^3$].
View Answer
12. Reduce the following big-O natations:
O[ $e^n + an^{10}$] =
a) O[ $an^{10}$ ].
b) O[ $n^{10}$ ].
c) O[ $e^n$ ].
d) O[ $e^n + n^{10}$ ].
View Answer
13. Reduce the following big-O natations:
O [ $n! + n^{50}$ ] =
a) O [ $n! + n^{50}$ ].
b) O [ n! ].
c) O [ $n^{50}$].
d) None of the Mentioned
View Answer
Answer: b
Explanation: O [ $n! + n^{50}$ ] = O [ n! ].

1. Use Caesar's Cipher to decipher the following
HQFUBSWHG WHAW
a) ABANDONED LOCK
b) ENCRYPTED TEXT
c) ABANDONED TEXT
d) ENCRYPTED LOCK
View Answer
Answer: b
Explanation: Caesar Cipher uses C =(p+3) mod 26 to encrypt.
2. Caesar Cipher is an example of
a) Poly-alphabetic Cipher
b) Mono-alphabetic Cipher
c) Multi-alphabetic Cipher
d) Bi-alphabetic Cipher
View Answer
Answer: b
Explanation: Caesar Cipher is an example of Mono-alphabetic cipher, as single alphabets are encrypted or decrypted at a time.
3. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.
a) True
b) False
View Answer
Answer: b
Explanation: Monoalphabetic ciphers are easier to break because they reflect the frequency of the original alphabet.

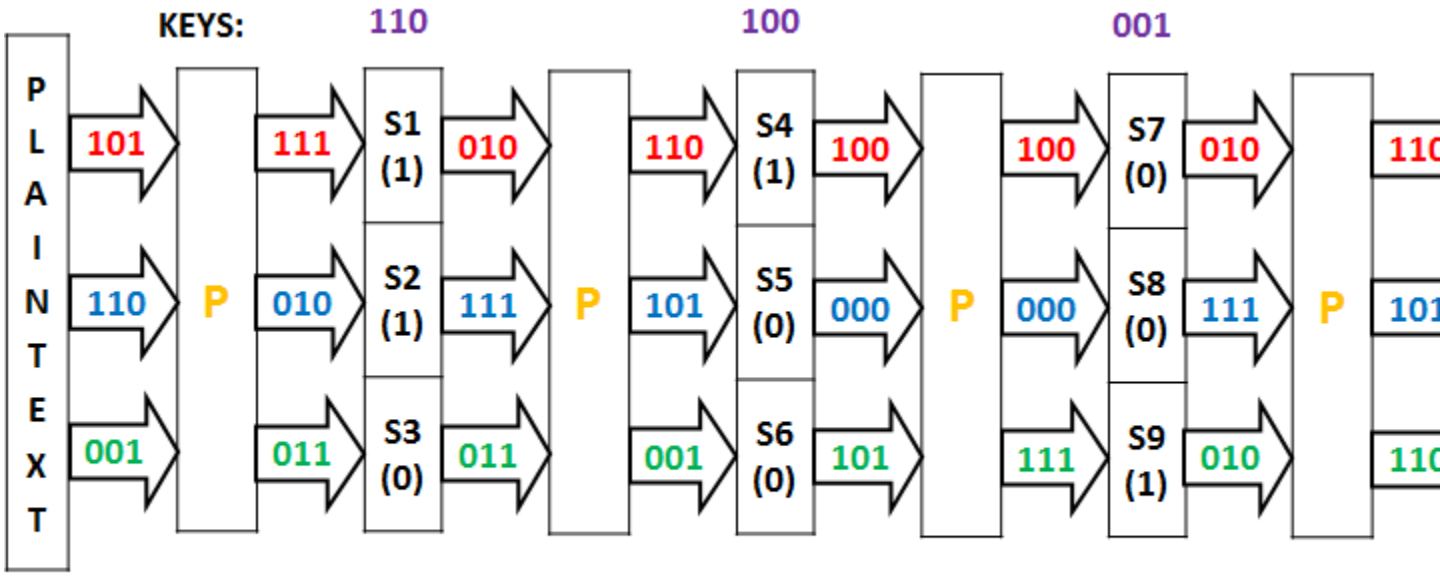
4. Which are the most frequently found letters in the English language ?
a) e,a
b) e,o
c) e,t
d) e,i
View Answer
Answer: c
Explanation: The relativity frequency of these letters in percent : e-12.702, a-8.167, t-9.056, i-6.996, o-7.507.
5. Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis.
a) Random Polyalphabetic, Plaintext, Playfair
b) Random Polyalphabetic, Playfair, Vignere
c) Random Polyalphabetic, Vignere, Playfair, Plaintext
d) Random Polyalphabetic, Plaintext, Beaufort, Playfair
View Answer
Answer: c
Explanation: Random Polyalphabetic is the most resistant to frequency analysis, followed by Vignere, Playfair and then Plaintext.
6. On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-
a) abqdnwewuwjphfvrrtrfznsdokvl
b) abqdvmwuwjphfvvyyrfznydokvl
c) tbqyrvmwuwjphfvvyyrfznydokvl
d) baiuvmwuwjphfoeiyrfznydokvl
View Answer
Answer: b
Explanation: Cipher text:= Ci = Pi + ki mod m (mod 26).
7. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text
a) nlazeiibljji
b) nlazeiibljii
c) olaaeiibljki
d) mlaaeiibljki
View Answer
Answer: a
Explanation: Cipher text:= Ci = Pi + ki mod m (mod 26).
8. The Index of Coincidence for English language is approximately
a) 0.068
b) 0.038
c) 0.065
d) 0.048
View Answer
Answer: c
Explanation: The IC for the English language is approximately 0.065.
9. If all letters have the same chance of being chosen, the IC is approximately
a) 0.065
b) 0.035
c) 0.048

d) 0.038
View Answer
10. Consider the cipher text message with relative frequencies:
4 0 10 25 5 32 24 15 6 11 5 5 1 2 6 6 15 19 10 0 6 28 8 2 3 2
The Index of Coincidence is
a) 0.065
b) 0.048
c) 0.067
d) 0.042
View Answer
Answer: c
Explanation: Number of letters = 250. From this, IC=0.0676627. This is very strong evidence that the message came from a Monoalphabetic ciphering scheme.
11.Consider the cipher text message:
YJIHX RVHKK KSKHK IQQEV IFLRK QUZVA EVFYZ RVFBX UKGBP KYVVB QTAJK TGBQO ISGHU CWIKX QUXIH DUGIU LMWKG CHXJV WEKIH HEHGR EXXSF DMIIL UPSLW UPSLW AJKTR WTOWP IVXBW NPTGW EKBYU SBQWS
Relative Frequencies –
3 7 2 2 5 5 7 9 11 4 14 4 2 1 3 4 6 5 6 5 7 10 9 8 4 2
The Index of Coincidence is –
a) 0.065
b) 0.048
c) 0.067
d) 0.044
View Answer
Answer: d
Explanation: Number of letters = 145.From this, IC=0.0438697 .This is very strong evidence that the message came from a polyalphabetic ciphering scheme.
12. A symmetric cipher system has an IC of 0.041. What is the length of the key ‘m’?
a) 1
b) 3
c) 2
d) 5
View Answer
Answer: d
Explanation: Using the formula for calculating ‘m’ we get m=5, where m≈0.027n/(I_c (n-1)-0.038n+0.065).

1. In affine block cipher systems if f(m)=Am + t, what is f(m1+m2) ?
a) f(m1) + f(m2) + t
b) f(m1) + f(m2) + 2t
c) f(m1) + t
d) f(m1) + f(m2)
View Answer
Answer: a
Explanation: In general f(∑(i=1 to n) m_i = ∑(i=1 to n) f(m_i) + tδ_n) where δ_n=0 if n is odd and 1 if n is even.

2. In affine block cipher systems if f(m)=Am + t, what is f(m1+m2+m3) ?
a) f(m1) + f(m2) + f(m3) + t
b) f(m1) + f(m2) + f(m3) +2t
c) f(m1) + f(m2) + f(m3)
d) 2(f(m1) + f(m2) + f(m3))
View Answer
Answer: c
Explanation: In general f(∑(i=1 to n) m_i =∑(i=1 to n) f(m_i ) + tδ_n) where δ_n=0 if n is odd and 1 if n is even.
3. If the block size is ‘s’, how many affine transformations are possible ?
a) $2^s$ $(2^s-1)(2^s-1)(2^s-1^2)……(2^s-1^{(s-1)})$
b) $2^s$ $(2^s-1)(2^s-2)(2^s-2^2)……(2^s-2^{(s-2)})$
c) $2^s$s $(2^s-1)(2^s-2)(2^s-2^2)……(2^s-2^{(s-1)})$
d) $2^s$ $(2^s-1)(2^s-2)(2^s-2^2)……(2^s-2^{(s-3)})$
View Answer
Answer: c
Explanation: $2^s$ $(2^s-1)(2^s-2)(2^s-2^2)……(2^s-2^{(s-1)})$ is the maximum number of affine transformations possible for a block size ‘s’ matrix.
4. What is the number of possible 3 x 3 affine cipher transformations ?
a) 168
b) 840
c) 1024
d) 1344
View Answer
Answer: d
Explanation: Since ‘A’ cannot have columns of ‘0’s. so there are ‘7’ choices i.e. 001/010/011/100/101/110/111. ‘a1’ is chosen for first column of ‘A.
We have ‘6’ choices for second column, let ‘a2’ be chosen for second column.
The final column can be any 3-tuple except 0, a1, a2, a1+a2. That means any one of the remaining ‘4’ 3-tuples may be chosen for the final column.
(Total number of@ possibilities for A)}=k=7×6×4=168
(Number of affine@ block cipher transformation)}=k×t=8×168 =1344
5. Super-Encipherment using two affine transformations results in another affine transformation.
a) True
b) False
View Answer
Answer: a
Explanation: f(g(m))=A_1 g(m)+c_1
f(g(m))=A_1 (A_2 m+c_2)+c_1 f(g(m))=A_1 A_2 m+A_1 c_2+c_1 f(x)=A_3 m+c_3
where
A_3=A_1 A_2
c_3=A_1 c_2+c_1
This results in another affine transformation, and does not improve the security.
6. If the key is 110100001, the output of the SP network for the plaintext: 101110001 is
a) 110100011
b) 110101110
c) 010110111

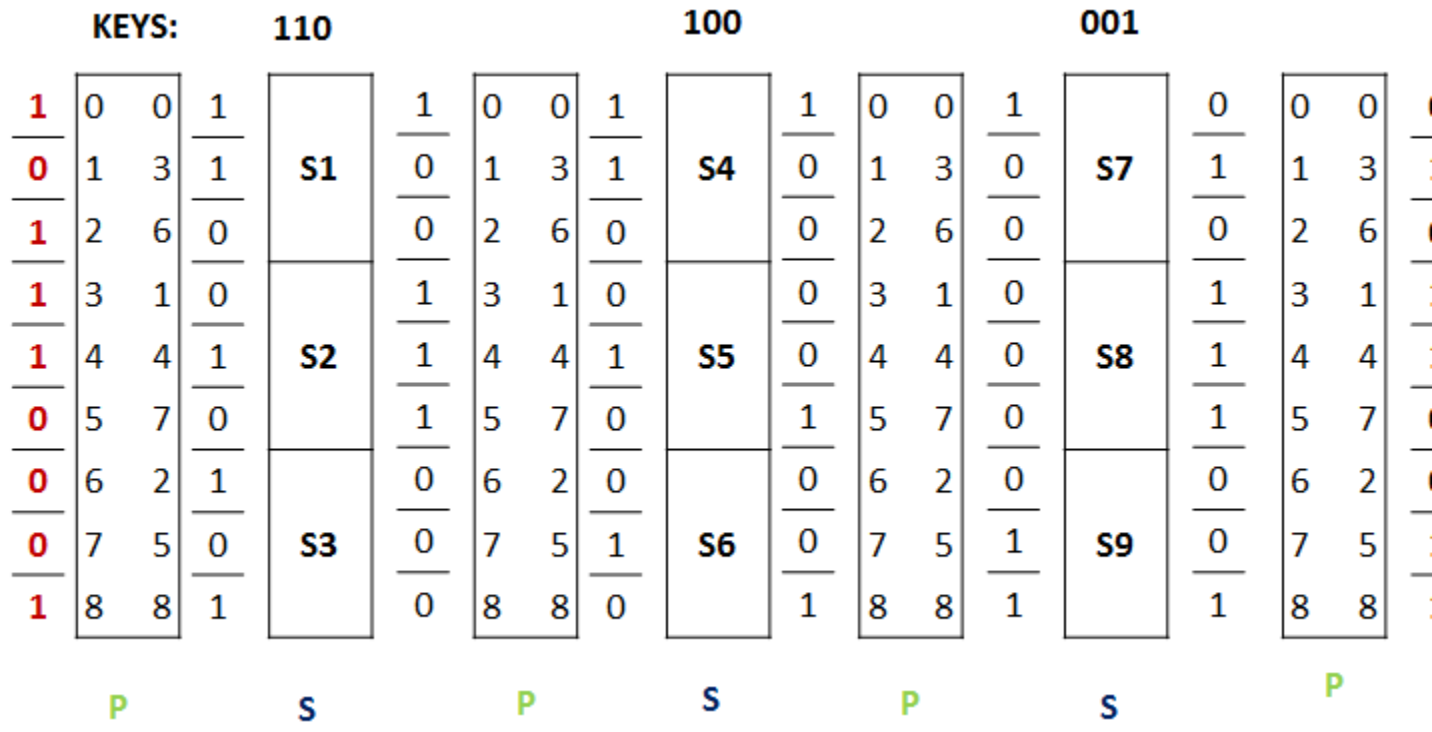
d) 011111010
View Answer
Answer: b
Explanation:




**Ciphertext is: 110101110**

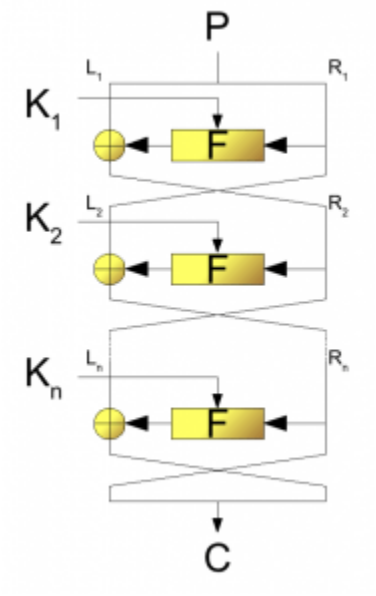
7. If the key is 110100001 where,
If ki=0, then S_i (x)=((1 1 0 | 0 1 1 | 1 0 0 ))x+((1 1 1))
and If ki=1, then S_i (x)=((0 1 1 | 1 0 1 | 1 0 0))x+((0 1 1))
then the output of the SP network for the plaintext: 101110001 is
a) 010110011
b) 111000011
c) 110110111
d) 010110110
View Answer

Answer: a
Explanation:




8. Confusion hides the relationship between the ciphertext and the plaintext.
a) True
b) False
View Answer
Answer: b
Explanation: Confusion hides the relationship between the ciphertext and the key.
9. The S-Box is used to provide confusion, as it is dependent on the unknown key.
a) True
b) False
View Answer

10. This is an example of




a) SP Networks
b) Feistel Cipher
c) Hash Algorithm
d) Hill Cipher
View Answer
Answer: b
Explanation: The figure is the Feistel Cipher Structure.
11. Which of the following slows the cryptographic algorithm –
1) Increase in Number of rounds
2) Decrease in Block size
3) Decrease in Key Size
4) Increase in Sub key Generation
a) 1 and 3
b) 2 and 3
c) 3 and 4
d) 2 and 4
View Answer
Answer: b
Explanation: Increase in any of the above 4 leads to slowing of the cipher algorithm i.e. more computational time will be required.

1. What is the size of the key in the SDES algorithm?
a) 24 bits
b) 16 bits
c) 20 bits
d) 10 bits
View Answer
Answer: d
Explanation: The size of the key in the SDES algorithm is 10 bits.

2. Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K1?
a) 10100100
b) 01011011
c) 01101000
d) 10100111
View Answer
Answer: a
Explanation: The permuted key P10 = 1000001100. Input to P8: 0000111000 and K1 is 10100100.
3. Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K2?
a) 10100111
b) 01000011
c) 00100100
d) 01011010
View Answer
Answer: b
Explanation: Input to P8: 0010000011 and K2 is 01000011.
4. The Ciphertext for the Plaintext 01110010, given that the keys K1 is 10100100 and K2 is 01000011 is
a) 01110111
b) 10010110
c) 01010110
d) 01000101
View Answer
Answer: a
Explanation: Perform the SDES algorithm and compute the cipher text.
5. The Ciphertext for the Plaintext 11010101, given that the key is 0111010001 is
a) 00010001
b) 10110010
c) 11010010
d) 01110011
View Answer
Answer: d
Explanation: Perform the SDES Encryption algorithm and compute the cipher text.
6. The Plaintext for the Ciphertext 00100010, given that the key is 1111111111 is
a) 01100111
b) 00001010
c) 01001000
d) 01001100
View Answer
Answer: d
Explanation: Perform the SDES Decryption algorithm and compute the cipher text.
7. In SDES, Encryption algorithm can be written as a composition of functions:
IP-1 o fK2 o fK1 o SW o IP
a) True
b) False
View Answer
Answer: b
Explanation: The SDES algorithm follows the order – IP-1 o fK2 o SW o fK1 o IP.

8. Assume input 10-bit key, K: 0010010111 for the SDES algorithm. What is K1?
a) 00101111
b) 01011011
c) 01101000
d) 10100111
View Answer
Answer: a
Explanation: The permuted key P10 = 1000010111. Input to P8: 0000101111 and K1 is 00101111.
9. The Plaintext for the Ciphertext 00001111, given that the key is 1111111111 is
a) 01100111
b) 00001010
c) 11111111
d) 01101101
View Answer
Answer: c
Explanation: Perform the SDES Decryption algorithm and compute the cipher text.
10. The Plaintext for the Ciphertext 11110000, given that the key is 0000000000 is
a) 01100111
b) 00000000
c) 01001000
d) 01101100
View Answer
Answer: b
Explanation: Perform the SDES Decryption algorithm and compute the cipher text.
11. Assume input 10-bit key, K: 0010010111 for the SDES algorithm. What is K2?
a) 11101010
b) 11011011
c) 01101000
d) 10101111
View Answer
12.The Plaintext for the Ciphertext 10100101, given that the key is 0010010111 is
a) 01100111
b) 00110110
c) 01001000
d) 01001100
View Answer
Answer: b
Explanation: Perform the SDES Decryption algorithm and compute the cipher text.

This set of Cryptography Multiple Choice Questions & Answers (MCQs) focuses on “Number Theory”.
1. If a|b and b|c, then a|c.
a) True
b) False
View Answer

Answer: a
Explanation: The statement is true. For ex, 11|66 and 66|198 = 11|198.
2. GCD(a,b) is the same as GCD(|a|,|b|).
a) True
b) False
View Answer
Answer: a
Explanation:This is true. gcd(60,24) = gcd(60,-24) = 12.
3. Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
a) 882
b) 770
c) 1078
d) 1225
View Answer
Answer: c
Explanation: GCD(1160718174, 316258250) = 1078.
4. Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm.
a) 11
b) 12
c) 8
d) 6
View Answer
Answer: d
Explanation: GCD(102947526, 239821932) = 6.
5. Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm.
a) 13
b) 12
c) 17
d) 7
View Answer
Answer: a
Explanation: GCD(8376238, 1921023) = 13.
6. What is 11 mod 7 and -11 mod 7?
a) 4 and 5
b) 4 and 4
c) 5 and 3
d) 4 and -4
View Answer
Answer: d
Explanation:11 mod 7 = 4 ; -11 mod 7 = -4 mod 7 = 3 mod 7.
7. Which of the following is a valid property for concurrency?
a) a = b (mod n) if n|(a-b)
b) a = b (mod n) implies b = a (mod n)
c) a = b (mod n) and b = c (mod n) implies a = c (mod n)
d) All of the mentioned
View Answer
Answer: d
Explanation: All are valid properties of congruences and can be checked by using substituting values.

8. [(a mod n) + (b mod n)] mod n = (a+b) mod n
a) True
b) False
View Answer
Answer: a
Explanation: The equivalence is true and can be checked by substituting values.
9. [(a mod n) – (b mod n)] mod n = (b – a) mod n
a) True
b) False
View Answer
Answer:b
Explanation:The equivalence is false and can be checked by substituting values. The correct equivalence would be [(a mod n) – (b mod n)] mod n = (a – b) mod n.
10. $11^7$ mod 13 =
a) 3
b) 7
c) 5
d) 15
View Answer
Answer: d
Explanation: The correct answer is 2. Or in this case 15 mod 13 = 2.
11. The multiplicative Inverse of 1234 mod 4321 is
a) 3239
b) 3213
c) 3242
d) Does not exist
View Answer
Answer: a
Explanation: The multiplicative Inverse of 1234 mod 4321 is 3239.
12. The multiplicative Inverse of 550 mod 1769 is
a) 434
b) 224
c) 550
d) Does not exist
View Answer
Answer: a
Explanation: The multiplicative Inverse of 550 mod 1769 is 550.
13. The multiplicative Inverse of 24140 mod 40902 is
a) 2355
b) 5343
c) 3534
d) Does not exist
View Answer
Answer: d
Explanation: The multiplicative Inverse does not exist as GCD (24140, 40902) = 34
1. DES follows
a) Hash Algorithm
b) Caesars Cipher
c) Feistel Cipher Structure

d) SP Networks
View Answer
Answer: c
Explanation: DES follows Feistel Cipher Structure.
2. The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key
a) 12
b) 18
c) 9
d) 16
View Answer
Answer: d
Explanation: The DES Algorithm Cipher System consists of 16 rounds (iterations) each with a round key.
3. The DES algorithm has a key length of
a) 128 Bits
b) 32 Bits
c) 64 Bits
d) 16 Bits
View Answer
Answer: c
Explanation: DES encrypts blocks of 64 bits using a 64 bit key.
4. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.
a) True
b) False
View Answer
Answer: b
Explanation: 56 bits are used, the rest 8 bits are parity bits.
5. In the DES algorithm the round key is _____ bit and the Round Input is _____bits.
a) 48, 32
b) 64,32
c) 56, 24
d) 32, 32
View Answer
Answer: a
Explanation: The round key is 48 bits. The input is 32 bits.
6. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
a) Scaling of the existing bits
b) Duplication of the existing bits
c) Addition of zeros
d) Addition of ones
View Answer
Answer: a
Explanation: The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits (permutation plus an expansion), that involves duplication of 16 of the bits.

7. The Initial Permutation table/matrix is of size
a) 16×8
b) 12×8
c) 8×8
d) 4×8
View Answer
Answer: c
Explanation: There are 64 bits to permute and this requires a 8×8 matrix.
8. The number of unique substitution boxes in DES after the 48 bit XOR operation are
a) 8
b) 4
c) 6
d) 12
View Answer
Answer: a
Explanation: The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.
9. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.
a) True
b) False
View Answer
Answer: b
Explanation: Every 8th bit is ignored to shorten the key length.

1. During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.
a) True
b) False
View Answer
2. A preferable cryptographic algorithm should have a good avalanche effect.
a) True
b) False
View Answer
Answer: a
Explanation: Thus statement is true as a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect.
3. The number of tests required to break the DES algorithm are
a) $2.8\times10^{14}$
b) $4.2\times10^{9}$
c) $1.84\times10^{19}$
d) $7.2\times10^{16}$
View Answer
Answer: d
Explanation: There are $2^{56}$ keys $=7.2\times10^{16}$.
4. The number of tests required to break the Double DES algorithm are
a) 2112
b) 2111

c) 2128
d) 2119
View Answer
Answer: b
Explanation: For Double DES key is 2112 bits, should require 2111 tests to break.
5. How many keys does the Triple DES algorithm use?
a) 2
b) 3
c) 2 or 3
d) 3 or 4
View Answer
Answer: c
Explanation: For Triple DES we can either have 2 or 3 keys.
Using two keys: c = Ek1(Dk2(Ek1(m)))
Using three keys: c = Ek3(Ek2(Ek1(m))).
6. In triple DES, the key size is ___ and meet in the middle attack takes ___ tests to break the key.
a) 2192 ,2112
b) 2184,2111
c) 2168,2111
d) 2168,2112
View Answer
Answer: d
Explanation: The key size is 2168 and meet in the middle attack takes 2112 tests to break.
7. Using Differential Crypt-analysis, the minimum computations required to decipher the DES algorithm is
a) $2^{56}$
b) $2^{43}$
c) $2^{55}$
d) $2^{47}$
View Answer
Answer: d
Explanation: Differential Crypt-analysis requires only $2^{47}$ computations to decipher the DES algorithm.
8.Using Linear Crypt-analysis, the minimum computations required to decipher the DES algorithm is
a) $2^{48}$
b) $2^{43}$
c) $2^{56}$
d) $2^{64}$
View Answer
Answer: b
Explanation: Linear Crypt-analysis requires only $2^{43}$ computations to decipher the DES algorithm.
1. GCD(a,b) = GCD(b,a mod b)
a) True
b) False
View Answer

Answer: a
Explanation: The statement is true. For example, GCD(55,22) = GCD(22,55 mod 22) = GCD(22,11) = 11
Consider the Following properties Properties
G-i) Closure
G-ii) Associative
G-iii) Identity Element
G-iv) Inverse Element
G-v) Commutative
Consider the Following properties Properties
R-i) Closure under multiplication
R-ii) Associativity of multiplication
R-iii) Distributive Law
R-iv) Commutativity of multiplication
R-v) Multiplicative Identity
R-vi) No zero divisors
R-vii) Multiplicative Inverse
2. All groups satisfy properties
a) G-i to G-v
b) G-i to G-iv
c) G-i to R-v
d) R-i to R-v
View Answer
Answer: b
Explanation: Group G denoted by {G,o}, is a set of elements that satisfy the properties G-i to G-iv.
3. An Abelian Group satisfies the properties
a) G-i to G-v
b) G-i to R-iv
c) G-i to R-v
d) R-i to R-v
View Answer
Answer: a
Explanation: An Abelian group is a group that satisfies the Commutative property also.
4. A Ring satisfies the properties
a) R-i to R-v
b) G-i to G-iv
c) G-i to R-v
d) G-i to R-iii
View Answer
Answer: d
Explanation: A ring R denoted by {R, + , x} is a set of elements with two binary operations addition and multiplication and satisfy axioms G-i to R-iii.
5. A Ring is said to be commutative if it also satisfies the property
a) R-vi
b) R-v
c) R-vii
d) R-iv
View Answer

Answer: d
Explanation: A Ring is said to be commutative if it also satisfies the property R-iv: Commutativity of multiplication.
6. An ‘Integral Domain’ satisfies the properties
a) G-i to G-iii
b) G-i to R-v
c) G-i to R-vi
d) G-i to R-iii
View Answer
Answer: c
Explanation:An ‘Integral Domain’ satisfies the properties G-i to R-vi.
7. A Field satisfies all the properties above from G-i to R-vi.
a) True
b) False
View Answer
Answer: a
Explanation: A Field satisfies all the properties above from G-i to R-vi and is denoted by {F, +, x}.
8. In modular arithmetic : (a/b) = b(a^-1)
a) True
b) False
View Answer
Answer: b
Explanation: This statement is not true. The correct version would be : $(a/b) = a(b^{-1})$.
9. a.(b.c) = (a.b).c is the representation for which property?
a) G-ii
b) G-iii
c) R-ii
d) R-iii
View Answer
Answer: a
Explanation: a.(b.c) = (a.b).c represents the Associative property.
10. a(b+c) = ac+bc is the representation for which property?
a) G-ii
b) G-iii
c) R-ii
d) R-iii
View Answer
Answer: d
Explanation: a(b+c) = ac+bc represents the Distributive Property.
11. For the group Sn of all permutations of n distinct symbols, what is the number of elements in Sn?
a) n
b) n-1
c) 2n
d) n!
View Answer
Answer: d
Explanation: There there are n distinct symbols there will be n! elements.

12. For the group Sn of all permutations of n distinct symbols, Sn is an abelian group for all values of n.
a) True
b) False
View Answer
Answer: b
Explanation: For n>2 it does not form a Abelian Group.
13. Is S a ring from the following multiplication and addition tables?
+ a b x a b
a a b a a a
b b a b a b
a) Yes
b) No
c) Can’t Say
d) Insufficient Data
View Answer
Answer: a
Explanation: S is a ring as it satisfies the properties G-i to R-iii.
14. Does the set of residue classes (mod 3) form a group with respect to modular addition?
a) Yes
b) No
c) Can’t Say
d) Insufficient Data
View Answer
Answer: a
Explanation: Yes. The identity element is 0, and the inverses of 0, 1, 2 are respectively 0, 2, 1.
15. Does the set of residue classes (mod 3) form a group with respect to modular addition?
a) Yes
b) No
c) Can’t Say
d) Insufficient Data
View Answer
Answer: b
Explanation: No. The identity element is 1, but 0 has no inve