CNS-LA1

Total points 6/20

Answer all 20 Questions. It will be evaluated to 10 Marks.

0 of 0 points

USN *

a

Name *

s

Section *

● A

○ B

○ C

CNS LA1

6 of 20 points

✗ 9 * 0/1

_______________number of times DES encryption algorithm is used in triple DES

○ 48

● 16 ✗

○ 3

○ 2

✓ 20 * 1/1

What are the characteristics of signature based IDS?

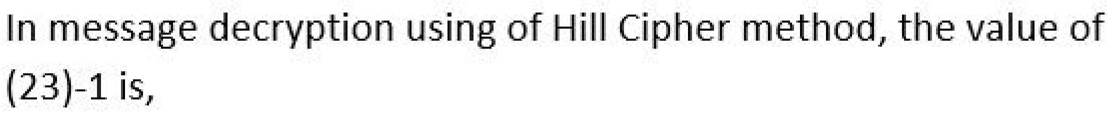
● Most are based on simple pattern matching algorithms ✓

○ It is programmed to interpret a certain series of packets

○ It models the normal usage of network as a noise characterization

○ Anything distinct from the noise is assumed to be intrusion activity

✗ 4 * 0/1



In message decryption using of Hill Cipher method, the value of (23)-1 is,

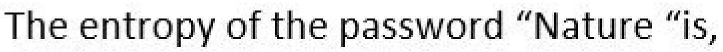
● 3 ✗

○ 26

○ 17

○ 23

✗ 1 * 0/1



The entropy of the password "Nature "is,

● 30.6 bits ✗

○ 28.2 bits

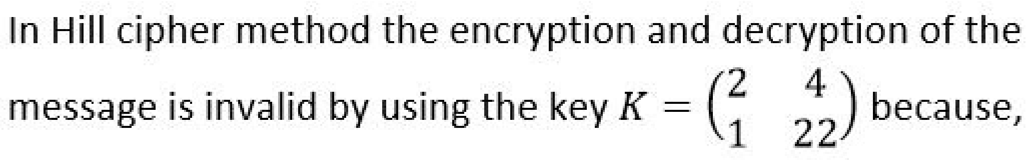
○ 39.6 bits

○ 34.2 bits

Feedback

The correct answer is right because x, y, z

✗ 2 * 0/1



In Hill cipher method the encryption and decryption of the message is invalid by using the key $K = \begin{pmatrix} 2 & 4 \\ 1 & 22 \end{pmatrix}$ because,

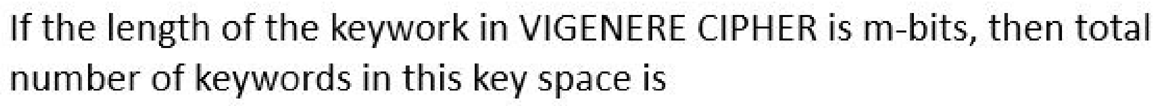
● None ✗

○ GCD (|K|, 26) =1

○ (|K|, 26) are relatively prime numbers

○ (|K|, 26) are not relatively prime numbers

✗ 11 * 0/1



If the length of the keywork in VIGENERE CIPHER is m-bits, then total number of keywords in this key space is

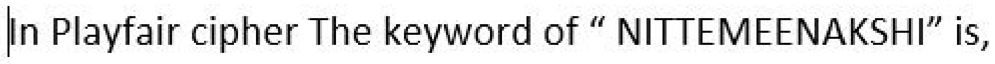
● m! ✗

○ 2^m

○ m^2

○ 26^m

✓ 3 * 1/1


In Playfair cipher The keyword of “ NITTEMEENAKSHI” is,

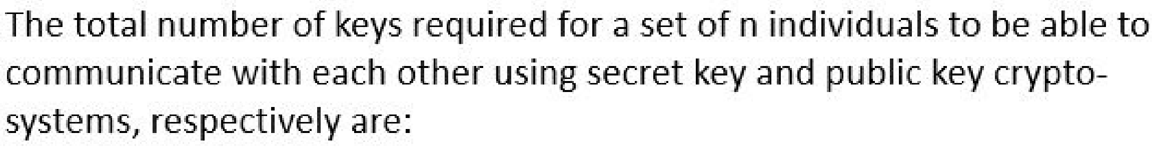
● NITEMNAKSH ✓

○ NITTEMNAKSHI

○ NITEMENAKS

○ NONE

✗ 12 * 0/1


The total number of keys required for a set of n individuals to be able to communicate with each other using secret key and public key crypto-systems, respectively are:

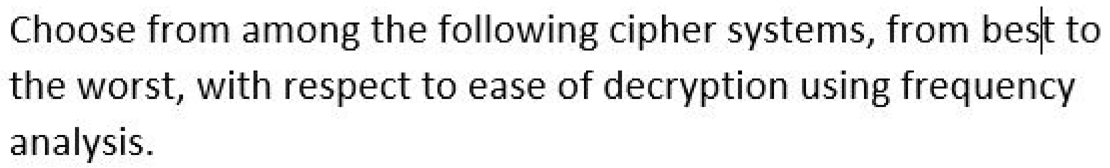
● n(n-1) and 2n ✗

○ 2n and ((n(n – 1))/2)

○ ((n(n – 1))/2) and 2n

○ ((n(n – 1))/2) and n

✕ 17 * 0/1



Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis.

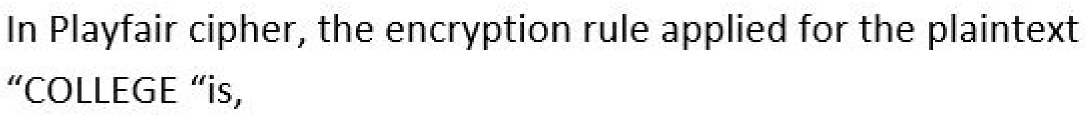
● Polyalphabetic, Plaintext, Playfair ✕

○ Polyalphabetic, Playfair, Vignere

○ Polyalphabetic, Vignere, Playfair, Plaintext

○ Polyalphabetic, Plaintext, Beaufort, Playfair

✓ 5 * 1/1



In Playfair cipher, the encryption rule applied for the plaintext “COLLEGE “is,

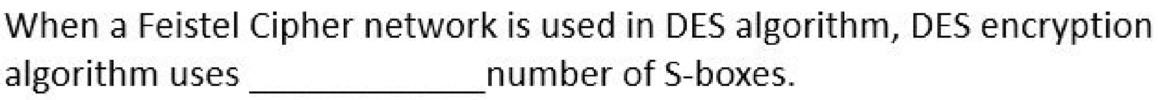
● CO LX LE GE ✓

○ CO LL EG EX

○ CO LL EG E

○ COLLEGE

✗ 10 * 0/1



When a Feistel Cipher network is used in DES algorithm, DES encryption algorithm uses ______________number of S-boxes.

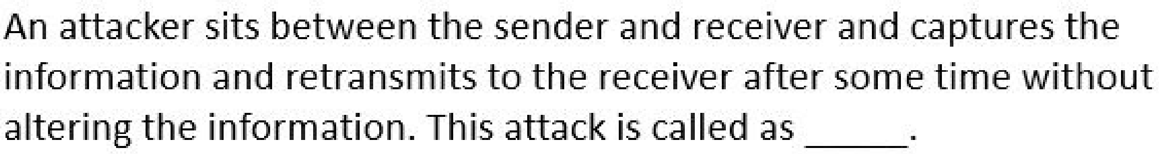
● 16 ✗

○ 12

○ 8

○ 6

✓ 14 * 1/1



An attacker sits between the sender and receiver and captures the information and retransmits to the receiver after some time without altering the information. This attack is called as ______.

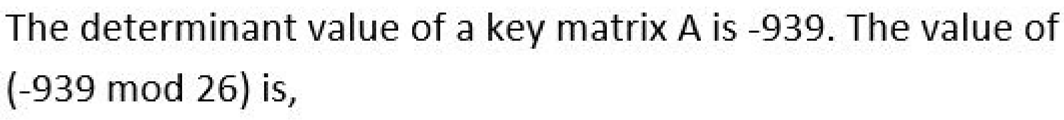
● DoS attack ✓

○ Masquarade attack

○ Simple attack

○ Complex attack

✗ 6 * 0/1


The determinant value of a key matrix A is -939. The value of (-939 mod 26) is,

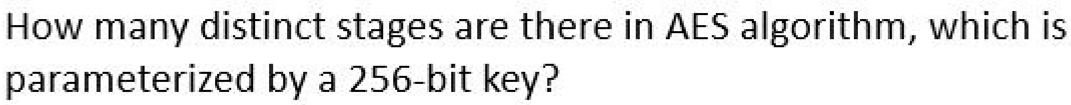
● -3 ✗

○ 23

○ 26

○ 939

✗ 13 * 0/1


How many distinct stages are there in AES algorithm, which is parameterized by a 256-bit key?

● 16 ✗

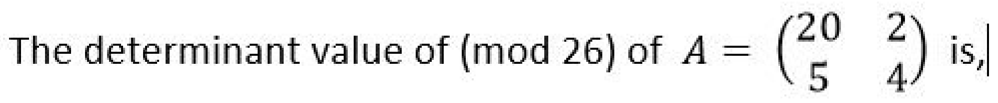
○ 14

○ 12

○ 10

✗ 8 *

0/1



The determinant value of (mod 26) of $A = \begin{pmatrix} 20 & 2 \\ 5 & 4 \end{pmatrix}$ is,

● 10 ✗

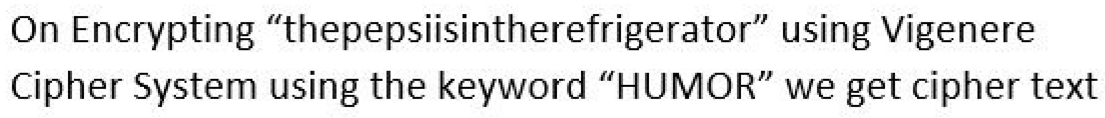
○ 12

○ 18

○ 16

✗ 18 *

0/1



On Encrypting “thepepsiisintherefrigerator” using Vigenere Cipher System using the keyword “HUMOR” we get cipher text

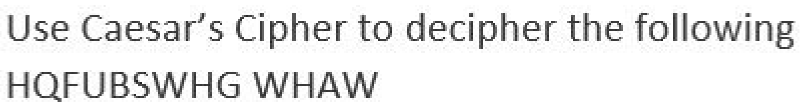
● abqdnwewuwjphfvrrtrfznsdokvl ✗

○ abqdvmwuwjphfvvyyrfznydokvl

○ tbqyrvmwuwjphfvvyyrfznydokvl

○ baiuvmwuwjphfoeiyrfznydokvl

✗ 16 * 0/1



Use Caesar's Cipher to decipher the following
HQFUBSWHG WHAW

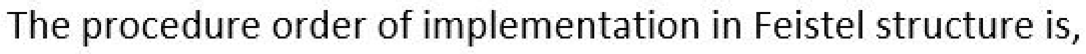
● ABANDONED LOCK ✗

○ ENCRYPTED TEXT

○ ABANDONED TEXT

○ ENCRYPTED LOCK

✓ 7 * 1/1



The procedure order of implementation in Feistel structure is,

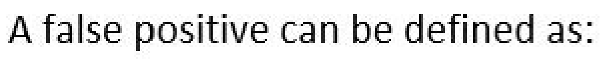
● Block size, Permutation, Round function, Swapping, Inversion ✓

○ Block size, Round function, Permutation, Inversion, Swapping

○ Block size, Permutation, Swapping, Round function, Inversion

○ Block size, Round function, Swapping, Inversion, Permutation

✓ 19 * 1/1



A false positive can be defined as:

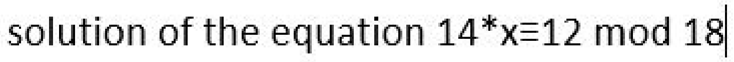
● An alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behavior ✓

○ An alert that indicates nefarious activity on a system that, upon further inspection, turns out to truly be nefarious activity

○ The lack of an alert for nefarious activity

○ All of the above

✗ 15 * 0/1



solution of the equation 14*x≡12 mod 18

● 12 ✗

○ 10

○ 8

○ 6

This form was created inside of Nitte Meenakshi Institute of Technology.

Google Forms