PROJECT CS-254

Spring 2017

RSA and BLOWFISH

Submitted by
Bandaru Harsha Vardhan,Ganesh Raj

Under the guidance of
Dr. Kapil Ahuja

Department of Computer Science and Engineering
Indian Institute of Technology Indore
Simrol, India

Index

1. Motivation

- Data Integrity
- Data Confidentiality
- Data Authentication
- Access Control over Data
- Resist Against Eavesdroppers
- Many More

Figure 1.1:

2. Cryptography

2.1 Simple Definition

Study of secure communications techniques.

2.2 Past Most Used Methods

- Substitution
- Transposition
- Some algorithms are emerged but Many Failed because security depends on secrecy of algorithms.This technique is called Restricted Algorithms.

So paths emerged for the techniques in which security depends on secrecy of key not on the secrecy of algorithms.

2.3 Cryptography Types

Present Days,Cryptographic Key is used to Encrypt and Decrypt.Based on that cryptography is divided into two types,they are

- Asymmetric
- Symmetric

Now a days cryptographic keys are produced by pseudorandom key generators.

2.4 Symmetric Cryptography

In Symmetric Cryptography,same cryptographic key is used to Encrypt and Decrypt message. Types are:

- Block: Encryption takes place on blocks of message and produces same cipher under similar conditions
- stream: Encryption takes place on every single bit of message and produces different cipher under similar conditions

Examples: IDEA(International Data Encryption Algorithm) ,DEA(Data Encryption Algorithm) ,AES(Advanced Encryption Standard).

2.5 BLOWFISH

Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard now receives more attention. Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the ageing DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial/government secrets..Uses Variable key size and 64 bit symmetric block cipher.Blowfish consist of two parts.

- Key-expansion part(generation of sub-keys from key)
- Data- encryption part

Algorithm:

- p array consist of 18 32-bit subkeys
- p1,p2....
- There are four s-boxes of 32-bit with 256 entries for sub-keys
- Divide ”X” message into two 32bits parts xl,xr
- for i=1 to 16
- xl = xl xor pi

- xr = F(xl) xor xr
- In F(xl),D function divides xl into a,b,c,d 8-bit quarters parts
- F(xl) = ((S1,a + S2,b mod 2$\hat{3}$2) XOR S3,c) + S4,d mod 2$\hat{3}$2
- swap(xl,xr)
- end for
- swap(xl,xr)
- xr = xr xor p17
- xl = xl xor p18
- recombine xl,xr to form cipher

2.6 Defects of Symmetric Cryptography

- Trust Issues
- Key establishment
- Many more

2.7 Asymmetric Cryptography

Definition: Different cryptographic keys used to Encrypt and Decrypt message. Generally use 2 Keys:

- Public Key(Released to public)
- Private Key(lies with individual)

Generally, Message is encrypted with public key and decrypted with private key Remember cipher means Encrypted message. And Private is checked by public key as concept is used by Digital Signatures. To improve the protection mechanism Public Key Cryptosystem was introduced in 1976 by Whitfield Diffe and Martin Hellman of Stanford University. It uses a pair of related keys one for encryption and other for decryption. One key, which is called the private key, is kept secret and other one known as public key is disclosed. The message is encrypted with public key and can only be decrypted by using the private key. So, the encrypted message cannot be decrypted by anyone who knows the public key and thus secure communication is possible Public Key Cryptography is Asymmetric algorithm..RSA belongs to PKC.

2.8 RSA

In 1977,Rivest, Adi Shamir, and Leonard Adleman public proposed this algorithm.RSA uses "TRAP DOOR" concept to produce Keys.

Algorithm

In simple, It is Easy to get product of two numbers but hard to get those numbers back from resultant value. Example:

- Choose p = 3 and q = 11
- compute n = p*q = 3*11 = 33
- compute k = (p-1)*(q-1) = 2 * 10 = 20
- Choose e such that 1 < e <k and e and k are Co-prime .Let e = 7
- Compute for d such that (d*e)/k = 1 .Here d = 3
- Public Key is (e,n) = (7,33)
- Private Key is (d,n) = (3,33)
- The encryption of m = 2 is c = $2\hat{7}$ %33 = 29(m - message)
- The decryption of c = 29 is m = $29\hat{3}$ % 33 = 2

2.9 Brief analyse of algorithm

- Finding the power of large number.
- Finding Two large prime number.
- checking whether chosen number are prime numbers.
- Finding the Mod value of large numbers.
- Factorization of Two numbers.

Finding the power of a large number in log(n) multiplications

Code:

- #include"bits/stdc++.h"
- using namespace std;
- vector¡int¿ dectobits(int input)
- vector¡int¿ v;
- while(input != 1)
- v.insert(v.begin(),input
- input = input/2

- v.insert(v.begin(),1);
- return v;

- void powerof(int x,int power)
- vector¡int¿ v(dectobits(power));
- int size = v.size();
- int a = 1;
- for(int i =0;i¡size;i++)
- a = a*a;
- if(v[i] == 1)
- a = x*a;

- cout¡¡"Answer is :"¡¡a¡¡endl;
- return ;

- int main()
- int x,pow1;
- cin¿¿x;
- cin¿¿pow1;
- powerof(x,pow1);
- return 0;

- Complexity of the algorithm depends on Length of the power in bits.

Find the number is Prime or not

As we have find the whether given number is prime or not.
We AKS algorithm whose complexity is polynomial time.
Algorithm: Let x be variable and p is the prime number.
(x-1)p̂ - (xp̂-1)
This expression gives all coefficients are multiples of p.
Another Method to find the given number is prime number.One of the method is probabilistic algorithm .Those are
Randomized Algorithm Monte-Carlo-Algorithm.Complexity is Log(n) here n is the number of bits to store the number.

- Yes - Monte-Carlo-Algorithm: In this Algorithm tells Yes then the given number is true Prime number But when it says no it has some error probability.
- No - Monte-Carlo-Algorithm.:In this Algorithm tells No then the given number is true non prime number but when it says yes it has some error probability.
- When is n is not a prime but algorithm claims it is prime then those are called Pseudo prime number.

Generally,Number of primes up to N is equal and less than equal to N/Log(N) and probability of number to be prime is 1/Log(N).So try Log(N) give at least one prime number.

Quadratic Residue

Suppose P is an odd prime and a is an integer.a is defined to be a quadratic residue modulo P is a is not multiple of P and the congruence $y\hat{2} = a(\text{mod } P)$ has a solution y belongs to Z. a is defined to be a quadratic non residue modulo P is if a is not a multiple of P and a is not a quadratic residue modulo P.
There are exactly (p-1)/2 QR(Quadratic Residues).
Example:Z11

- $1\hat{2} = 1$
- $2\hat{2} = 4$
- $3\hat{2} = 9$
- $4\hat{2} = 5$
- $5\hat{2} = 3$
- $6\hat{2} = 3$
- $7\hat{2} = 5$
- $8\hat{2} = 8$
- $9\hat{2} = 4$
- $10\hat{2} = 1$
- There are exactly (11 -1)/2 = 5 QR

- There exist only two solutions for x$\hat{2}$ = a(mod P)

To check whether a number is QR or not in polynomial time.

Euler's Criterion

Let a P be prime number.Then a is a quadratic residue modulo P if and only if
(a$\hat{}$(p-1)/2)%p = 1
This checking algorithm has complexity of O(Log P)$\hat{3}$

Another primality Checking Algorithm

Fermat's Theorem: If n is prime,then a$\hat{}$(n-1)%p== 1 for any integer a less than p.Whose complexity is less than N or root N.

Factorization of Number N Methods:

Some of the methods are

- Quadratic Sieve.
- Elliptic Curve Factoring Steve .
- Number Field Sieve.
- Pollard's P-1 Algorithm.
- Pollard's rho Algorithm.
- Dixon's Random Squares Algorithm.
- trial Division Method.

Pollard's P-1 Algorithm

Algorithm

- Suppose P.Q are prime and N = PQ .The Euler-Fermat theorem guarantees.
- a$\hat{}$(p-1)%p = 1
- For all a relatively prime to P.
- Suppose P-1 is a factor of L.Then L = (P-1)*K,so
- a$\hat{L}$ % P= (a$\hat{}$(P-Q))$\hat{k}$ or 1
- Consequently P divides a$\hat{L}$ -1,and since P is a factor p of N.the GCD of a$\hat{L}$-1 and N will include P.Generally L,we take some factorial of number.And answer of factorial will not include Trivial cases.

Example:

- Factor 1403(N) using Pollard's P-1 method.
- $2\hat{2}$ -1, 1403 will be 1.So,it is not the answer.
- $2\hat{3}$ - 1,1403 will be 1.so,it is not the answer.
- $2\hat{4}$ -1,1403 will be 1.so,it is not the answer.
- $2\hat{5}$ -1,1403 will be 61.so,it is the answer.1403 = 61 X 23.
- Complexity of Algorithm is Log(B)$\hat{k}$.K can be any +ve number

We assumed that by the above knowledge the over complexity is (Log(N))$\hat{K}$,K is any number.

2.10 Defects of RSA

- As technology is Developing ,more advance machines are increasing to factorize the number quicker.
- Astronomically development in factorization research and methods
- Slow encryption and Decryption of messages
- For more secure.we need Large Keys.

But now Latest algorithms uses both symmetric and asymmetric algorithms and hashing for better performance and better security.

Uses of Cryptography

- Security
- Digital Signature
- Access Control
- Authentication
- Many more

Resources

- Youtube.
- Nptel
- Wikipedia
- Some website.