ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A Review on Public Key Cryptography: Algorithms

Yashaswini J

Assistant Professor, Dept. of Computer Science, PBMMPGC, K.R.S. Road, Mysuru, Karnataka, India

ABSTRACT: Network security is an important aspect of information sharing. Attempts have been made to remove various insecurities over internet. For this, many technological implementations and security policies have been developed. The amount of data, transferred, is not a factor. The basic factor is, how much security, the channel provides while transmitting data. Cryptography is one such technique, which allows secure data transmission without losing its confidentiality and integrity. Based on the key distribution, cryptography is further classified into two major types- Symmetric Key Cryptography and Asymmetric Key Cryptography. In this paper, the basic algorithms related Asymmetric Key Cryptography are surveyed.

KEYWORDS: Cryptography, Symmetric Cryptography, Asymmetric Cryptography

I. INTRODUCTION

During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of Cryptography. The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck.

Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. "Cryptography" derives from the Greek word kruptos, meaning "hidden". The key to hiding data is to devise a hiding (encryption) mechanism that is very difficult to reverse (i.e., to find the original data) without using the decryption key. Usually, the harder it is to discover the key, the more secure the mechanism. In symmetric (also called "secret-key") encryption, the same key is used for both encryption and decryption. In asymmetric (also called "public key") encryption, one key is used for encryption and another for decryption.

II. CRYPTOGRAPHY

Data that can be read and understood without any special measures is called plaintext or clear-text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. The process of reverting cipher-text to its original plaintext is called decryption.

In a typical situation where cryptography is used, two parties (X and Y) communicate over an insecure channel. X and Y want to ensure that their communication remains incomprehensible by anyone who might be

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

listening. Furthermore, because X and Y are in remote locations, X must be sure that the information she receives from Y has not been modified by anyone during transmission. In addition, she must be sure that the information really does originate from Y and not someone impersonating Y.
Cryptography is used to achieve the following goals:

A. CONFIDENTIALITY

To ensure data remains private. Confidentiality is usually achieved using encryption. Encryption algorithms (that use encryption keys) are used to convert plain text into cipher text and the equivalent decryption algorithm is used to convert the cipher text back to plain text. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use a public/private key pair.

B. DATA INTEGRITY

To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication code or hashes. A hash value is a fixed length numeric value derived from a sequence of data. Hash values are used to verify the integrity of data sent through insecure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered.

C. AUTHENTICATION

To assure that data originates from a particular party. Digital certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent.

III. TYPES OF CRYPTOGRAPHY

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into cipher text (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms. The most common types are i) Secret Key Cryptography which is also known as Symmetric Key Cryptography and ii) Public Key Cryptography which is also known as Asymmetric Key Cryptography. In other words, if the same key is used for encryption and decryption, we call the mechanism as Symmetric Key Cryptography. However, if two different keys are used in a cryptographic mechanism, wherein one key is used for encryption, and another, different key is used for decryption; we call the mechanism as Asymmetric Key Cryptography. This is shown in Figure 1 [2]

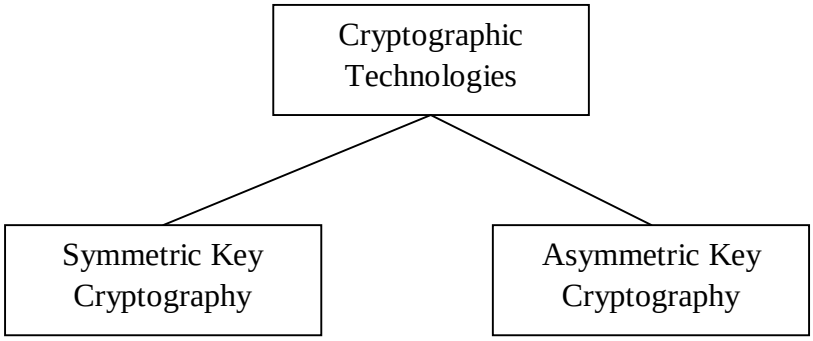

Figure 1: Cryptography techniques

A. SECRET KEY CRYPTOGRAPHY

In secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 2, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key [5].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

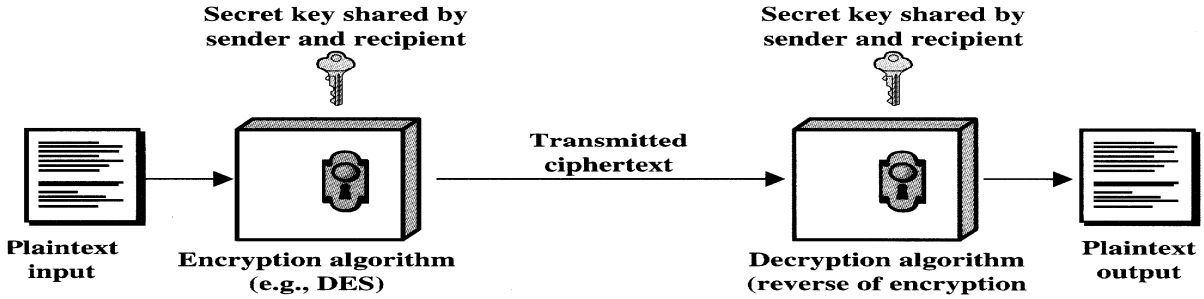

Figure 2: Symmetric key Crypto System

B. PUBLIC KEY CRYPTOGRAPHY

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is

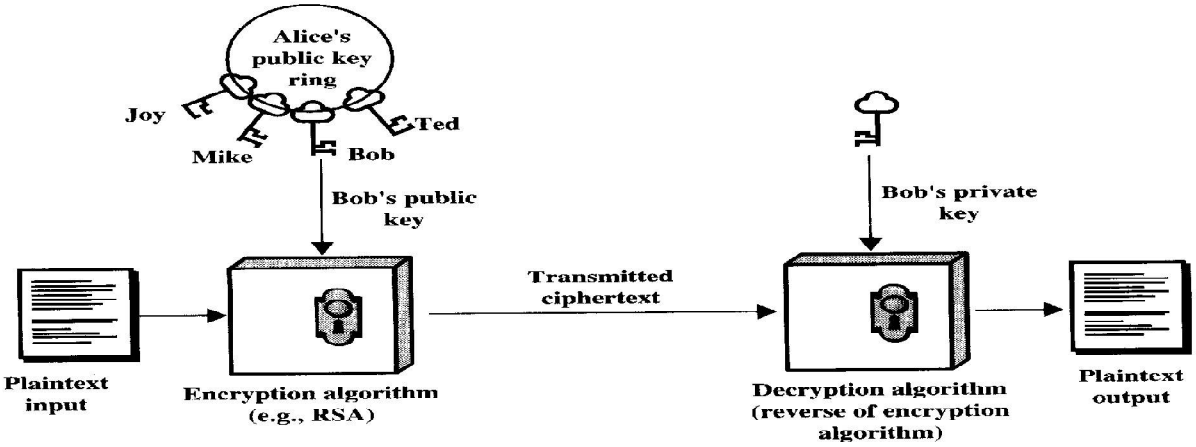

Figure 3: Public key Cryptosystem

responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement. Figure 3 describes the Public Key Cryptography [3].

IV. ALGORITHMS USED IN ASYMMETRIC KEY CRYPTOGRAPHY

Modern/Public-key cryptography started in 1976 with the publication of the following paper.

– W. Diffie and M.E.Hellman. "New directions in cryptography". IEEE Transactions on Information Theory, 22 (1976) 644-654.

Right up to modern times all cryptosystems are based on the elementary tools of substitution and permutation. Public-key algorithms are based on mathematical functions and are asymmetric in nature, involving the use of two keys, as opposed to conventional single key encryption.

These algorithms have the following important characteristic: It is computationally infeasible to determine the decryption key given only knowledge of the algorithm and the encryption key. In addition, some algorithms such as

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

RSA, also exhibits the following characteristics: Either of the two related keys can be used for encryption, with the other used for decryption.

IV.I. DIFFIE–HELLMAN KEY EXCHANGE (D–H)

The question of key exchange was one of the first problems addressed by a cryptographic protocol. This was prior to the invention of public key cryptography. The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel. The point is to agree on a key that two parties can use for a symmetric encryption, in such a way that an eavesdropper cannot obtain the key.

Diffie–Hellman Key Exchange establishes a shared secret between two parties that can be used for secret communication for exchanging data over a public network. The following figure 4 illustrates the general idea of the key exchange by using colors instead of very large numbers.

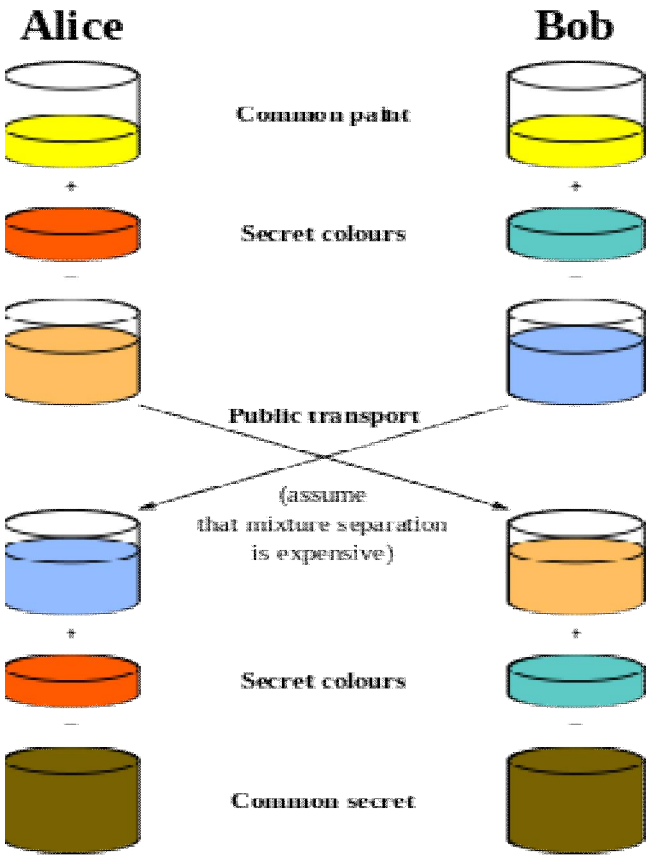

Figure 4: General idea of D-H key exchange

The process begins by having the two parties, Alice and Bob, agree on an arbitrary starting color that does not need to be kept secret (but should be different every time) in this example the color is yellow. Each of them selects a secret color–red and aqua respectively–that they keep to themselves. The crucial part of the process is that Alice and Bob now mix their secret color together with their mutually shared color, resulting in orange and blue mixtures respectively, then publicly exchange the two mixed colors. Finally, each of the two mix together the color they received from the partner with their own private color. The result is a final color mixture (brown) that is identical to the partner's color mixture.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A. D-H Key Exchange algorithm:

1 Alice and Bob agree on a prime number p and a base g.
2 Alice chooses a secret number a, and sends Bob (g^a mod p).
3 Bob chooses a secret number b, and sends Alice (g^b mod p).
4 Alice computes ((g b mod p) a mod p).
5 Bob computes ((g a mod p) b mod p). Both Alice and Bob can use this number as their key. Notice tha t p and g need not be protected.

Example: 1.Alice and Bob agree on p = 23 and g = 5.
2 Alice chooses a = 6 and sends 5^6 mod 23 = 8.
3 Bob chooses b = 15 and sends 5^{15} mod 23 = 19.
4 Alice computes 19^6 mod 23 = 2.
5 Bob computes 8^{15} mod 23 = 2. Then 2 is the shared secret. Clearly, much larger values of a, b, and p are required. An eavesdropper cannot discover this value even if she knows p and g and can obtain each of the messages.

IV.II. RSA ALGORITHM

RSA (RIVEST, SHAMIR, ADLEMAN) ALGORITHM: RSA was discovered in 1978. RSA is a Public (asymmetric) key cryptography algorithm; it is named after the initials of its discoveres, Ron Rivest, Adi Shamir and Len Adelman in 1977. It is the most popular asymmetric key cryptographic algorithm which is used to provide both secrecy and digital signature. It uses the prime numbers to generate public and private keys based on mathematical calculations and multiplying large numbers together [7]. Steps involved in RSA algorithm are generation of public and Private keys, Encryption Process, Decryption Process.

A. Generation of Public and Private Keys, Following steps are used for generating keys:

- Choose any two prime numbers say p & q. (p & q cannot be divided by any other number except 1 and itself).
- Calculate n, n = p x q.
- Calculate another number Ø also known as Euler's totient function, Value of Ø = (p-1) x (q-1).
- Now assume a number e such that d x e = 1 (mod Ø).
- The value of e should lie between 1 and Ø. Number e should be a prime number. Number e and Ø should be co-prime means e and Ø are not divisible by any other number except 1 or in other words g.c.d. of e and Ø should be 1. Now calculate the value of d by using extended Euclidean algorithm's table method. After calculating the value of d, public keys (e and n) are announced to the public and private keys (d and Ø) are kept secret.

B. Encryption process: Now anyone can send a message by using public keys (e and n). Plain text (Original message) is converted into Cipher text (scrambled message) by using the following formula:

$$\mathbf{C = P^e \pmod n}$$

C. Decryption process: Cipher text is converted into Plain text by using private key d. Cipher text (scrambled message) is converted into Plain text (original message) by using the following formula:

$$\mathbf{P = C^d \pmod n}$$

Modular exponentiation is used for Encryption and Decryption process. RSA algorithm requires complex computation and hence it is very slow. In Public key algorithms, the underlying modular exponentiation and factoring large numbers into prime numbers depend on multiplication and division, which are inherently slower and requires a lot of processing power.

IV.III. ELGAMAL CRYPTOSYSTEM:

ElGamal Cryptosystem is based on Discreate Logarithm problem . The ElGamal Cryptosystem is non-deterministic, since the ciphertext depends on both the plaintext x and on the random value k chosen by encryptor. So there will be many ciphertexts that are encryptions of the same plaintext.

A. ElGamal Public-key Cryptosystem in Z^*_p

• Let p be a prime such that the discrete log problem in Zp is intractable, and let $\alpha \in Z^*_p$ be a primitive element.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

• Let P = Z^*_p , C = $Z^*_p \times Z^*_p$, and define K = {(p, α, a, β) : β ≡ α a (mod p)}. • The values p, α and β are public, and a is secret. K = (p, α, a, β), for a (secret) random number k ∈ Zp−1, define eK(x, k) = (y1, y2), where y1 = α k mod p and y2 = xβk mod p.
• For y1, y2 ∈ Z^*_p, define dK(y1, y2) = y2(y a 1) −1 mod p.
Example: Suppose p = 2579, α = 2, a = 765, and hence β = 2765 mod 2579 = 949.
Now, suppose that Alice wishes to send the message x = 1299 to Bob. Say k = 853 is the random integer she chooses. Then she compute y1 = 2853 mod 2579 = 435 and y2 = 1299 × 949853 mod 2579 = 2396.
When Bob receives the ciphertext y = (435, 2396), he compute x = 2396 × (435765) −1 mod 2579 = 1299, which was the plaintext that Alice encrypted.

- **Genaral algorithm:** choose a large prime *p* - at least with 150 digits
  - choose two random integers *1* Ł *q*, *x* < *p* - where *q* is a primitive element of Z^*_p
  - calculate $y = q^x \bmod p$. Public key: *p*, *q*, *y*; trapdoor: x
  - Encryption of a plaintext *w*: chose a random *r* and compute
    $a = q^r \bmod p$, $b = y^r w \bmod p$
  - Cryptotext: *c* = (*a*, *b*) (Cryptotext contains indirectly *r* and the plaintext is masked by multiplying with y^r (and taking modulo *p*))
  - Decryption:

$$w = \frac{b}{a^x} \bmod p = ba^{-x} \bmod p.$$

IV.IV. ELLIPTIC CURVE (EC):

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of nonzero elements of) the underlying finite field. Elliptic curve cryptography [ECC] is a public-key cryptosystem just like RSA and El Gamal. Every user has a public and a private key. Public key is used for encryption/signature verification. Private key is used for decryption/signature generation. Elliptic curves are used as an extension to other current cryptosystems.

- Elliptic Curve Diffie-Hellman Key Exchange
- Elliptic Curve Digital Signature Algorithm

The central part of any cryptosystem involving elliptic curves is the elliptic group. All public-key cryptosystems have some underlying mathematical operation. RSA has exponentiation (raising the message or ciphertext to the public or private values) where as ECC has point multiplication (repeated addition of two points). Both parties agree to some publicly-known data items. Ex: Eliptic curves over Z_p, $p > 3$ be prime. The elliptic curve $y^2 = x^3 + ax + b$ over Zp is the set of solutions (x, y) ∈ Zp × Zp to the congruence $y^2 = x^3 + ax + b$, where a, b ∈ Zp are constants such that $4a^3 + 27b^2$ not ≡ 0 (mod p), together with a special point O called the point at infinity.

V. APPLICATIONS FOR P-K CRYPTOSYSTEMS

In broad terms, we can classify the use of public-key cryptosystems into three categories:
1. Encryption/decryption: where the sender encrypts the message with the receivers public key.
2. Digital signature: where the sender “signs” a message with his private key.
3. Key exchange: several approaches later. • However, not all algorithms are suitable for all three applications. Some can only be used for say digital signature. RSA however can be used for all three as will be seen.

VI. CONCLUSION

Cryptography can be used make secure communication over an internet. Cryptography provides integrity, authentication and confidentiality. Cryptography as two versions, one is symmetric cryptography, where in which only one key used to make encryption and decryption and another is asymmetric key cryptography, which involves two keys, one for encryption and other for decryption. There are many algorithms available to implement public key cryptographic system. Using which one can achieve an authenticity, integrity and confidentiality over an insecure communication channel.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

REFERENCES

1) S. William, Cryptography and Network Security: Principles and Practice, 5nd edition
2) Computer and Network security by ATUL KAHATE.
3) Fundamentals of Computer Security, Springer publications "Basic Cryptographic Algorithms", an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.html#Algorithms
4) S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html
5) "Introduction to Public-Key Cryptography", an article available at "developer.netscape.com"
6) https://en.wikipedia.org.
7) Mohit Marwaha, Rajeev Bedi, "Comparative analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, IV/III/JulySept.,2013/16-18, E-ISSN 0976-3945.