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. 3, Issue 9, September 2015

A Review on Cryptography Algorithms, Attacks and Encryption Tools

Rajesh R Mane[1]

Research Scholar, Dept. of Computer Science, Symbiosis International University, Pune, India[1]

ABSTRACT: Data Security has become crucial aspect nowadays in every sectors .So in order to protect it various methods and Algorithms have been implemented. Cryptography combines Mathematics, Computer Science (Software+Hardware), Engineering and Networking. In this paper we have reviewed three basic cryptography algorithms. What are the different types of attacks to slow down network are defined. Basic tools of encryption for secure messaging, transactions and connectivity are pointed out.

KEYWORDS: algorithm, cryptography, data, encryption, security.

I. HISTORY & INTRODUCTION

Providing security and protecting data has become a very difficult task. Every organization today must have policies regarding data security .In order to provide security certain algorithms, tools should be implemented. Cryptography often called "code breaking" exists way back from ancient days. Most of it was used during wars to send messages in hidden format. In fact, the very word cryptography comes from the Greek words kryptos and graphein, which mean hidden and writing, respectively [1].It is mainly concern with algorithm. The initial recognized application of cryptography is originated in non-standard hieroglyphs engraved into monuments from the Old Kingdom of Egypt circa 1900 B.C. It was design in such a way to send message in coded format and would be easy for the receiver to read the message who knows to decode it . The sixth Century BC, consisted of covering a roll of paper around a cylinder and then marking the message on the paper. The unrolled paper was then send to the recipient, who could easily decode the message if he knew the diameter of the unique cylinder [10]. 2000 years ago Julius Caesar used a simple switch over cipher, recognized as the Caesar cipher Roger bacon described a number of methods in 1200s. Blaise de Vigenère published a book on cryptology in 1585, & explained the polyalphabetic substitution cipher. In India, secret writing was actually more superior, and the government used secret codes to be in touch with a network of spies spread all the way through the country. We bring up two of the outstanding offerings from this civilization. One of them is still used today, namely finger communications. Ancient India called this kind of communication "nirabhasa", where joints of fingers represented vowels and the other parts use for consonants. The second part of Indian civilization of ancient times is that they are accountable for the first reference in recorded history for the use of cryptanalysis for political purposes. Although no mechanisms are given for carrying out such suggestions, there is some cryptographic development seated in the information that such cryptanalysis could certainly be achieved [9]. In simple terms Cryptography is the technique to convert the message (Plain text) into coded message (encrypt) from Sender and transmit it to Receiver who converts(decrypt) the message into readable format(Plain text) after receiving it to avoid the message from getting stolen, damaged or lost and in order to protect it.. Cryptography has been emerged as important tool for data transmission. A variety of algorithms of cryptography have been studied[2].

Security Services: In security of information then following components need to be considered.

1. Privacy.
2. Verification.
3. Data Integrity.
4. Method ensures message transfer between parties.
5. Accessibility rights of Data.
6. Availability [4].

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. 3, Issue 9, September 2015

II. CRYPTOGRAPHY ALGORITHMS

1. SECRET KEY CRYPTOGRAPHY (SYMMETRIC) SKC:

It uses single key for *encryption* and *decryption*.

Types of Algorithms in SKC:

1. Data Encryption Standard (DES): The most familiar SKC format used these days, DES was proposed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for viable and inherent government applications. DES is a block-cipher method with a 56-bit key that operates on 64-bit blocks. DES has an important set of rules and transformations that were proposed in particular to give fast hardware implementations and slow software implementations.

Two significant components that built up DES are:

- Triple-DES (3DES): A variation of DES that uses up to three 56-bit keys and makes three encryption/decryption passes over the block;
- DESX: A alternative devised by Ron Rivest. By mixing 64 additional key bits to the plaintext earlier to encryption, increases the key length to 120 bits.

2. Advanced Encryption Standard (AES): In 1997, NIST initiated a very public, 4-1/2 year system to build up a creative secure cryptosystem for U.S. government applications. The end result, the Advanced Encryption Standard, became the official heir to DES in December 2001. AES uses an SKC design called Rijndael, a block cipher planned by Belgian cryptographers Joan Daemen and Vincent Rijmen. The algorithm can apply a variable block length and key length; the most modern dimension suitable for several combinations of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits.
3. International Data Encryption Algorithm (IDEA): Secret-key cryptosystem written by Xuejia Lai and James Massey, in 1992 and patented by Ascom; a 64-bit SKC block cipher operates with a 128-bit key.
4. Rivest Ciphers (aka Ron's Code): Named for Ron Rivest, a series of SKC algorithms.

RC1: Noted on paper but not at all implemented.
RC2: A 64-bit block cipher using variable-sized keys intended to change DES.
RC3: Found to be breakable at some stage in development.
RC4: A stream cipher with variable-sized keys; it is broadly used in business cryptography products.
RC5: A block-cipher sustaining a variety of block sizes (32, 64, or 128 bits), key sizes, and quantity of encryption passes in excess of the data.
RC6: A 128-bit block cipher based upon, and an upgrading over,RC5; .

5. *Secure and Fast Encryption Routine (SAFER):* Secret-key crypto system proposed for execution in software.
6. *SEED:* A block cipher using 128-bit blocks and 128-bit keys. Developed by the Korea Information Security Agency (KISA) and adopted as a national standard encryption algorithm in South Korea.
7. *ARIA:* A 128-bit block cipher employing 128-, 192-, and 256-bit keys. Developed by large group of researchers from academic institutions, research institutes, and federal agencies in South Korea in 2003, and subsequently named a national standard.
8. *GPRS (General Packet Radio Service) encryption:* GSM mobile phone systems use GPRS for information applications, and GPRS uses a various encryption methods, offering diverse levels of data safeguard.
9. Blowfish [10] is one of the most familiar public domain encryption algorithms developed by Bruce Schneier – one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specialized in cryptography and computer safekeeping. The Blowfish algorithm was first introduced in 1993.

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. 3, Issue 9, September 2015

TABLE1: COMPARISON OF ALGORITHMS

ALGORITHMS	CREATED BY	KEY SIZE	BLOCK SIZE
DES	IBM in 1975	56	64
3DES	IBM in 1978	112 or 168	64
AES	Joan Daemen & Vincent Rijmen in 1998	256	128
BLOWFISH	Bruce Schneier in 1993	32-448	64

Source: E. Thambiraja, G.Ramesh and Dr. R. Umarani in [12] have done survey on most common encryption techniques. Monika Agrawal and Pradeep Mishra in [13] have also done a comparative survey on Symmetric Key Encryption Techniques. Gurjeevan Singh, Ashwani Kumar Singla and K.S.Sandha in [14] have provided comparison of various cryptographic algorithms.

2. Public Key Cryptography (Asymmetric) PKC:

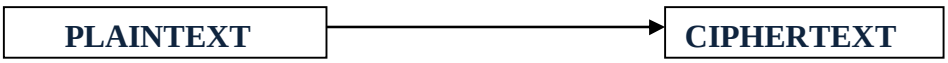
It uses two separate keys, one for *encryption* and second for *decryption*.

Types of Algorithms in PKC:

1. The first, and still most familiar, PKC development, named for the three MIT mathematicians who implemented it — Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA nowadays is used in hundreds of software products and can be used as a means of substitute, digital signatures, or coding of little blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is resultant from a very large number, *n*, that is the product of two prime numbers preferred according to special rules; these primes may be 100 or more digits in length each, yielding an *n* with almost twice as many digits as the prime factors. The public key information includes *n* and a derivative of one of the factors of *n*; an attacker cannot agree on the prime factors of *n* (and, as a result, the private key) from this information alone and that is what makes the RSA algorithm so safe and sound.
2. *Diffie-Hellman:* After the RSA algorithm was available, Diffie and Hellman came up and about with their individual algorithm. D-H is used for secret-key replace only, and not for verification or digital signatures.
3. *Digital Signature Algorithm (DSA):* The algorithm particular in NIST's Digital Signature Standard (DSS), provides digital signature skill for the proof of messages.
4. *ElGamal:* Designed by Taher Elgamal, a PKC system related to Diffie-Hellman and used for key swap over.

3. Hash Functions:

Hash Function



Hash functions, also called *message digests* and *one-way encryption*, are algorithms that, in some reason, use no key Instead; a fixed-length hash value is calculated based upon the plaintext that makes it not possible for both the contents and extent of the plaintext to be recovered. Hash methods are frequently used to present a *digital fingerprint* of a file's inside often used to make certain that the file has not been changed by an intruder or virus. Hash functions are also frequently engaged by many operating systems to encrypt passwords.

1. *Message* Digest *(MD)* algorithms*:* A sequence of byte-oriented algorithms that create a 128-bit hash value from an arbitrary-length message.
2. *Secure* Hash *Algorithm (SHA):* Algorithm for NIST's Secure Hash Standard (SHS).

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. 3, Issue 9, September 2015

3. RIPEMD*:* A sequence of message digests that at the start came from the RIPE (RACE Integrity Primitives Evaluation) project.
4. HAVAL *(HAsh of VAriable Length):* Designed by Y. Zheng, J. Pieprzyk and J. Seberry, a hash algorithm with numerous levels of safety measures. HAVAL can create hash values that are 128, 160, 192, 224, or 256 bits in length.
5. Tiger*:* Designed by Ross Anderson and Eli Biham, Tiger is intentional to be safe, run capably on 64-bit processors.

III.TYPES OF ATTACK

A. Security Threats

There are an amount of security threats that can be the beginning of a network security attack. Most important security threats are denial of service, distributed denial of service, viruses, Trojan horses, spywares, malwares, illegal way in to the network property and data, accidental erasure of the records and the uncontrolled internet access.

B. Virus assault

A computer virus is a program or an executable code that when executed and computer-generated, act upon different unwanted and damaging functions for a computer and a network. Viruses know how to destroy down your hard disks and processors, utilize memory at a very large scale and wipe out the overall performance of a computer or network. A Trojan is a malicious code that performs critical actions but it cannot be replicated. Trojan is capable of erasing systems important records. A computer worm is a program that replicates to all network and wipe out useful information. The viruses, malware, adware and Trojan horses can be controlled if you have a modernized antivirus program with the most up to date pattern files.

C. Unauthorized Access

Admission to the network resources and records should be allowed only to the approved persons. Every common folder and resources in your network must have been accessed only by the sanctioned persons and supposed to be scanned and monitored repeatedly.

D. Data stealing and cryptography attacks

One more threat to a network is loss of the major information and this loss can be prohibited, if you use good encryption methods such as 128 bit security or 256 bit security encryption techniques. In this manner your data when transferred during FTP programs, can be encrypted and cannot be read or use.

E. Unauthorized application installations

An additional virus and security assault prevention method is to install only the certified software applications to our set of connections i.e. server and all client computers. No one should be permitted to install any kind of program which can be source of security threats such as songs or video programs, gaming software or additional internet based applications.

F. Application-Level Attacks

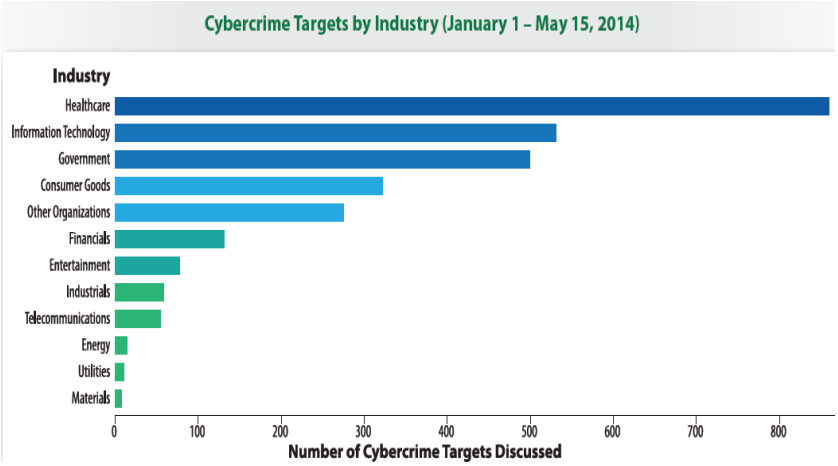
The invader exploits the limitation in the application layer – for example, security limitation in the web server, or in faulty controls in the filtering of an input on the server side. Examples malicious software attack (viruses, Trojans, etc.), internet server attacks, and SQL injection [5].

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. 3, Issue 9, September 2015



SOURCE: www.uscybersecurity.net/Pages/online_magazine.html [15]

IV. CYBER SECURITY TECHNOLOGIES:

1. Access Control and Identity Management:
The username/password combination has been a fundamental of computer access control since the early 1960s.
2. Authentication:
Documents need to be authenticated as having originated from a trusted source and that they have not been subsequently altered.

3. Malware scanners:
Software that is regularly scans files and messages for malicious code.

4. Firewalls:
A firewall program will monitor traffic both into and out of a computer and alert the user to apparent unauthorized usage.

5. Cryptography:
It is used in two main ways in information security. The better known is to provide confidentiality by encrypting stored data and data in transit [7].

V.ENCRYPTION TOOLS

One can setup a secure messaging system (email encryption), secure transactions (SSL enabled web browsers) and secure connectivity (VPNs and SSH) on a very small budget. Some of the small business/individual solutions available include:

EMAIL

- **PGP** – It is the defacto secure messaging standard on the Internet.
- **Hushmail** - Encryption tool for email. But unlike software tools it is a service built into web based email.

FILE ENCRYPTION

- **Private File -** Private File is a fast and easy way to protect yourself and your organizations by encrypting your files before sending them. With a simple drag-and-drop, or a menu point-and-click.
- **F-Secure FileCrypto** - developed by Datafellows Corp, this is a long standing file encryption application.
- **ShyFile** - free and paid versions of a strong encryption application that lets you create self-executable, encrypted packages.

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. 3, Issue 9, September 2015

VPNs

- **PGP** - certain versions of this application allow point to point encrypted VPN sessions.
- **Windows NT/2000/XP/Vista/7 & Linux -** they allow 'secure' data transmission between two nodes using the PPTP protocol.
- **Steg** runs on Linux, Windows, and OS X and can be used to securely hide data inside of other files. Steg's best feature may be that you can evaluate the changes that will be made to the host file so you can determine if they will be obvious to anyone who views the file that something else is going on[8].

VI. SUMMARY

Cryptography makes sure that the data when transferred over network is not modified. So in order to maintain data privacy cryptography algorithms are used to prevent the data being altered while in transit state. One can maintain security by having setup like anti-virus, anti-malware, regular updates, monitoring, spreading awareness and education.

REFERENCES

[1]Pawlan, M. (1998, February). Cryptography: the ancient art of secret messages. Retrieved May 4, 2009, from http://www.pawlan.com/Monica/crypto/.
[2] Pranab Garg1, Jaswinder Singh Dilawari2, A Review Paper on Cryptography and Significance of Key Length, IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012.
[3] Gary C. Kessler, An Overview of Cryptography, 1998-2015 — A much shorter, edited version of this paper appears in the 1999 Edition of Handbook on Local Area Networks, published by Auerbach in September 1998., http://www.garykessler.net/library/crypto.html.
[4] Vishwa gupta,2. Gajendra Singh ,3.Ravindra Gupta, Advance cryptography algorithm for improving data security, www.ijarcsse.com, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.
[5] Siddharth Ghansela, Network Security: Attacks, Tools and Techniques, www.ijarcsse.com, Volume 3, Issue 6, June 2013 ISSN: 2277 128X.
[6] http://www.crypto-it.net/eng/theory/introduction.html.
[7] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518.
[8] http://www.gfi.com/blog/the-top-24-free-tools-for-data-encryption.
[9] Debasis Das1, U. A. Lanjewar2 and S. J. Sharma3, The Art of Cryptology: From Ancient Number System to Strange Number System, Web Site: www.ijaiem.org, Volume 2, Issue 4, April 2013 ISSN 2319 – 4847.
[10] Kartalopoulos, Stamatios V. "A Primer on Cryptography in Communications." IEEE Communications Magazine (2006): 146-151. EBSCOHost. Georgia Tech Library, Metz. 16 July 2006.
[11] Pratap Chnadra Mandal "Superiority of Blowfish Algorithm," International Journal Of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.
[12] E. Thambiraja, G.Ramesh, Dr. R. Umarani, "A survey on various most common encryption techniques," International Journal of Advanced Research in ComputerScience and Software Engineering, Vol 2, Issue 7, July 2012.
[13] Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques," International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.
[14] Gurjeevan Singh, Ashwani Kumar Singla,K.S.Sandha " Performance Evaluation of SymmetricCryptography Algorithms," International Journal of Electronics and Communication Technology Volume 2 Issue 3, September 2011.
[15] Healthcare is a Growing Target for Cybercrime, and It's Only Going to Get Worse," United States Cybersecurity Magazine, Summer 2014, 1(4), p. 56. www.uscybersecurity.net/Pages/online_magazine.html.

BIOGRAPHY

Rajesh R Mane is a Research Scholar at Symbiosis International University, Pune, working at Vivekanand College,Kolhapur. He received MPHil in 2014, Master of Computer Application (MCA) degree in 2003. He has presented and published papers at various international conferences.His research interests are Cryptography,ICT,Information Security.