CNS FOCUS ANSWER

1.Why is asymmetric cryptography bad for huge data? Specify the reason?

Ans- Because asymmetric crypto algorithms are slower and more CPU intensive than symmetric. Because of this , they are not well suited to bulk message encryption, but they are a great way to exchange symmetric keys.

II) It's computationally expensive and slow due to the complex mathematical calculations involved in key generation, encryption, and decryption.

2.Convert the given text "COMPUTERSCIENCE " Into cipher text using Rail fence Technique?

Ans- Plaintext: C O M P U T E R S C I E N C E

Depth-2

C M U E S I N E

O P T R C E C

1st row-CMUESINE

2nd row-OPTRCEC

Ciphertext: C E S M R T U O I E N P C

3.Encrypt the plain text " follow the second route" with given secret key "DANCE" by using vigenere cipher?

Ans- Plain text:- f o l l o w t h e s e c o n d r o u t e

V: 5 14 11 11 14 2219 74 18 4 2 1413 3 17 14 20 19 4

K: D A N C E D A N C E D A N C E D A N C E

V: 3 0 1 3 2 4 3 0 1 3 2 4 3 0 1 3 2 4 3 0 1 3 2 4

C: 18 14 24 13 18 25 19 20 6 22 7 2 07 15 7 20 14 33 21 8

V: i o y n s z t u g w h c b p h u o h v i

Cipher text:- i o y n s z t u g w h c b p h u o h v i

4.Discuss the properties that are satisfied by Groups and fields?

Ans- Closure:- The result of any operation between group elements stays within the group, ensuring predictable outcomes.

Associativity:-Group operations are associative, making it easier to combine operations in encryption processes .

Identity Element:- There is an element that does not change other elements, ensuring stability.

Inverse Element:- Each element has an inverse ,allowing for reversible operations, crucial in decryption.

Fields:-

1.Commutative groups for addition and multiplication:-Both operations must be commutative ,aiding symmetric operations in encryptions.

2.Distributivity:- Ensures that encryption/decryption processes are efficient, particularly in polynomial - based cryptographic schemes like AES.

5.Explain Ring with an example?

Ans-A ring is a set with two binary operations that satisfy certain properties. It is a ring is a mathematical structure used to perform operations like addition and multiplication , which are essential in many cryptographic algorithms.

Ex:- In RSA encryption, the set of integers modulo n forms a ring.

Here:- Addition:- a + b mod n.

Multiplication:- A * b mod n .