Jessica Braganza
BE comp 2 PAGE NO: PITUS 151 DATE:
F17112151 DATE;
1c9 Resignment 6
17 Explain in brief working of RSA Algorithm
Ans. The RSA Algorithm is an asymmetric vyptography algorithm,
this means that it was a public key and a private key
Cie. two different mathematically linked keys?
- Following steps highlight the working of RSA Algorithm.
is Generating the keys
- solut two large prime numbers, a and y. The prime numbers
need to be large so that they will be difficult for someone
to figure out.
- latitate n= x+4
- calculate the totlest function; $\phi(n) = (x-1)(y-1)$
- select an integer e, such that e is 10-prime to \$(n) and I < e < \$(n)
The pair of numbers (n,e) makes up the public key.
- Calculate d such that the e,d = 1 med ()(n)
dean be found using the extended cuilidean algorithm. The pair
(n,d) makes up the private key.
ay Enoughtien
- Given a plaintant P, supresented as a number, the eighertext C is
calculated as: $C = P^2 \mod n$
calculated as
ay Decryption:
그리아 하루를 즐겁게 하셨다. 그리아 이렇게 하는데 어머니는 이렇게 하는데 얼마나가 나면 하는데 되었다면 되는데 아니는데 되는데 되었다면 되는데 그렇게 하는데 아들이 아들이 아들이 되었다.
- using the private key (n,d), the plaintext can be found using!
P: c ⁴ mod n
by Give mathematical imposednce of Euler's Tottent Function.
Ans - Euler's totient function wounts the positive Integers upto a given integers
n that are relatively prime to n. it is conitten using Greek letter
phi as d(n)

- it is the number of integers k in the range 1 < k < n for which
- It is the name of the ord (n k) is equal to 2.
the greatest common dinson ged (n, k) is equal to 1.
- The integers to of this form are sometimes referred to as
totatives of n.
- It is a multiplicative function, meaning that it two numbers
m and n are relatively prime, then & (mn) = \phi(m). \phi(n).
- This function gives the order of the multiplicative group of
integers modulo n:
The state of the s
34 Pexform encryption and decryption using the RSA algorithm
For the following: p=3, 9=11, e=7, M=5
n=prq = 3 x 11 = 33
$f(n) = (p-1)(q-1) = 2 \times (0.5) = 20$
Carlow when there is a manage of the life time to require the large of the second
Now, we need to compute d= e-1 mod f(n) by using backward
substitution of act algorithm:
Audiding to aco:
20=7#2+6
7 = 6 *1 + 1
6 = 1 +6 + 0
Therefore, we have
1=7-6=7-(20-7+2)=7-20+7+2=-20+7+3
Hence, we get d = e' mod f(n) = e' mod 20 = 3 mod 30 = 3
so the public key is \$ 7,33 } and the private key is \$3,33 } _
PBA enoughton and decayption is as follows:
Course Securition
Plaintext Cuphenkar Plaintext Plaint
PH = (9, 33)
ay conat is one way function in RSA oxyptooystem?
Ans - Gre-way function is a Function that is carry to compute but

F 10 12 13

	computationally have to sevence.
	1. Easy to calculate f(x) from x.
	2. Haved to invent 1 to calculate & from f(x).
	- There is no proof that one way functions exist on even real
	evidence that they can be wonstructed.
	- Even so, there are examples that seem one way, they are early
-	to compute but we know of no easy way to reverse them.
	for example, x2 is easy to compute but 21/2 is not
	- One way functions are used in pseudomandom generatores.
	st what is trapdoor in RSA?
	Ans - Trapdoor one-way functions are types of one-way functions
-	that contain a kind of "back door" (trapdoor)
n y sapariju ve ara p ila n	- As in the case of excinary one-way functions it is easy to
	compute their values for given data but it is very difficult
	to compute their inverse functions.
	- However, if one has some additional secret information, helshe
	can easily compute the invovese function as well
-y-sz-spekkis	- A mapdoor one-way function is easy to compute but computationally
	hand to severse.
manager of depth	1. Easy to calculate (xe mod n) from x.
-	2. Hard to invert : to colculate a from (xe mod n)
	- Examples of such hapdoon one-way Punctions may be
-	finding the prime factors of large numbers.
No. of the last	
The second special second	