ISSN No:-2456-2165

Cryptosystems Using Algorithms, Mechanism Techniques and Network Privacy Management- A Survey

G. Avinash [1], B.Ashwin Meshak [2] , K.Gokul Prasath [3], R.Karthick Raja [4], U. Sarath [5]
Department of Electronics and Telecommunication Engineering
Karpagam College of Engineering, Coimbatore

Abstract:- With the advancement in technology, a need for secured data communication also arises which is fulfilled by security mechanism techniques like data integrity, digital signatures, Traffic Padding, Routing Control, and access control. In various organizations, enterprises and institutions, network privacy is involved and it is one of the major parameters. Confidentiality of the information is a foremost thing for a concern. For the protection of data and secured communication, this paper aims at implementing several algorithms and mechanism techniques.

I. INTRODUCTION

The term cryptography refers to "secret writing". Commonly termed as "Cipher-system", Cryptography is a technique used to transform and transmit highly confidential data or Information in an encoded way so that only authorized can obtain or work on it and illegal data accessing can be avoided. It is a Greek origin word in which "crypto" refers to hidden and "graphy" refers to writing, so cryptography refers to hiding or secret writing. Cryptography can also be referred to the "art and science of achieving security by encoding message to make them non-readable which means it is used for privacy purpose" .Cryptography introduces techniques such as confidentiality, integrity and authenticity within on-going data communication.

Two different types of cryptography exist. They are symmetric key and asymmetric key cryptography. Plain text, cipher text, encryption and decryption are the most important key terms that deals a cryptosystem. Another technique used in the data hiding is "Steganography". In this technique, hidden message is absent and original data can't be accessed. Steganography means cover writing. Steganography prevents secret information by creating the suspicion. Steganography refers to the practice of communicating using hidden messages, often disguised within something else where one would not expect a message to be contained in. Various forms of steganography include text, audio, video, images.

II. HACKING – A LITERATURE REVIEW

The term "Hacker" originally refers to someone who analysed computers deeply. Today, media recognised Hackers as "those who committed computer crimes" [1].Two serious types of hackers include paid hackers and underemployed hackers. Criminal hackers, students, security experts are the major categories in which a hacker is likely to fall under. Ethical hacking is hired in large internet service based corporations. Hacking trend is increasing on a large basis particularly among the students. Students enroll in computer-related courses. 80% of hacking activity on the Internet is caused because of student hackers. Using a computer network directly, Internet connection, Remote control server are the major ways through which a hacker tries to access network. A series of methods are used by hackers in order to target an attack. When the resources are infected with virus or malware significant data loss occurs along with the eradication of components of the network [6]. Through these virus activities, hard disks and processors gets destroyed and it utilises large scale memory and slows down the system's performance[9].

Fig 1

Criminal hackers are those who have compromised internet services to steal credit or debit card numbers, aadhar card details and other details[1]. Recently, camscanner, a mobile application that allows Android devices to be used as image scanners has been hacked. On August 27, 2019, Russian security provider Kaspersky Lab found that recent versions of the Android app distributed an advertising library containing a Trojan Dropper, which was also included in some apps preinstalled on several Chinese mobiles and our personal data hacking. The advertising library decrypts a Zip archive which subsequently downloads additional files from serves controlled by hackers, allowing the hackers controlling the

ISSN No:-2456-2165

device [2]. Google ,an American based organization, removed the application from the Google playstore. A new version of the application was launched by Google Play Store on September 5, 2019.

III. ANALYSIS OF ALGORITHMS TO IMPLEMENT PRIVACY MANAGEMENT

In general, a cryptographic system has two types of keys namely secret key or private key and public key. When the same key is used for both encryption and decryption such encryption, then that mechanism is known as secret key cryptography [8]. In a public key cryptosystem, different keys are used for encryption and decryption process. In a public key encryption cryptosystem, major elements are involved are plain text, encryption algorithm, decryption algorithm, public keys, private keys and cipher text. A plain text is an information which is an input data and cipher text is the encrypted message which is also the output[4]. Public and private keys have been selected for encryption and decryption process. The encryption process on the plaintext and decryption process on the cipher text follows several algorithms.

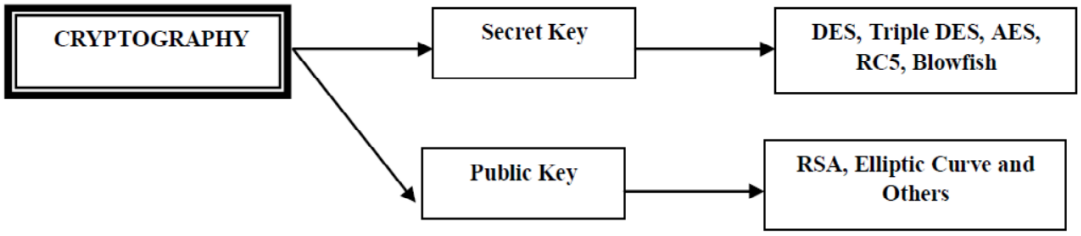


Fig 2

A. Diffie-Hellman Key Exchange:

Two users namely Alice and Bob have to agree on p and q in private and they choose positive whole-number personal keys as a and b, both less than the prime-number modulo p. Each side maintain 'a' as private value and 'b' as public value. Next, Alice and Bob figures out public keys a* and b* based on their personal keys according to the formulas:

- $a^* = q^a \bmod p$

and

- $b^* = q^b \bmod p$

These two users share their public keys a* and b* over a transmission medium assumed to be insecure, such as the Internet. From these public keys, a number x can be made to generate by either user on the basis of their own personal keys. To compute X, Alice uses the formula

- $x = (b^*)^a \bmod p$

Bob computes x using the formula

- $x = (a^*)^b \bmod p$

The value of x turns out to be the same according any of the above two formulas. Exchanging of secret value has been made. However, the personal keys a and b, which are critical in the calculation of x, have not been transmitted/passed over a public medium. Because it is a large and apparently a random number, the two users can therefore, communicate privately over a public medium with an encryption method of their choice using the decryption key x[4].

B. RSA Algorithm:

RSA stands for Rivest, Shamir and Adleman who discovered one of the most secured way of encryption. It is a public key encryption technique. It is also named as RSA algorithm[7]. RSA algorithm consists of two keys namely a public key and a private key.

➢ *Implementing Rsa Algorithm:*

STEP 1: GENERATION OF RSA MODULES:
In the generation of RSA module, given two prime numbers p and q, their product 'N' can be evaluated as follows:

N=p*q

Here, we assume 'N' to be a specified large number.

STEP 2: DERIVED INTEGER
Here, we assume a number 'e' such that |e|>1 and it should be less than (p-1) and (q-1). There should be no common factor of (p-1) and (q-1) except 1(prime number).

STEP 3: GENERATION OF PUBLIC KEY
The two pair of numbers n and e forms the RSA public key and it is made public.

STEP 4: GENERATION OF PRIVATE KEY
To evaluate private key 'd' from the numbers p, q and e. The mathematical relationship between the numbers is given by

M= (p-1)*(q-1);
e*d=1 mod(M);

Extended Euclidean Algorithm uses the same formula which takes p and q as the input parameters.

➢ *Formula for Encryption:*

To encrypt the plain text message in the given scenario , we have a sender who sends the plain text message to another user whose public key is (n,e). The syntax is:

C = (P*e) mod n

➢ *Formula for Decryption:*

The decryption process includes analytics for calculation in a systematic approach[4]. Considering receiver C with private key d, the result modulus will be calculated as –

Plaintext = Cd mod n

C. Data Encryption Standard:

The Data encryption standard(DES), the data blocks are encrypted in a 64-bit block with a 56-bit key[4]. In this algorithm, transformation of 64-bit input to 64-bit output takes place. For reversing encryption, the same key is followed. The inputs include a plain text to be encrypted and the encryption key. The length of the plain text is 64-bits and the key length is 56-bits.

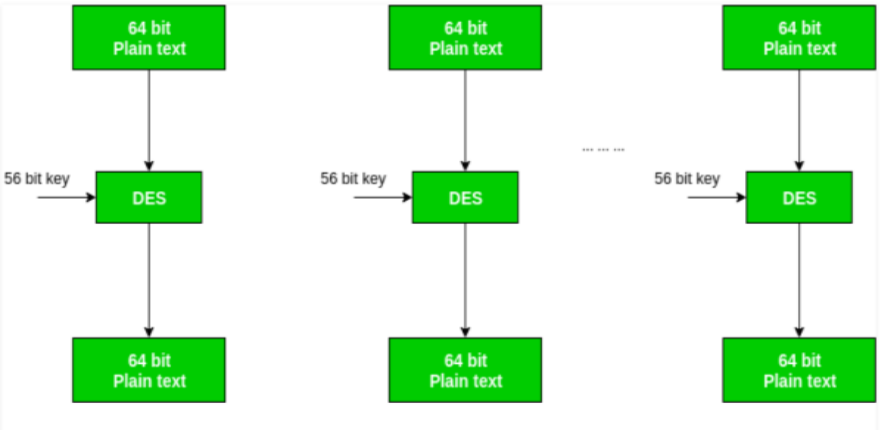
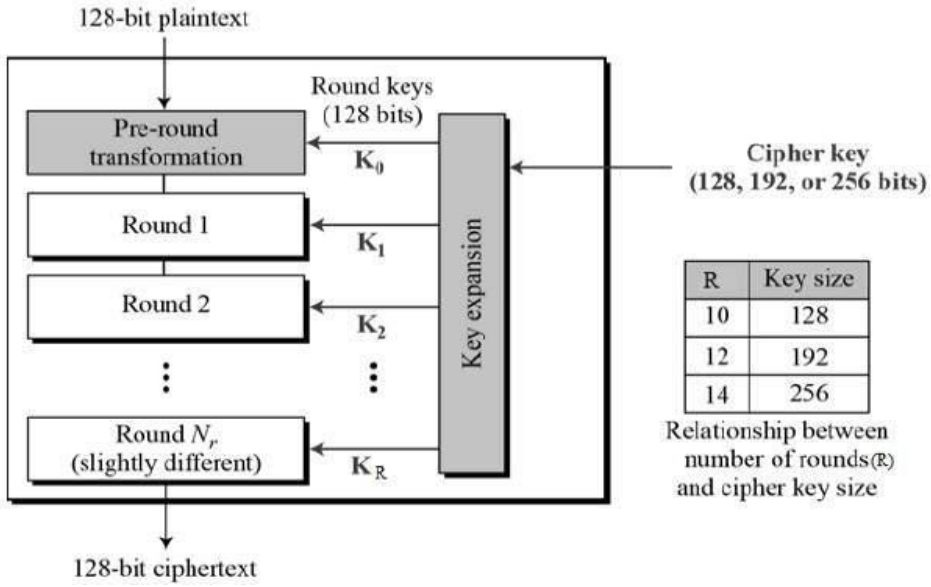


Fig 3

The left and right halves of the output are interchanged and pre-output is produced[4]. DES structure is similar to Feistal cipher. In the case of DES decryption, the same technique which is used for data encryption standard is followed with the keys reversed.

D. Advanced Encryption Standard:

Advanced Encryption standard also known as AES which is intended for replacing DES method of encryption. It is a symmetric block cipher technique[4]. In AES, the block size of plaintext is 128-bits which is considered by the cipher. The length of the key can be 16,24 ,32 bytes. This can be referred to as AES-128, AES-192 or AES-256 algorithms which depends on the length of the key.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds (R) and cipher key size

Fig 4

The input given to the encryption and decryption algorithm is always a 128-bit block. In the case of FIPS PUB, 4*4 square matrix of bits is the input considered. The cipher consists of 'N' number of rounds and 'N' depends upon the key length. The number of transformations to be performed on data stored in an array is defined by AES structure. In the first (N-1) rounds, four distinct functions occur. They are SubBytes, ShiftRows, MixColumns and AddRoundKey[4]. In each transformation, there will be one or more 4*4 matrix as input and 4*4 matrix as output.

E. Blowfish:

Blowfish algorithm uses cipher whose key varies within 32 to 448 bits of length. It's features include selection of secured way of message transformation[1].

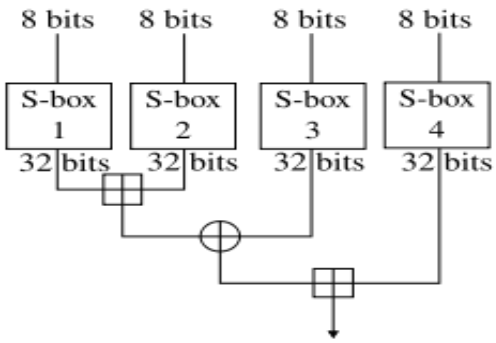


Fig 5

Linear and differential cryptosystems can be significantly analysed. It is available to both private as well as public sectors. It is a feistel network and it can be inverted simply performing XOR with blocks P17 and P18 to the ciphertext block.

IV. TECHNIQUES TO ACHIEVE A SECURED SYSTEM

A most significant component in information security is network security management. Network security consists of underlying computer network infrastructure, policies adopted by the network administrator in order to protect the network and its resources from unauthorized access, and continuous monitoring of the information. In the modern digital technology, organizations highly rely on computer networks to share the data throughout the organization in an efficient and productive manner. Confidentiality, Integrity, availability are the three major elements that contribute to a secured system which is represented by a CIA triangle[3].

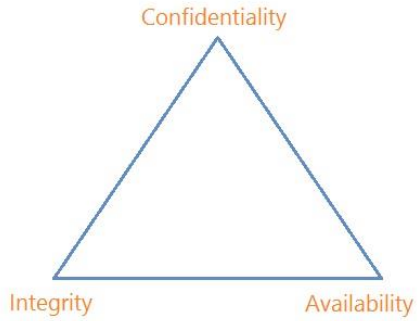


Fig 6

A. Confidentiality:

Confidentiality element of a network Security makes sure that the data is available only authorized persons The components of confidentiality include data encryption, access control, authentication, authorization and physical security. An authentication is a mechanism that ensures and confirms a user's unique identity that someone has. All data received needs to be authenticated if it is sent by trusted sender[6]. It is the necessity of every organization and institutions because it enables them to keep their networks secure by permitting only authenticated users to access its protected resources. The resources covers computer systems, databases, websites and other network-aided applications. Authorization is another security mechanism which gives permission to do or have something. It is used to determine whether a person or system is allowed access to resources, based on an access control policy. User identity verification is performed using authorization. System administrator's duty includes assigning permission levels covering all system and user resources. Physical security describes measures to design and to deny the unauthorized access of personnel resources and other properties from damage. It protects these assets from physical threats including theft, vandalism, fire and natural disasters.

B. Integrity:

Maintaining and assuring the accuracy and consistency of data is a way to achieve integrity of data. The data received by the recipient must be exactly same as the data sent from the sender, without change in even one bit of data. The elements of integrity include backups, checksums and data correcting codes. Backup includes archiving of data periodically. It is a process of making duplicate copies of data to use it in the event when the original data or data files are eradicated. It is mainly used to make copies for historical purposes, such as for longitudinal studies to meet the requirements of a data retention policy. A checksum is a numerical value that is generated by the data in a process to verify the integrity of a file. A checksum function entirely relies on the entire contents of a file. It is a method for storing data in such a way that small changes can be easily detected and automatically corrected.

C. Availability:

The term "Availability" in network Security is to ensure that the resources (data) are available to the legitimate users, whenever they require it. Availability ensures timely and reliable access to use the data[4].Physical safeguard and computational redundancies are the major elements in the availability of data. Physical safeguard is to keep information available even in the event of physical challenges. It ensure sensitive information is housed in secure areas.

Security services are provided by a protocol layer of communicating open systems to ensure adequate security of the systems or of data transfer[4]. This falls under X.800. Also the RFC 2828 defines security services as a communication service that is provided by a system to give a specific kind of security to system resources. Security Services can be implemented by security policy and mechanisms techniques.

- *Encipherment:*

It involves hiding and covering the data to achieve confidentiality. Traffic flow information is provided by encipherment technique to support other security mechanisms.

- *Data Integrity:*

Data integrity technique consists of a short checkvalue which is generated by the data during a particular process. At the receiving end, the receiver gets the data and the checkvalue. Receiver creates a new checkvalue from the received data and compares the new checkvalue and the received checkvalue. If the two checkvalues matches, data integrity is ensured.

- *Digital Signature:*

A digital signature is a technique through which sender electronically signs the data and the receiver verifies the signature in an electronic way. Public key and private key relationships are ensured and both the sender and the receiver prove their identities to each other. In other words, a digital signature ensures whether an electronic document is authentic or not. Digital signatures rely upon certain types of encryption process to ensure authentication. In encryption, all the data that one computer is sending to another is taken and encoded it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source[4].

- *Authentication Exchange:*

In this method, two users exchange key with each other to ensure their identities to each other[5]. Each user must have their unique usernames and secret key so that authorized persons can use it [6].

- *Access Control:*

Access control uses mechanisms to prove that a user has the right to use identities, information of principals[5]. If a mechanism attempts to use an unauthorized resource, the access control function ignores the attempt and reports this incident to produce alarm and recording it.

- *Traffic Padding:*

Traffic padding mechanisms are used in order to safeguard from heavy traffic analysis and its attacks. Traffic padding refers to the generation of bogus data and data units to reduce traffic congestion[5].

- *Routing Control:*

Routing control involves continuously monitoring the route to establish the shortest path between the sender and the receiver to provide communication. The information which is carried on certain security labels may be restricted by a security policy to pass through certain links. Handling the switching policy of outgoing data between ISPs in real time and its evaluation can be analysed using routing control[10].

- *Notarization:*

Notarization mechanisms allows establishing a third party to control communication between two or more entities, such as its integrity. With the third party establishment, repudiation is prevented[5]. This is done to store the sender's request and delaying is reduced.

V. CONCLUSION

Privacy management is the most important element in cryptography Techniques. This paper significantly examined several private and public key encryption techniques such as AES, DES, Blowfish, Diffie-Hellman ,RSA. Information security has become significant. Several algorithms have been evaluated and discussed. One can maintain privacy for his data using different security mechanism techniques like Cryptography, encipherment, data integrity, digital signatures, authentication exchange, firewalls, access controls and steganography. Essential mechanism techniques have been discussed to safeguard our personal data.

REFERENCES

[1]. Firewalls by Matthew Strebe, Charles Perkins.
[2]. https://en.wikipedia.org/wiki/CamScanner.
[3]. https://www.javatpoint.com/cyber-security-goals.
[4]. Cryptography and Network security by William Stallings.
[5]. Cryptography and Network Security by Behrouz A.Forouzan.
[6]. Anu, Divya Shree and Seema Ahlawat, " A review on Cryptography, Attacks and Cyber Security", IJARCS,Volume.8, No.5, May-June 2017.
[7]. Neha Sharma, Prabhjot and Er.Harpreet kaur, " A review on Information Security using Cryptography technique", IJARCS, Volume.8, No.4, May 2017.
[8]. A. Joseph Amalraj1, Dr. J. John Raybin Jose2, " A survey paper on Cryptography techniques", IJCSMC, Volume.5, Issue.8,August 2016,pp.55-59.
[9]. Rajesh R Mane," A review on Cryptography Algorithms, Attacks and Encryption Tools",IJIRCCE, Volume.3, Issue-9, September 2015.
[10]. https://www.webopedia.com/TERM/R/route_control.html