POFFE Assignment - 01 * Air > Write a program in 0++ on Java to implement RSA algorithm for key generation and apter verification To be the state of Objective - To study: - 1 Concept of public and private kery 2. Public key algorithm 3. Werking of RSA algorithm indicated the state of the state of Jan + Theory + - Asspronetrio 1 Public kery Algorithm : Public - key algorithms were evolved to - solve the public of key distribution in symmetric absorithms. This is achieved by using different keys for encryption and decryption. A public key encryption scheric has 6 components: 1. Plaintent - Readable ressage or data that is god as input 2. Encryption algorithm - Performs various transformations on the - plaintent 3. Public and private key - Pair of selected kerys one is used for enoughtion, and the other of for decryption 4. aphertent - Scrambled ressage produced as output of plaintent reand that keize = The service = files 5. Decryption algorithm = Accepts + aphen tent and the ratching key and prioduces the original plan plaintent. put for est - (it - et a maine mainte de Tett A-15 3 T-11) es RSA Algorithm; RSA stands - for Rivert, Sharin and Adleran & - who first 14-1 publically described it - RSA involves 3 steps - key generation energytron and decryption. = +31- 22 F - greet) stronger = 5 FET, +7 - greet filler RSA is a block apper with each block having a binary value less than - some number n, 1-e 1- block - size & log_n Enoughtion - 5 0 0 M Mod n Decryption - EM V C Mod n = + Til c - aphertent M - plaintent block

mycompanion 43304 1. Both sender and necesser know the value of n. 2. Only the sender knows the value of e 3. Only the necesser knows the value of d. Fried for filler to from the front of the state of · Algorithm 5 1. Choose 2 distinct prive numbers p and q. 2. Compute n v pa 3. Compute of ln) - lp-D * (q-1) = where of is Euler's totrent function 4. Choose an integer e such that ite (fin) and ged (e, p(n)) or 1 -, i.e., e and p(n) are co-prive 5. Determine do e-1 mod of no ine , d is the multiplicative inverse of e mod of (n) Public kery - PV = 3e, n3 - Private kery - PR - 2d, n3 1- 1-1 i fit fit m- fine garage Encryption > C & Mr moder in Decryption > Misi-cd - moding = 111 instrument and the secretary of the former 1. select 2 princ numbers, po- 17 and go 11 2. Calculate no par of 19 x 11 0 187 3- Calculate (n) = (p-) (q-1) = 10 × 10 0 160 4. Select e such that relatively prime to \$100 and less than of (n); we choose e====: 10001. 5. Détermine d'such that de = 1 (mod-160) and d < 160. The correct value of d is 23. 5 because 23 * 7 0 161 0 160+1 . The resulting keys are :-Public kery = 37,1873 Private kery = 323, 1875 Input - Input PT 17 , 9 T-1) ST PV + 7, 187 plaintent = 88 The second of the second of should trating -1: Just in -

7-7-1	mycompanion 43304
*	Conclusion - Tens in this assignment, we learnt about
	the working of RSA algorithm and implemented a program
	to demonstrate the same.
	ar to a getting the second of
	The state of the s
	The state of the s
	y of my
	reg to the property of the
	April of the state
	and the second of the second o
T E-1	
	The state of the s