J. Computing & Int. Systems (2017) 41–44

SACRED HEART RESEARCH PUBLICATIONS

Journal of Computing and Intelligent Systems

Journal homepage: www.shcpub.edu.in

ISSN: 2456-9496

A SURVEY ON ASYMMETRIC ENCRYPTION ALGORITHMS

B. Raihana Begum#1, E. George Dharma Prakash Raj#2

Received on 9th Mar 2018, Accepted on 21st Mar 2018

Abstract *— Asymmetric key encryption is also called public key encryption. The two different keys are used for encryption and decryption. It is called public key and other is private key.Asymmetric encryption can be used for confidentiality, authentication, or both. some public key algorithms and its advantages and disadvantages can be discussed in this paper such as Rivest Shamir Adleman, Diffie-Hellman, Elliptic Curve Cryptography, Elliptic Curve Diffie-Hellman, ElGamal Encryption Algorithm, Knapsack Algorithm, Digital Signature Algorithm and Short Range Natural Numbers.*

Keywords - RSA, DH, ECC, ECDH, ElGamal Encryption, Knapsack, Digital Signature and SRNN.

I INTRODUCTION

The public-key cryptography developmentis the greatest and perhaps the only true revolution with in theentire history of cryptography. The most widely used public-key cryptosystem is RSA. Whitfield Daffier and Martin Hellman introduced the concept of public key cryptography in 1976. the problem of confidentiality can be clearly solved by Public key encryption. The identification problem can be solved bySigning a message with a signature encrypted with ones private key. One key in the pair can be shared with everyone; it is called the public key. The other one key in the pair is kept secret, it is called the private key. It was developed in 1977 by Ron Rivest, AdiShamir, and Adleman at MIT and first published in1978.RSA is the public key algorithm most used in the world. general number field sieve(GNFS) isthe best known Shamir Adleman, Diffie-Hellman, Elliptic Curve Cryptography, Elliptic Curve Diffie-Hellman, ElGamal Encryption Algorithm, Knapsack Algorithm, Digital Signature Algorithm and Short Range Natural Numbers.

II PUBLIC KEY CRYPTOGRAPHY ALGORITHMS

A. *Rivest Shamir Adleman*

RSA algorithm for factoring integers. It offers good security and secured digital signature. It uses the co-prime numbers to generate the public K_E and private $K_D$keys.

Theencryption scheme uses RSA and signature of the fact that

$$med \equiv m(mod\ n)\ (1)$$

for m integer. The encryption and decryption schemes are presented in algorithms 1 and2. The decryption works because cd ≡ (me)d≡ m(mod n).The safety lies in the difficultyof computing a clear text m from a cipher text c = me mod n and the public parameters n (e).

Algorithm 1: RSA Encryption

Input: RSA public key (n,e), Plain text m ∈ [0, n-1]
Output: Cipher text c
begin
1. Compute c = me mod n
2. Return c.
End

Algorithm 2: Decryption RSA

Input: Public key (n,e),Private key d, Cipher text c
Output: Plain text m
Begin
Compute m = cd mod n
Return m.
End

B. *Diffie-Hellman key exchange (D-H)*

The Diffie–Hellman key exchange scheme was first published by Whitfield Diffie and Martin Hellman in[1976]. Diffie-Hellman Protocols are to allow the construction of common secret key over an unconfident contact channel and to exchange keys.DH is a method for securely exchanging a secret shared between two parties, in real-time, over an unfrosted network.

There are two publically better-known numbers they are a prime number q and an integer α that is a primitive root of q. Suppose the users A and B would like to exchange a key. User A selects a random integer $XA<q$ and computes $YA=\alpha^X \bmod q$. Similarly, user B independently selects a random integer $XB<q$ and computes $YB=\alpha^X \bmod q$.

Each side keeps the X value as private that is non-public and makes the Y value available as publicly to the other side. User A computes the key as $K=(YB)^X \bmod q$ and user B computes the key as $K=(YA)^X \bmod q$. these two calculations produce the same result by the rules of modular arithmetic

$$K = (YB)^X \bmod q$$
$$= (\alpha^X \bmod q)A \bmod q$$

* Corresponding author: E-mail: raiha.8994@gmail.com, georgeprakashraj@yahoo.com.

[1] Research Scholar, Department Of Computer Science, Bharathidasan University, Trichy, India Tamilnadu, India.

[2] Assistant Professor, Department Of Computer Science,Bharathidasan University,Trichy,India.

Key Exchange algorithm

Let us assume that A and B want to agree upon a key that is to be used for encryption / decrypting messages that would be exchanged between them. The Diffie-Hellman key exchange algorithm works as follows [2].

1. *Firstly, A and B agree on two large prime numbers n and g. These two integers need not be kept secret. A and B can use an insecure channel to agree on them.*
2. *A chooses another large random number x and calculates c such that c=g x mod n*
3. *A sends the number c to B*
4. *B independently chooses another large random integer y and calculate d such that d=g y mod n*
5. *B sends number d to A*
6. *A now compute the secret key K1 as follows*
   K1= d x mod n
7. *B now computes the secret key K2 as follows.*
   K2=c y mod n

C. Elliptic curve cryptography (ECC)

The Elliptic curves in cryptography idea was introduced by Victor Millerand N. Koblitz in 1985 as an alternative to established public-key systems such as DSA and RSA.Elliptical curve cryptography (ECC) may be a (PKC) public key encryption technique based on elliptic curve theory that can be used to create faster in speed, smaller in size, and more efficient Cryptographic keys to provide authentication scheme to RFID system.

Elliptic Curve Encryption/Decryption algorithm can be explained by following procedure.

Assume user A wish to send message M to B.

1. *'A' chooses a random positive integer 'k', a private key 'nA'.*
2. *Generates the public key PKA = nA × G.*
3. *Calculates the cipher text 'CM'consisting of pair of points CM={ kG , M + kPKB } where G is the base point selected on the Elliptic Curve, PKB= nB × G is the public key of B with private key 'nB'.*
4. *To decrypt the cipher text, B multiplies the 1st point in the pair by B's secret & subtracts the result from the 2nd point M + kPKB - nB(kG) = M + k(nB G) – nB(kG)=M*

D. Elliptic curve Diffie–Hellman (ECDH)

Elliptic curve Diffie-Hellman is an associate degree anonymous key agreement protocol that permits two parties, each having an associate degree elliptic curve public key–private key combine pair.ECDH, a variant of DH, may be a key agreement Formula.It is for generating a shared secret between A and B with ECDH, each got to agree au courant Elliptic Curve domain parameters.

Assume that Alice and Bob use the identical set of domain parameters *D = (p, a, b, P, n, h)* for his or her computations.

– *Alice generates an ephemeral key pair (kA,QA), i.e.generates a randomnumber kA in the interval [1, n−1] and then performs a scalar multiplicationto get the corresponding public key QA = kA · P. She sends QA to Bob.*
– *Bob generates an ephemeral key pair (kB,QB) with QB = kB ·P in the sameway as described above and sends the general public key QB to Alice.*
– *Once Alice receives Bob's ephemeral public key QB, she performs a scalarmultiplication to get the shared secret S = kA · QB.*
– *Once Bob receives the ephemeral public key QA from Alice, obtains theshared secret through computation of S = kB · QA.*

E. ElGamal Encryption Algorithm

In 1984,T.Elgamal announced a public key scheme based on discrete logarithms.It consists of boththe encryption and signature algorithms.The El-Gamal signature algorithm is similar to the encryption algorithm inthat the two keys public key and private key have the same form; However, encryption is not the same as signatureverification.

ElGamal Key Encryption

The encryption algorithm works as follows: To encrypt a message m to A under the public key ,(G,q,g.h).

1. *B chooses a random y from {1.....,(q-1)} then calculates c1 =gy*
2. *B calculates the shared secret s=hy*
3. *B converts the secret message m into m' an element of G*
4. *B calculates . c2=m'.s*
5. *B sends the ciphertext (c1, c2)= (gy ,m'.hy) =(gy ,m'.(gx)y) to A.*

Note that one can find easilyhy if one knows m'. Therefore,to improve security a new y can be generated for every message. For this reason, y is also called an ephemeral key.

ElGamalDecryption

The decryption algorithm works as follows:
to decrypt a ciphertext (c1,c2) with the
private key x,

1. A calculates the shared secret s=c1x

2.Then A computes m'=c2.s-1 is converted back into the plaintext message m , where inverse of s in the group is s-1. (E.g. modular multiplicative inverse if G is a subgroups of a multiplicative group of integers modulo n).

The decryption algorithm produces the intended message, since *c2.s-1=m'.hy.(gxy)-1=m'.gxy .g-xy =m'*

F. Knapsack Algorithm

The Merkle–Hellman knapsack cryptosystem was invented by Ralph Merkle and Martin Hellman in 1978.It was one of the earliest public key cryptosystems.Knapsack problem consider an optimal solution 0-1.

knapsack problem can't be resolved by greedy methodologyas a result of it's not fill the capacity of knapsack and empty quantity lower the effective value per pound of the load, and we should estimate the answer to the sub problem with in which the item is exclude before we are able to build the dainty.Let *G* be a finitely generated group, and let *A* be a finitegenerating set for *G*.

Then, elements of G can be represented by finite words over the alphabet $A^{\pm}1 = A\ [\ A-1]$. An *exponent equation* over G is an equation of the form

$$h0gx11\ h1gx22\ h2, \ldots, gxkk\ hk = 1$$

where $g1, g2, \ldots, gk, h0, h1, \ldots, hk2\ G$ are group elements that are given by finite wordsover the alphabet $A^{\pm}1$ and x1, x2,..., x*k*are not necessarily distinct variables. Such anexponent equation is *solvable* if there exists a mapping - {x1, . . . , x*k*} ! N such that *h0g_(x1)1 h1g_(x2)1 h2 · ·g_(xk) k hk*= 1 in the group *G*. The *size* of an equation is P*k*

P *i*=0 |*hi*| + *ki*=1 |*gi*|, where |*g*| denotes the length of the shortest word *w* 2 (*A*±1)_ representing *g*.

Solvability of exponent equations over G is the following computational problem

Input - An exponent equation *E* over *G* (with elements of *G* specified by words over $A^{\pm}1$). Now calculate the sequence β = (β1, β2... β*n*) where β*i* = *rwi*mod *q*.

The public key is β, while the private key is (*w*, *q*, *and r*).

(ii) Encryption
To encrypt an *n*-bit message
α = (α1, α2... α*n*),
Where
Is the *i*-th bit of the message and {0, 1}, calculate
The cryptogram then is *c*.

(iii) Decryption
In order to decrypt a cipher text *c* thena receiver has to find the message bits α*i* such that they satisfy.

G.Digital Signature Algorithm

The Digital signatures and hand-writtensignatures both rely on the factthat it isvery hard to find twoWith the same signature. People used public-keycryptography to compute digital signatures by associating something unique with each person.

The DSA makes use of the following parameters:
1. p = a prime modulus, where ever 2L-1 < p < 2L for 512 £ L£ 1024 and L a multiple of 64.
2. q = a prime divisor of p - 1, where ever 2159 < q < 2160.
3. g = h(p-1)/q mod p, where ever h is any integer with 1 < h <p - 1 such that h(p-1)/q mod p > 1(g has order q mod p).
4. x = a randomly or pseudo randomly generated integerwith 0 < x < q.
5. y = gx mod p.
6. k = a randomly generated integerwith 0 < k < q.

Key generation

In dynamic group signature schemes the key generation algorithm **GK** gis used to generate the group public key and the group manager secret keys.group managergenerate these keys.

Join procedure

It is for admitting a new valid member to the group every dynamic group executes the Join procedure. This procedure is executed between the group manager and the member that is who wish to join the group.Uponsuccessful admission for signing the new member receives the secret key and the group manager gathers the secret information required in order to open the signature generated by the new member.

H. Short Range Natural Numbers Algorithm (SRNN)

SRNN algorithm is similar to RSA algorithm with some modifications.In addition to this we have used two naturalnumbers in pair of keys (public, private).These natural numbers increases the security of cryptosystem.
so its name is "modified as RSA public key cryptosystem using short range natural number algorithm"Difference between SRNN and RSA with modulus length 1024 bits are approximately 5080 milliseconds (SRNN 1024 bits > RSA 1024 bits) whereas difference of RSA 2048 bits and SRNN 1024 bits are 5338 milliseconds (RSA 2048 bits > SRNN 1024 bits). Hence SRNN with modulus length 1024 bits are in good balance between speed and security.

(i) Key generation
1. Generate two large random prime p, q.
*2. Compute n=p*q*
3. Compute phi= (p-1) (q-1)
*4. Choose an integer e, 1<e<phi, such that gcd (e, phi) =1 compute the such that (e*d) mod phi=1*
*5. Pick short range natural number **u** randomly such that u<phi-1*
*6.Pick another Short range natural number **a** randomly such that phi>a>u and compute ua*
7.Find d such that,
*e*d mod ((p-1) (q-1)) =1*
8. Public key is (n, e, ua)
9. Private Key is (d, a, u) P, q, phi should also be kept secret.

(ii) *Encryption process*
Sender does the following obtains the recipient's public key (n,e,ua)

- Represents the plaintext message as a positive integer m.
- Computes the cipher text c = (m ua) e mod n.
- Sends the cipher text c to recipient.

(iii)*Decryption process*
Recipient does the following

Uses his private key (d, a, u) to compute m = (v e c) d mod n Where v= u phi-a mod n. Extracts the plaintext from the integer representative m.

The following table analyses the various Public Key Cryptography Algorithms and its advantages and disadvantages.

S.NO	Algorithms	Advantages	Disadvantages
1	RSA	Only intended ser can read the message using their private key.	Many secret key encryption methods that is significantly faster than any current available public-key encryption.
2	Diffie-Hellman	No secret sharing necessary.	Slower or computationally intensive.
3	ECC	Short key is faster and requires less computing power.	It is more expensive and it shortens the life of batteries.
4	ECDH	Very secure means of exchanging keys between two parties	Little difficulty in exchanging keys.
5	Elgamal	The advantages of the same plaintext gives a different cipher text each time, it is called encryption.	The main disadvantage of El-Gamal is the Need for randomness, and its slower speed(especially for signing).
6	knapsack	A perfect protocol for distribution of secret keys	deciphering keys are easy sequences, they are breakable
7	DSA	It is used in many crypto products for authenticatio n.	DSA is not used for Encryption but for digital signature.
8	SRNN	SRNN algorithm is Better in security	SRNN algorithm is slower in speed

III.CONCLUSION

This paper present various key algorithms of asymmetric like RSA, ECC, ECDH, Elgamal, knapsack, DSA and SRNN, RSA is one of the most effective encryption algorithm in terms of security and tenability.ElGamal algorithm is more secured as compared to RSA algorithm because it generates a more complex cipher textand it was also slow because when we encrypt and decrypt it, it generates more than one public keys.Elliptic Curve Cryptosystem is more secure.Elliptic curve replaces ElGamal also and use discrete logarithmic problem.

REFERENCES

[1] Caregia Mellon Software Engineering institute "Public Key Cryptography",2003.

[2] William Stallings, "Cryptography and Network Security Principal and Practice", Fourth Edition, Pearson 2005.

[3] Gustavo da Silva Quirino and Edward David Moreno,"architectural evaluation of algorithms RSA, ECCand MQQ in arm processors", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.

[4] Gustavo S.Quirino,Edward David Moreno,and Leila B.C.Matos,"PerformanceEvalution of Asymmetric Encryption Algorithms in embedded platforms used in WSN,Further information:www.nist.gov.

[5] S Nithya, Dr E. George Dharma Prakash Raj, "Survey on Asymmetric key Cryptography Algorithms", Journal of Advanced Computing Technologies (ISSN: 2347-2804) Volume NO. 2 Issue No. 1,Febuary 2014.

[6] PrashantkumarArya,DrMahendra Singh Aswal,DrVinodKumar,"Comparative Study of Asymmetric Key Cryptographic Algorithms",ISSN:2249-5789 Prashant Kumar Arya et al , International Journal of Computer Science & Communication Networks,Vol 5(1),17-21.

[7] GauravYadav,Mrs.AparnaMajare,"A Comparative Study of Performance Analysis of Various Encryption Algorithms",(ICEMTE-2017)Volume:5 Issue:3,ISSN:2321-8169,70-73.March 2017.

[8] E. George Dharma Prakash Raj, k. Sheela, "Survey on public key cryptography algorithms", IJSRCSMS July 2013.

[9] David A. Carts," A Review of the Diffie-Hellman Algorithmand its Use in Secure Internet Protocols",SANS Institute of InfoSec Reading Room,November 5, 2001.

[10] Monika Nayak, Deepak Rajput, "Cryptography Algorithms – The Science of Information Security - Review Paper", IJIRCCE, Vol.5, Issue 3, March 2017.

[11] Himja Agarwal and B.R.Badada Pure, "A Survey Paper On Elliptic Curve Cryptography ", IRJET, Volume - 03 Issue: 04 | Apr-2016.

[12] H T Loriya, A.Kulshreshta, D.R. Keraliya, "Security Analysis of Various Public Key Cryptosystems for Authentication and Key Agreement in Wireless Communication Network", IJARCCE, Vol. 6, Issue 2, February 2017.

[13] Annapoorna Shetty, Shravya Shetty K, Krithika K,"A Review on Asymmetric Cryptography –RSA and ElGamal Algorithm", IJIRCCE,Vol.2, Special Issue 5, October 2014.

[14] Veenu Yadav, ShikhaSingh, " A Review Paper on Solving 0-1 knapsack Problem with Genetic Algorithms", Veenu Yadav et al, International Journal of Computer Science and Information Technologies, Vol. 7 (2) , 2016, 830-832.

[15] Markus Lohrey and Georg Zetzsche, " The Complexity of Knapsack in Graph Groups", STACS, 2017.