DESIGN.pdf

Githika Annapureddy

February 2023

1 keygen

Produces a public and private key pair.

First, we generate two really large prime numbers p and q.
We use make_prime() to generate a number then use is_prime() to verify that it is prime.
The rules of the SS Algorithm are such that
1. p cannot divide (q-1)
2. q cannot divide (p-1)
Once we find a p and q that satisfy these conditions, we use the formula
n = p*p*q
to find n.

n is our public key. We use it to encrypt the message. The reason this cryptography method works is because no one can factor n in factorial time. n's only factors are p and q, which are both really large prime numbers.
In code, this is done using void ss_make_pub(p, q, n, nbits, iters)
Once n is found, we need to find d. d is the private key.

2 encrypt

Encrypts file using public key.

3 decrypt

Decrypts file using private key.
To decrypt the file, we have to find a d such that the (encrypted message to the d-th power) mod n equals the original message.

4 functions

bool is_prime(n, iters)
indicates whether or not n is prime. used to create two really large prime numebrs: p and q.
void make_prime(p, bits, iters)
generates a prime number which needs to be tested by is_prime()