IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Cryptography

Mr. Swapnil S. Dalve

Dept of Computer Science, Dr. Babasaheb Nandurkar Collage of Physical Education and Computer Science, Yavatmal

Abstract: The uses of computer & communication systems by industry has increased day by day and the theft of proprietary information is also increased. For protecting those information encryption is a primary method which is used for protecting valuable electronic information now a days by the industry and military department. Cryptography is the most important aspect of communication and network security. Cryptography is encryption and decryption of the information which is transferred through internet and even more than this. Authentication is a part of privacy which provides the unique identity to the sender and receiver too. We use authentication in everyday lives - when we sign our name to some documents it shows that it's a valid document for this we need to have electronic techniques for providing authentication. A digital signature is also works like authentication in which sender needs to use his own digital signature which show that the information is send by the authorized sender. These cryptographic mechanisms can be used to control access to a shared disk drive, a high security installation. The problem of providing the security to the electronic information and electronic business transaction are became critical so for securing this data we are using all the above techniques: Symmetric Encryption Algorithm, Asymmetric Encryption Algorithm and many more.

Keywords: RSA- Rivest-Shamir-Adleman, DS- Digital signature, DES- Data Encryption Standard, 3DES- Triple Data Encryption Standard, AES-Advanced Encryption Standards, IDES- International Data Encryption Standard, Encryption, Decryption, Cryptography.

1. INTRODUCTION

1.1 Cryptography:
Cryptography is a Greek word krypton "hidden, secret" and graphing "Writing". It means secret writing of messages or files (data). Cryptography is art and science of preparing coded or protected communications through messages. Cryptography is the practice and study of hiding information using secret key of codes. In cryptography the original message is called as clear text or plaintext. The cryptography and cryptology are the terms used interchangeably by the academicians and researchers. The cryptography is important while communicating over a untrusted or trusted medium. The telecommunication and an internet are widely used network and many communications and transaction takes place on the internet. For the safe communication there are specific security requirements which include:

O Authentication: Authentication is the process of providing the identity of user.
O Privacy/Confidentiality: the process to confirm that the message has been read by only intendedreceiver.
O Integrity: Integrity the process in which the receiver ensured that the message has not be altered inany way from original.
O Non-repudiation: It is the process that ensures that the sender really sends this message.

The cryptography protects the data from theft or alteration. It is useful for user authentication. There are three types of cryptographic schemes.

1) Secret Key or Symmetric cryptography algorithm
2) Public Key or Asymmetric cryptography algorithm
3) Hash Function.

The scheme for the cryptography is shown on following fig.

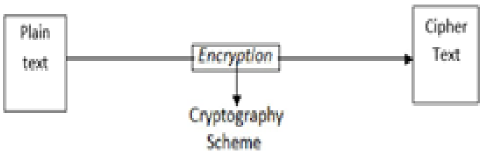

Figure1. Basic concept for cryptography algorithm

1.2 Cryptanalysis:
Cryptanalysis is the process of study of various encrypted information for obtaining the meaning of encrypted information. Cryptanalysis is the study of cipher text, cipher or encrypted message. Cryptanalysis is used to gain the access to the content of encrypted messages, even if we don't know the secret key. Cryptanalysis is known as breaking of the cipher, cipher text or encrypted messages. The main goal of cryptanalysis is to fine some weakness or insecurity in cryptographic scheme. Cryptanalysis is the common misconception that can be broken every encrypted method.

2. TERMS RELATED TO CRYPTOGRAPHY

1) Plaintext: Plaintext is a message or information which is original message before encryption.
2) Cipher text: Cipher text is a message or information after the encryption. When sender wants to send the message to someone and he applies some encryption algorithm on it and the output message is cipher text.
3) Secret Key: The secret key is input to the encryption algorithm for performing encryption on the plaintext.
4) Encryption Algorithm: The encryption algorithm performs number of substitutions and transformationson the original message to convert it into the cipher text or encrypted message.
5) Decryption Algorithm: This algorithm is reverse of

DOI 10.17148/IJARCCE.2016.56129

encryption algorithm. It takes the cipher text andthe secret key and produce original message or plaintext. It used to convert cipher text into plaintext.

3. TYPES OF CRYPTOGRAPHY ALGORITHMS

There are three types of cryptography algorithm. These algorithms are categorized based on the number of keys that are used for encryption and decryption.

1) Symmetric Encryption Algorithm/ Secret Key Cryptography: This algorithm uses only one key or same key forencryption and decryption too.
2) Asymmetric Encryption Algorithm / Public Key Cryptography: This encryption uses one key forencryption which is public key of receivers and another key for decryption which is receiver's private key.
3) Hash Function: This algorithm uses mathematical transformation to encrypt theinformation.

3.1 Symmetric Encrypt On Algorithm / Secret Key Cryptography

Symmetric algorithm is a secret key or it also called as shared / secret / single key algorithm. In this algorithm a single key is used for encryption and decryption.

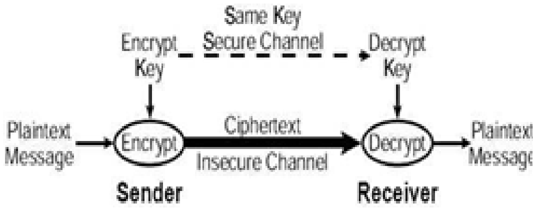

Figure 2: Basic Concept for Symmetric Cryptography

A sender uses the key to encrypt the plaintext. This encrypted plaintext sends to the receiver. The receiver uses the same key to decrypt and to recover the plaintext or the original message.

A single key is used for encryption and decryption. Hence secret key cryptography is called as symmetric encryption algorithm. The secret key must be known to sender and receiver also. The secret key cryptography faces the biggest difficulty that is distribution of key.

The encryption / secret key cryptography scheme is categorized into two types.

1) Block Cipher
2) Stream Cipher

3.1.1 Block Cipher: Block cipher is works on one block of data at a time. It uses the same key on eachblock. In general the same plaintext block always encrypt to the cipher text.

3.1.2

3.1.3 Stream Cipher: Stream cipher is works on a single bit or byte or computer word at a time. In thisscheme the key is constantly changing the security of this scheme depends on key stream generator.

3.2 Asymmetric Encryption Algorithm

Asymmetric algorithm (Public Key Algorithm) use two different keys for encryption and decryption and the decryption key cannot be derived from the encryption. Asymmetric algorithm uses one key for encryption which is public key of receivers and another key for decryption which is receiver's private key. The following fig. shows Asymmetric Encryption Algorithm.

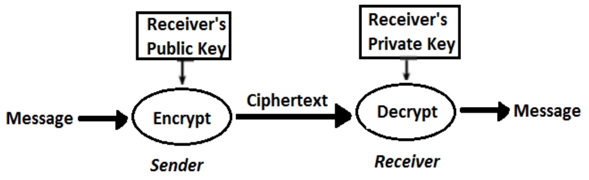

Figure 3. Basic concept for Asymmetric Encryption algorithm

Types of Asymmetric Algorithm

○ RSA (Rivest-Shamir-Adleman)
○ Digital Signature Algorithm m (DSA)

RSA (Rivest-Shamir- Adleman):

Rivest-Shamir-Adleman is the most widely used asymmetric algorithm (Public Key Algorithm). RSA is an algorithm used by modern computers to encrypt and decrypt messages. In RSA user creates and then publishes the product of two large prime numbers with an auxiliary value as their public key. The prime factor must be kept secret. RSA involve a public key and private key. The public key may be known to everyone. It is used to encrypt messages. Messages encrypted by using public key can be decrypted only using private key. The keys for the RSA algorithm are generated the following way:

Choose two different large prime numbers

p and q.Calculate n = p*q.

To encrypt a message m, it is exponential with a small public exponent e.

For decryption, the recipient of the cipher text

C = m e (mod n)

Compute the multiplicative reverse

d = e – 1(mod (p-1) * (q-1)) and obtains

c d = m e d = m(m od n).

The private key consists of n, p, q, e and d (where p & q can be omitted). The public key contains only n & e. The key should be greater than 1024 bits for a reasonable level of security. The following fig. shows the RSA.

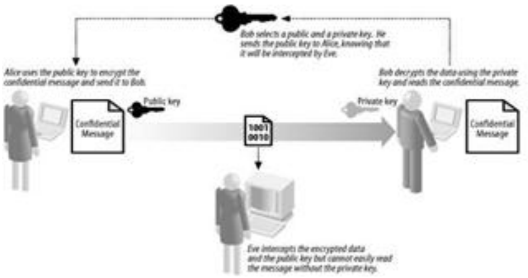
Bob selects a public and a private key. He sends the public key to Alice, knowing that it will be intercepted by Eve.
Alice uses the public key to encrypt the confidential message and send it to Bob.
Bob decrypts the data using the private key and reads the confidential message.
Public key
Private key
Confidential Message
1001 0010
Confidential Message
Eve intercepts the encrypted data and the public key but cannot easily read the message without the private key.

Figure4. Basic concept for RSA

Digital Signature (DS):
Digital signature is a cryptographic technique used to indicate the owner or creator of a document. Digital signature should be done in such way that a digital signature is verifiable, no-forgible and non – reputable. This is easily accomplished with public key cryptography. The following fig. shows the Digital Signature.

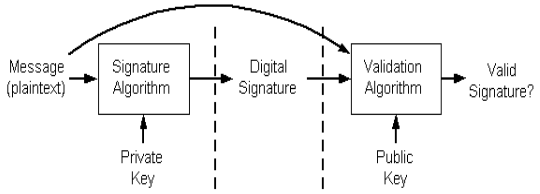

Figure 5. Basic concept for Digital Signature

In digital signature, sender uses his private key and DS algorithm and encrypt message then send the message to the receiver. Receiver uses senders public key to validate message and decrypt it.

3.3 Hash Functions:
Hash functions is called as message digests and one-way encryption. This algorithm use nokey Instead; a fixed-length hash value which is computed based upon the plaintext that makes it impossible to recover the plaintext. Hash algorithm isused to provide a digitalfingerprint to the contents of a file's to ensure that the file does not altered by an intruder or virus. Hashfunctions are also employed by many operating systems to encrypt passwords. Hash functions provide a measure of the integrity of a file.

4. CLASSICAL ENCRYPTION TECHNIQUES

All encryption algorithms are based on two general principles:

1) Substitution Techniques (Substitution Cipher)
2) Transposition Techniques (Transposition Cipher)

4.1 Substitution techniques :
Substitution is a technique in which each element in the plaintext (bit, letter, group of bits or letters) is mapped or replaced by another element. A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols for converting plaintext into cipher text. Substitution techniques having some types as follows:

- Caesar Cipher
- Mono alphabetic Cipher
- Poly alphabetic Cipher
- One Time Pad Cipher

Caesar Cipher: The Caesar cipher is simple, easy and most widely used encryption technique and it is easy to cracked encryptiontechnique. It is substitution type of encryption technique. In this technique each letter of plaintext is replaced by a letter it may be alphabet, numbers of some fixed number of position down the alphabet. For example,
Plaintext: Meet me after the party
Ciphertext: PHHW PH DIWHU WKH WRJD SDUWB
We can define the transformation by listing all possibilities, as follows:
Plain: a b c d e f g h I j k i m n o p q r s t u v w x y z
Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Mono alphabetic Cipher: Mono alphabetic cipher performs only 25 possible keys, the Caesar cipher is far from secure. A dramatic increase in the key space achieved by allowing an arbitrary substitution.
Consider the same example as above,
Plain : a b c d e f g h I j k i m n o p q r s t u v w x y z
Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! Or greater than 4 x 10^{26} possible keys. This is 10 order of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis approach is referred as a mono alphabetic substitution cipher.

Poly alphabetic Cipher: Poly alphabetic cipher is another way to improve the simple mono alphabetic technique.Which is use performs differentmono alphabetic substitutions on original message. This encryption technique is called as poly alphabetic substitution cipher. All these techniques have the following features in common:

- A set of related mono alphabetic substitution rules is used.

- A key determines which particular rule is chosen for a given transformation.

In Poly alphabetic cipher, the set of mono alphabetic substitutions consist 26 Caesar ciphers, with shift 0 through 25. Each cipher is replaced by a key letter which is the cipher text letter for that plaintext letter.Thus in this scheme B with a shift of 3 is replaced by the value E.

Key: deceptive deceptive deceptive

Plaintext :we are discovered save yourself

Cipher: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

One Time Pad Cipher: One time pad is said that it is a best cipher anywhere because it is untraceable as long as in this you can keep your message short, use shorthand and abbreviations, remove unnecessary letters, never reuse a pad, and have a good random source from data. This implementation will take the letters (and letters only) from the pad and encrypt the letters from your message. It leaves space, newlines, punctuation, numbers and all if the things that are not A-Z alone. Your message will not be encoded if your pad is at least as long as the number of characters in your message.

4.2 Transposition Techniques
Transposition technique is done by performing some kind of transformation on the plaintext letters or original message. Transposition techniques having some types which is as follows:

○ Rail Fence Cipher
○ Rout Cipher
○ Columnar transposition

○ Rail Fence Cipher: Rail fence cipher is form of transposition cipher. In this cipher the plaintext is written in downwards on successive "rail" of an imaginary railing then moving up when we get to the bottom, the message is then read off in the rows.

For example, if the plaintext is "meet me after the party", we can rearrange it by this way,

m e m a t r h p r y
e t e f e t e a t

So, we get the plaintext and cipher text like this:
Plaintext:meet me after the party

Ciphertext: mematrhoryetefeteat

○ Rout Cipher: In a rout cipher the plaintext is first written out in a grid of given dimension, then read off in apattern given in the key.

For example, using the plaintext
Plaintext: we are discovered flee at once.

w	r	i	o	r	f	e	o	e
e	e	s	v	e	l	a	n	j
a	d	c	e	d	e	t	c	x

The key might specify "spiral inwards, clockwise, starting from the top right" that would give a cipher text of

Cipher text: e jxctedecdaewriorfeonalevse

○ Columnar transposition: one more simple transposition cipher is called columnar transposition. In this cipher technique the message is written out in the form of row which is fixed length, and then read of again column by column. If the plaintext is "WE ARE DISCOVERED FLEE AT ONCE" we will compose the sentence into a 3 X 5 matrix.
For example:

Key:	4	1	2	3	5	6
Plaintext:	W	E	A	R	E	D
	I	S	C	O	V	E
	R	E	D	F	L	E
	E	A	T	O	N	C
	E	Q	K	J	E	U

Cipher text: ESEAQ ACDTK ROFOJ WIREE EVLNE DEECU

5. WIDELY USED SECRET KEY CRYPTOGRAPHY ALGORITHMS

○ DES (Data Encryption Standard)
○ AES (Advanced Encryption Standard)
○ IDES (International Data Encryption Standard)

5.1 Des (Data Encryption Standard):
The DES stands for Data Encryption Standard was once a symmetric key algorithm for the encryption of electric data. DES is now considered not too much secure for many applications this is because the 56-bit key size being too small. DES encodes plaintext in 64-bit chunks using a 64-bit key.The goal of DES is to completely scramble the data and key so that every bit of cipher text depends on every bit of the data and every bit of the key with good algorithm. Actually 8 of these 64 bits are odd parity bit so the DES key is effectively 56 bits long. The DES consist of two permutation steps (the first and last steps of the algorithm in which all 64 bits are permuted, and there are 16 identical rounds in between. The operation of each round is identical; it takes the output of the previous round as input. During each round, the rightmost 32 bit of input are moved to the left 32 bit of the output. The entire 64-bit input to the it round and the 48 bit key for the ith round are taken as input.

5.2 3DES:
If 56bit DES is considered to be insure, one can simply run the 56 bit algorithm multiples times taking the 64-bit output from one repetition of DES as the input to the next DES iteration, using different encryption key each time.
For example.

$C = E_{k3}[D_{k2}[E_{k1}[P]]]$
Where, C = cipher text
P = Plaintext
$E_k(x)$ = Encryption of X using key K.
$D_k(y)$ = Decryption of Y using key K.
Decryption is simple the same operation with the keys reversed.
$P = D_{k1}[E_{k2}[D_{k3}[C]]]$
3DES uses three keys and three execution of DES algorithm. The function follows an encryption – decryption – encryption as shown in following fig.

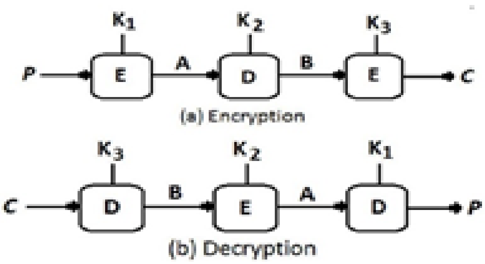

Figure 6. Basic for triple data encryption standard

5.3 AES (Advanced Encryption Standards):

AES intended by the NIST (National Institute of Standards and Technology) because of drawbacks of 3DES and DES is relatively slower. 3DES & DES is not a reasonable candidate for long term use. NIST 1997 issued call for proposal for a new Advanced Encryption Standard, which should have security strength equal to or better than 3DES. NIST specified that AES should be a symmetric block cipher with a block length of 128 bits & support for the key length of 128, 192 & 256 bits.

5.4 Ides (International Data Encryption Standard)

IDES stands for International Data Encryption Standard. IDES is originally called improved proposed Encryption Standard (IPES) is a symmetric key block cipher. IDES is designed by James Massey and Xenia Lai in 1991. This algorithm intended as a reinstatement for the Data Encryption Standard (DES). IDES operates on 64-bit block using 128 bit key.

6. CONCLUSION

Now a days we need to secure our data and business related information over the insecure network. For this security we are using cryptography techniques. In this scheme sender sends the information in secure manner over the open network so that the intruder could not alter or access that secured information. In this only sender and receiver are knows the keys of encryption technique to encrypt and decrypt the information. Today we are largely started using the cryptography scheme because all our information like business transactions, banking transactions, shopping transactions and other private information are done over the internet.

REFERENCES

[1] Dripto Chatterjee, JoyshreeNath, SuvadeepDasgupta, AsokeNath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[2] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms "2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 $26.00 © 2009 IEEE DOI 10.1109/CIS.2009.81.

[3] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 July, 2010, Vol-2,P-239-244.

[4] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[5] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag.

[6] By Klaus Felten "An Algorithm for Symmetric Cryptography with a wide range of scalability" published by 2nd International Workshop on Embedded Systems, Internet Programming and Industrial IT.

[7] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

DOI 10.17148/IJARCCE.2016.56129