International Journal of Scientific Research in Science, Engineering and Technology (www.ijsrset.com)
© 2020 IJSRSET | Volume 7 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
DOI : https://doi.org/10.32628/IJSRSET207292

Survey on Asymmetric Key Cryptographic Algorithms

Sabitha S[1], Binitha V Nair[2]

[1]Assistant Professor, Department of Information Technology, K R Gouri Amma College of Engineering, Alappuzha, Kerala, India.

[2] Assistant Professor, Department of Computer Science and Engineering, K R Gouri Amma College of Engineering, Alappuzha, Kerala, India.

ABSTRACT

Cryptography is an essential and effective method for securing information's and data. Several symmetric and asymmetric key cryptographic algorithms are used for securing the data. Symmetric key cryptography uses the same key for both encryption and decryption. Asymmetric Key Cryptography also known as public key cryptography uses two different keys – a public key and a private key. The public key is used for encryption and the private key is used for decryption. In this paper, certain asymmetric key algorithms such as RSA, Rabin, Diffie-Hellman, ElGamal and Elliptical curve cryptosystem, their security aspects and the processes involved in design and implementation of these algorithms are examined.

Keywords: RSA cryptosystem, Rabin cryptosystem, Diffie-Hellman cryptosystem, ElGamal cryptosystem, Elliptical curve cryptosystem and digital signature cryptosystem

I. INTRODUCTION

Asymmetric Key Encryption or Public Key Encryption [1] employs different keys for encryption and decryption. A public key is used for encryption and a private key or a secret key is used for decryption. Plaintext and ciphertext are treated as integers. They must be encoded as integers before encryption and the integer must be decoded into message after decryption. Mathematical functions are applied in these integers for encryption and decryption.

$$\text{Ciphertext, } C = f(k_{public}, P)$$

$$\text{Plaintext, } P = g(k_{private}, C)$$

f is used only for encryption and g is used only for decryption. f needs to be a trapdoor one-way function to allow receiver to decrypt the message but prevent other person from doing so.

Fig.1 gives the basic idea of asymmetric key cryptosystem.

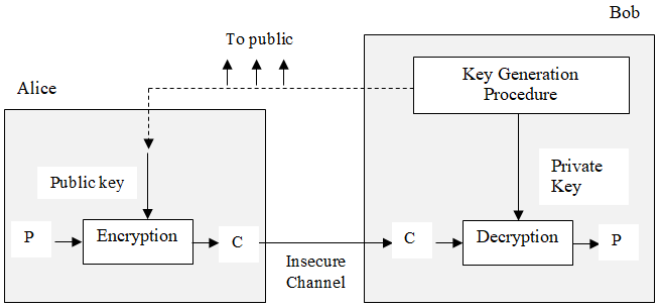

Fig.1. Basic idea of asymmetric key cryptosystem

A. Trapdoor one-way function (TOWF)

All public key encryption techniques are based on the notion of one-way functions. A TOWF is a function that is easy to compute in one direction but it is difficult to compute the inverse without special information. i.e. if f is a trapdoor function, then there exists certain secret information t, such that given f(x)

and t, it is easy to compute x. RSA and Rabin uses trapdoor functions which are related to prime factorization. ElGamal and ECC uses discrete logarithm functions but these functions are not known to be trapdoor.

Factorization problem

1. When n is large, $n = p \times q$ is a one-way function.
2. Given p & q, it is easy to calculate n.
3. Given n it is difficult to compute p & q.

Discrete logarithm Problem

If p is a very large prime, e_1 is a primitive root in the group $G =< Z_p^*, X >$ and r is an integer, and then $e_2 = e_1^r \bmod p$ is easy to compute using fast exponential algorithm. But, given e_2, e_1 and p it is infeasible to calculate $r = \log(e_1 e_2) \bmod p$.

B. Symmetric Vs. Asymmetric Key Cryptography

Sl No.	Symmetric	Asymmetric
1	Based on sharing secrecy	Based on personal secrecy
2	Same key is used for both encryption and decryption	Different key is used for encryption and decryption(public key, private key)
3	Symbols are permuted or substituted	Numbers are manipulated
4	Speed of encryption and decryption is very fast	Speed of encryption and decryption is slow
5	Key Exchange is a big problem	No problem for key exchange
6	Used mainly for encryption / decryption and cannot be used for digital signatures	Used for encryption / decryption as well as for digital signatures
7	Provides confidentiality	Provides confidentiality, authentication and non-repudiation
8	Examples: AES, DES 3DES, Blowfish etc.	Examples : RSA, DSA, Diffie Hellman, ECC, ElGamal etc.

Public key cryptography is used in applications such as digitally signed document, email encryption software such as MIME and PGP, digital signatures etc. This paper gives a brief description of various public key cryptographic algorithms such as RSA [7], Rabin [2], Diffie-Hellman [3], ElGamal [8] and Elliptical curve cryptosystems [9].

II. OVERVIEW OF ASYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS

This section explains a review of the existing symmetric key cryptographic algorithms.

A. RSA CRYPTOSYSTEM

RSA Cryptosystem is named after its inventors Rivest, Shamir and Adleman and was developed in 1978 and is based on exponentiation congruence. The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 & n-1 for some value of n. RSA is useful for short messages. It uses two keys e and d, where e is public (known to all users in the network) and d is private (secret and not shared to all). The three steps involved in RSA are generation of public/private key pair, encrypting plaintext into ciphertext and decrypting the ciphertext to generate the original data.

Algorithm for Key Generation

1. Select two large prime numbers p & q, $p \neq q$.
2. Calculate $n = p \times q$.
3. Calculate $\emptyset(n) = (p-1) \times (q-1)$.
4. Choose value of e such that $1 < e < \emptyset(n)$ and $\gcd(\emptyset(n), e) = 1$, i.e e and $\emptyset(n)$ are coprime.
5. Calculate $d = e^{-1} \bmod \emptyset(n)$
6. Public key = { e, n}
7. Private key = { d, n}

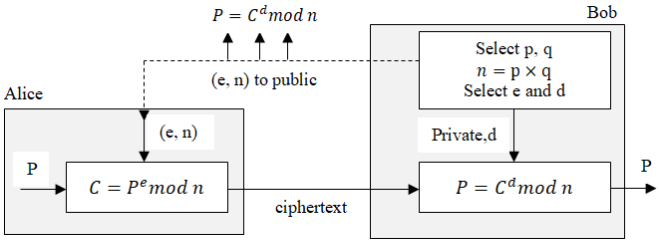

Fig.2. RSA Cryptosystem

Encryption: Ciphertext, $C = P^e \bmod n$, where $P < n$, P is the plaintext and e is public

Decryption: Plaintext, $P = C^d \bmod n$, C is the ciphertext and d is private.

RSA is used for smaller messages.

B. RABIN CRYPTOSYSTEM

Rabin Cryptosystem is named after its inventor M.Rabin and is based on Quadratic congruence. It is a variation of RSA. The value of e and d are fixed i.e. $e = 2$ and $d = 1/2$.

Algorithm for Key Generation

1. Choose two large prime numbers p and q in the form $4k + 3$ and $p \neq q$.
2. Calculate $n = p \times q$.
3. Public key = n
4. Private key = {q, n}

Encryption: Ciphertext, $C = P^2 \bmod n$

Decryption:

Decryption creates four equally probable plaintexts.

1. Find a_1, a_2, b_1 and b_2

$$a_1 = +\left(C^{(p+1)/4}\right) \bmod p,\ a_2 = -\left(C^{(p+1)/4}\right) \bmod p,$$
$$b_1 = +\left(C^{(q+1)/4}\right) \bmod q,$$
$$b_2 = -\left(C^{(q+1)/4}\right) \bmod q$$

2. Compute the plaintexts P_1, P_2, P_3 and P_4

$$P_1 = \text{Chinese\_Remainder}(a_1, b_1, p, q)$$
$$P_2 = Chinese\_Remainder(a_1, b_2, p, q)$$
$$P_3 = Chinese\_Remainder(a_2, b_1, p, q)$$
$$P_4 = Chinese\_Remainder(a_2, b_2, p, q)$$

The receiver chooses the right plaintext from the four plaintexts.

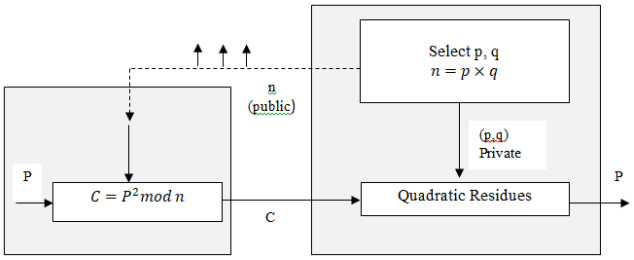

Fig.3. Rabin Cryptosystem

Rabin cryptosystem is secure as long as p and q are large numbers.

C. ELGAMAL CRYPTOSYSTEM

ElGamal Cryptosystem is named after its inventor Taher ElGamal and is based on Discrete Logarithmic Problem. It is used for key exchange, authentication, encryption and decryption of small messages.

Algorithm for Key Generation

1. Select a large prime number p.
2. Select decryption/private key, d to be a member of the group $G =< Z_p^*, X >$ such that $1 \leq d < p - 2$
3. Select encryption/public key, e_1 to be a primitive root in the group $G =< Z_p^*, X >$
4. Calculate $e_2 = e_1^d mod\ p$
5. Public key = {e_1, e_2, p}
6. Private key = d

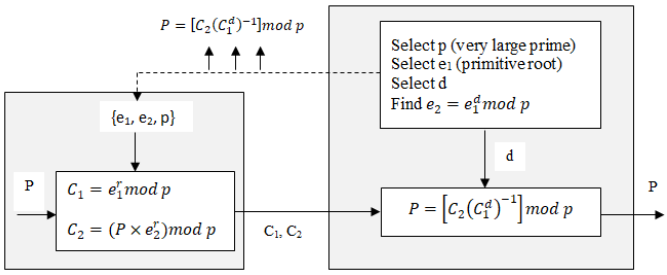

Fig.4. ElGamal Cryptosystem

Encryption:

1. Select a random integer r in the group,
$$G =< Z_p^*, X >$$
2. Find $C_1 = e_1^r mod\ p$
3. Find $C_2 = (P \times e_2^r) mod\ p$,
C_1 & C_2 are ciphertexts.

Decryption: Plaintext, $P = \left[C_2\left(C_1^d\right)^{-1}\right] mod\ p$

ElGamal is vulnerable to known-plaintext attack and low-modulus attacks.

D. DIFFIE – HELLMAN CRYPTOSYSTEM

It is a key exchange algorithm rather than encryption/ decryption algorithm.

Algorithm

1. Consider a prime number q.
2. Select α such that it must be the primitive root of q and $\alpha < q$.
3. Assume X_A be the private key of A and $X_A < q$, then public key of A, $Y_A = \alpha^{X_A} mod\ q$.
   Y_A is send to B.
4. Assume X_B be the private key of B and $X_B < q$, then public key of B, $Y_B = \alpha^{X_B} mod\ q$.
   Y_B is send to A.
5. Calculate the secret keys of both sender and receiver using public keys.
   $k_1 = (Y_B)^{X_A} mod\ q$ and $k_2 = (Y_A)^{X_B} mod\ q$

If $k_1 = k_2$, then key exchange is successful.

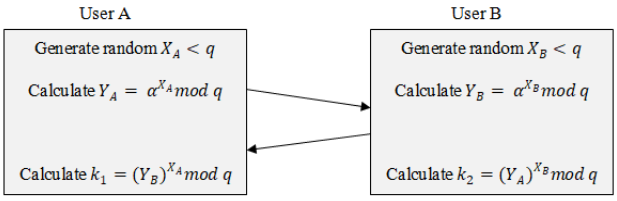

Fig.5. Diffie – Hellman Cryptosystem

Diffie – Hellman is vulnerable to man-in-the-middle attack.

E. ELLIPTIC CURVE CRYPTOSYSTEMS (ECC)

ECC provides equal security with smaller key sizes as compared to RSA and ElGamal systems. It makes use of elliptic curves ($y^2 = x^3 + ax + b$).

Let $E_q(a, b)$ be the elliptic curve with parameters a, b and q. q is a prime no. or an integer of the form 2^m. G is a point on the elliptic curve whose order is large value of n.

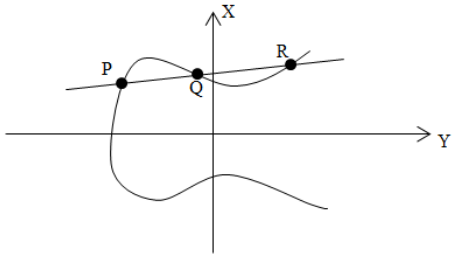

Fig.6. Basic Elliptic curve cryptography

User A key generation

1. Select private key, n_A, such that $n_A < n$
2. Calculate public key, p_A such that $p_A = n_A \times G$

User B key generation

1. Select private key,n_B such that $n_B < n$
2. Calculate public key, p_B such that $p_B = n_B \times G$

Calculation of secret key by user A: $k = n_A \times p_B$

Calculation of secret key by user B: $k = n_B \times p_A$

Encryption: Encode the plaintext P into a point on the elliptic curve, i.e. P_m

Then, Cipher point, $C_m = \{kG, P_m + kp_B\}$, where k is a random positive integer.

Decryption:

Multiply 1st point with receiver's secret key, i.e. $kG \times n_B$. Then subtract it from the second point. i.e. $P_m + kp_B - (kG \times n_B) = P_m + kp_B - kp_B = P_m$

The security of ECC depends in the difficulty in solving the elliptic curve logarithm problem.

III. COMPARATIVE ANALYSIS

Table I. Comparative analysis of asymmetric algorithms

Algorithm / Parameters	RSA	Rabin	ElGamal	Elliptical curve	Diffie-Hellman
Developed by	Ron Rivest, Adi Shamir, Leonard Adleman in 1977	Michael Rabin in 1977	Taher Elgamal in 1985	Neal Koblitz and Victor Miller in 1985	Whitfield Diffie and Martin Hellman in 2002
Based on	Exponentiation congruence	Quadratic Congruence	Discrete Logarithm Problem	Elliptic curves	Key exchange protocol based on public key cryptography
Advantages	Used for encryption and decryption of smaller messages, authentication, digital signatures	Secure against chosen plaintext attack	The same plaintext gives different ciphertext each time it is encrypted	Uses shorter keys, faster, requires less computing power	The shared secret key is never transmitted over the channel
Disadvantages	Lower security	Probabilistic, complex decryption	Slow, randomness. Long ciphertext	More expensive, shortens the lifespan of batteries	Lack of authentication
Level of Security	low	Low(same as RSA)	Medium	Medium	High
Attacks	Plaintext attack, Factorization Attack, common modulus attack, ,chosen ciphertext attack	Factorization Attack, common modulus attack, ,chosen ciphertext attack	Low modulus Attacks, Known-plaintext Attack	Side channel Attack	Meet-in-the-middle attack, Discrete Logarithm attack

IV. CONCLUSION

In public key cryptography there is no need of exchange of keys thereby eliminating key distribution problem. They provide better security as the private key is not transmitted and is not revealed to anyone.

They can provide digital signatures In this paper, a review based on different asymmetric key algorithms is presented. A detailed summary of algorithms such as RSA, Rabin, Diffie-Hellman, ElGamal, Elliptical curve cryptosystem is analysed. Each algorithm has different applications.

V. REFERENCES

[1]. Behroz A. Forouzan, “Cryptography & Network Security”, McGraw Hill Publication,2008, New Delhi.

[2]. W. Stallings, Cryptography and network security: principles and practices. Prentice Hall, 2005.

[3]. W. Diffie and Y. Hellman, “New Directions in Cryptography,” IEEE Trans. Information Theory, vol. 22, pp. 644-654, 1976.

[4]. Yaun Xue, “Public key Cryptography and RSA Algorithm”, Technical notes and papers.

[5]. W. Diffie, M.E. Hellman, “Privacy and Authentication: An Introduction to Cryptography”, in Proceedings IEEE, Vol 67 (3) Mar 1979 pp 397-427

[6]. J Menezes Alfred, C Paul, Oorschot van, A Vanstone Scot, Handbook of AppliedCryptography, CRC Press, 1997.

[7]. R.L Rivest, A Shamir, L Adleman,” A Method for obtaining Digital Signatures and Public Key Cryptosystems”, Communications of the ACM, 21 (1978), 120-126.

[8]. T ElGamal,”A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms”, IEEE Transactions on Information Theory, 31 (1985), 469-47.

[9]. N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, vol. 48, pp. 203-209, 1987

Cite this article as :

Sabitha S, Binitha V Nair, "Survey on Asymmetric Key Cryptographic Algorithms", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 2, pp. 404-408, March-April 2020. Available at doi : https://doi.org/10.32628/IJSRSET207292
Journal URL : http://ijsrset.com/IJSRSET207292