| | Roll No. 41163 |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Page No |
| | Date: / / |
| | Asignment B4 |
| | Execution Pate: 14/05/2021 |
| | Submission Note: 21/05/2021 |
| * V | |
| 15. | |
| | |
| | Problem Stulement: |
| | to implement RSA algorithm |
| | |
| | Objectives: |
| | Leon busic concepts of RSA |
| | Imprement RSA algorithm |
| | |
| | Outcomes: |
| | Students will be able to understand and implement |
| | RSA algorithm. |
| | |
| | |
| | Software Reguirements: |
| | - Jupyter Notebook |
| | - Pymon 3.8.5 |
| | - 64 bit operating system : |
| | |
| | Mordware Requirements: |
| | - Computer with 64 bit processor |
| | |
| | the state of the s |
| | |
| | |
| | |
| | a a |
| | |



Theory: RSA is one of the hist public lay cappo system

and is widely used for secure clote transmission.

It is a public key encryption algorithm. It is a block cipher which converts plain text into cipher text at sender side and vice a larsa at Heeiners side.

A user of RSA exceles and publishes a public key based on two large prime numbers. The prime numbers must be Kept secret.

RSA is relatively slow algorithm, because of this, it is less commonly used to encypt user duty, more often RSA posses encypted shored key for symmetric key cryptography which in turn can perform bulk encryption operations at much higher speed.

Algorianm:

Select the two prime numbers where a = b

Compute n= a*b

Compute \$(n) = (0-1) *(b-1)

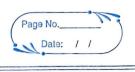
Select e such mot e is a coprime of $\beta(n)$ i.e. $\gcd(e, \beta(n)) = 1$ and $1 \le e \le \beta(n)$

Calculate private key of such must

(e #d) mod . \$(n) = 1



n= 2* 7 = 14



lot p= 3

: c=permod n = 35 mod 14 = 243 mod 14

C=5

For decryption ps cd mod n

= 5" mod n = 48828125 mod 14

fest cases:

Mes cription

1) dry with rondon Get decrypted sent which is some as prime numbers

Expected Op

pluin text

2) Pay with giren Cret decorpted tent which is some as.

pluin Hext, R=5. & dell

Conclusion:

example a:2,5=7

Therefore, we have successfully completed and implemented RSA algorithm.

Actual OIP

Successful

Successful