encryption systems report

Divya Mehta

June 2024

1 Introduction

This document is about three encryption schemes rsa ,pallier,elgamel.Algorithms ,security mechanisms,features,key generation,encryption and decryption is explained in this document. Every method has a different mathematical model involved to keep the text secure.the common thing between them is use of prime numbers

1. RSA scheme
   This scheme involves use of two large prime numbers p and q

   $$n = p * q$$

   $$w = (p - 1) * (q - 1)$$

   now we need a encryption exponent e,we need to have e such that e and w are relatively prime

   now we have a public key,

   $$(n, e)$$

   now we need to calculate a decryption exponent such that,

   $$d * e \equiv 1 * mod(w)$$

now we have the private key,

$$(n, d)$$

we encrypt it using public key, let m be message

$$c \equiv m^e mod(n)$$

we can decrypt the message ,c is encrypted message

$$m \equiv c^d mod(n)$$

2. PALLIER scheme
   This has two prime numbers having same conditions as above,

$$n = p * Q$$

$$w = (p-1) * (q-1)$$

$$g = n + 1$$

we have our public key

$$(n, g)$$

$$k * w \equiv mod(n)$$

now we have a private key,

$$(n, w, k)$$

now we can encrypt the message m,

$$c \equiv g^m * r^n mod(n^2)$$

$$d \equiv c^w mod(n^2)$$

$$e = (d-1)/n$$

now we can decrypt th message ,

$$e * k \equiv mmod(n)$$

3. ELGAMAL scheme
   This involves a selection of a prime number p
   Now need to select a primitive root b,primitive root of a prime number is a number when sum of remainder of raise to of b less than the divider is same as divider
   Then we need a non negetive number a less than p

$$d \equiv b^a mod(p)$$

   now public key is

$$(p, b, d)$$

   you need a number k greater than 0 and less than p-1,let message be m

$$(b^k, m * d^K) = (h, j)$$

   encryption has two parts,

$$(z, x) \equiv (h, j) mod(p)$$

   to decrypt the message,

$$m \equiv h^{p-1-a} mod(p)$$