Project Report

Name: Abeer Hussein Mohamed section: 1 BN: 34

Implementation of RSA:

I implemented it like the textbook

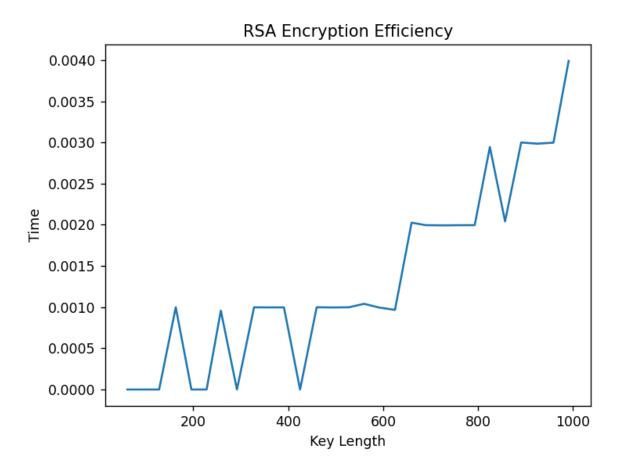
Project Report 1

RSA Algorithm:
KOA AGSTICKTO
1-Select P.9 (both are primes)
2- Calculate n = pxq
3- Calculate &(n) = (p-1)(q-1)
4- Select integer e Coprime with O(n) -> gcl(e,O(n))=1
1 <e<\(\gamma(n)\)< td=""></e<\(\gamma(n)\)<>
5 - Calculate d d=e-mod ocr)
6- publickey PU= Ze, n3
7- private kay pR = {d,n}
28 = 88 km * 5
for Confidintiality,
C = Me mod n
M= Cd mod h
Control of the later of the second of the se

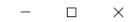
Implemented the communication using python socket.

Why the CCT happens: because the decryption of C-dash (the cipher with another random number) = Y, is easy due to the fact that e and d are inverses so Y = M*r mod e

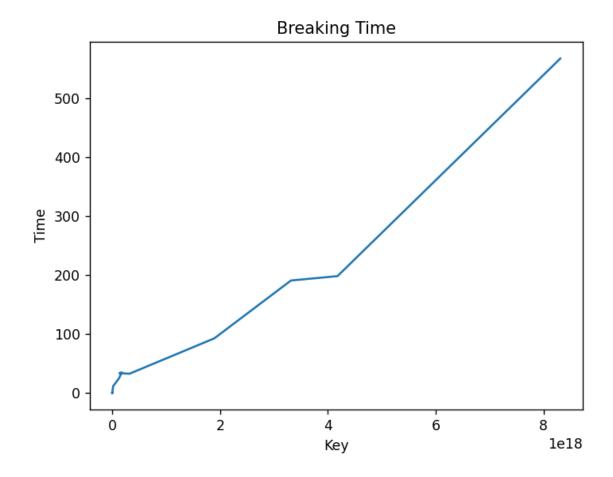








4



Project Report