2nd International Conference on Recent Innovations in Science, Engineering and Management
JNU Convention Center, Jawaharlal Nehru University, New Delhi (ICRISEM-15)
22 November 2015 www.conferenceworld.in ISBN: 978-81-931039-9-9

CRYPTOGRAPHY A BOUNDLESS SECTOR

Akshat Kapoor[1], Ashish Golcha[2], Raman Solanki3

[1,2]CS, B.tech, IPEC, UP, (India)

[3]IT, Guru Gobind Singh Indraprastha University, (India)

ABSTRACT

Each of the data systems which are pact with cryptography is called crypto systems. The security of every crypto system particularly computes upon the structure of algorithm which is relevantly related to the algorithm and is mainly distinguished by the following:

- *Number of solutions.*
- *Number of levels etc it can hold.*

Data protection is a line of thinking and instigating the matter in modern high-tech world. There is an extreme demand for avigorous encoding which is a daring quest to break even by the brightest intellects. So the guarding level has to increase with time and the difficulty of algorithm has to enlarge.

I. INTRODUCTION

Cryptography is a creativity of concealing vital data related to any profession, workplace, federation, institution etc. There are various types of encoding algorithms used for unassailable information gear structure. Cryptography is rationalized as one of the oldest techniques engaged by the past culture for private transmission or conversation. The Egyptians are generally well known to have used cryptography on the catacombs of dead kings and leaders. Till futuristic moment cryptography is mentioned virtually or fully as encryption, which is the procedure of transforming standard data (called unencrypted text) into meaningless blather (called code text) . Decoding is the inverse in one term, operating from meaningless code text and reverse to unencrypted text. A code (or cipher) is a set of algorithms that generate encoding back to decoding. The complex procedure of a code is supervised both by the algorithm and in every occurrence by a solution. In casual work, the phrase "cipher" is frequently used to signify any procedure for encoding or confidentiality of a definition. Cryptanalysis, on a major attention, is the art of "unraveling" or "decoding" of encoding techniques. Cryptanalysts attempt to crack the procedure used in establishing the structure. Cryptography and Cryptanalysis as an entire form is used to define what is called as Cryptology.[1][3]

II. WHY CRYPTOGRAPHY

Confidentiality: To make sure information remains hidden. Confidentiality is normally attained using encoding. Symmetric encoding algorithms use the identical solution for encoding and decoding, while asymmetric encoding algorithms use a public/private solution pair.[2]

Data Stability: To verify that information is preserved from unintended/intended (hostile) change.Stability is generally provided by a piece of information authorization of cipher or hashes. A hash value is a stable extent numeral value obtained from organizing information. Hash values used to confirm the stability of information shipped through unprotected passage.[2]

Authentication: To ensure that information arise from a certain group. Analog acceptances (certifications) are used to provide verification. Analog trademark are generally applied to hash values as these are appreciably little than the reference information.[2]

Cryptography timeline

2003 First commercial use of quantum encryption[4]

2000 Advanced Encryption Standard (AES) developed[4]

1991 First quantum encryption system developed[4]

1984 BB84 protocol proposing quantum encryption published[4]

1978 RSA published[4]

1977 Data Encryption Standard (DES) created[4]

1976 Public key encryption proposed by Hellman and Diffie[4]

1970 Lucifer algorithm developed, later evolved into triple-DES[4]

1943-1945 First computer created[4]

1942 Navajo windtalkers used in World War II[4]

1923 Arthur Scerbius builds the German Enigma machine[4]

1917 Vernam cipher invented[4]

1854 Charles Babbage reinvents the wheel cipher[4]

1790s Thomas Jefferson invents the wheel cipher[4]

1585 Blaise de Vigenére writes a book on ciphers[4]

1553 Password idea introduced by GiovanBelaso[4]

50-60 BC Caesar Cipher introduced by Julius Caesar[4]

486 BC Greek skytale presumably used[4]

500 – 600 BC Hebrew ATBASH cipher used in writing the book of Jeremiah[4]

1500 BC Mesopotamian tablet with encrypted recipe for pottery glaze[4]

1900 BC First documented cryptography in Egypt[4]

III. CRYPTOGRAPHIC METHODS THAT ARE BEEN USED THESE DAYS AND IS BEEN TRANSFORMING FREQUENTLY

3.1 Elliptic Curve Cryptography

In 1985, Elliptic Curve Cryptography (ECC) was put forward separately by cryptographers Victor Miller (IBM) and Neal Koblitz (University of Washington). ECC is formed on the complication of resolving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Similar to prime factorizationIssue, ECDLP is one more “tough” problem that is cleverly easy to express. Elliptic curves integrate number theory and algebraic geometry. These curves can be described above whichever range of numbers (i.e. real, integer, complex), while we usually see themused as above limited range for the implementation in cryptography. An elliptic curve composed of set of real numbers (x, y) that serve the equation y 2 = x3 + ax + b. The set of all the answers to the equation produce the elliptic curve. Altering b and a, alters the form of the curve, and small alteration in the framework can result in the great alteration in the set of (x, y) results.[6]

3.2 Latest use of ECC:

Internet

In September 2002, SUN Microsystems donated to the applications of an ECC cryptographic library and besides an ordinary gear structure for accelerating ECC (as well as RSA) to be used in OpenSSL. OpenSSL is an artistic toolbox for the application of SSL (Secure Sockets Layer) 17 and TLS (Transport Layer Security) system of rules, which are generally used today in over-the-world deals and guarded contract transfers. SUN expects to encourage ECC standardization with SSL, which is the superior protection protocol used on the web today.[5] Lately in 1998, the Treasury Department's Bureau of Engraving and Printing finished a four month e-commerce pilot project including the use of smart cards, embedded with ECC technology, in making online purchases. This program inculpate overall 9 companies including MasterCard, Certicom (who provided the ECC algorithms), Digital Signature Trust Co. (who provided the MasterCard smart cards) and GlobeSet (a SET trader), just to tag a few.[5]

Smart Cards

Smart cards are one of the majorly favored pieces of equipment for the work of ECC. Many manufacturing companies like Phillips, Fujitsu, MIPS Technologies and DataKey, where as vendors that sell these smart cards include Funge Wireless and Entrust Technologiesuse ECC algorithm. Smart cards are flexible and situation independent.[5]

PDAs

PDAs has more computing power compared to most of the other mobile devices, like cell phones or pagers so is a very popular choice. 3Com4 Corporation teamed up with Certicom to implement ECC in the January of 1998 for the upgraded versions of PalmPilot organizer series and Palm platform. This version provided confidential information protection on the hand-held organizers, wireless communications was protected with user authentication and e-commerce transactions, and also ensures data integrity and proof of transactions.[5]

PCs

Personal computers are the most suitable platform for implementing ECC. Several companies use ECC to created software products that can secure data, encrypt e-mail messages and even instant messages.[5]

3.3 Quantum Cryptography

Photon polarization principle and the Heisenberg Uncertainty principle are important components of quantum mechanics that it depends on. Principle of photon polarization states that "an eavesdropper cannot duplicate unknown qubits" whereas according to principle ofHeisenberg uncertaintyDeciding the quantum state of any system is not possible without distributing that system.At Columbia University in New York early 1970s Stephen Wisner, then introduced the concept of quantum conjugate coding. In 1983 Sigact News issued the plan, and meanwhile two scientists Bennet and Brassard, knowing the idea of Weisner, were ready to issue their individual ideas. Then in 1984 "BB84" names quantum cryptography protocol was first delivered by them. There is a quantum property according to which "attaining the information is only possible is the signal is distributed into 2 states and that two states we are trying to individualizeare not orthogonal". In 1991 the very first experimental prototype was made based on this which functioned over a 32 centimeters. In June 2004 in Cambridge, Massachusetts the first computer network with communication secured with quantum cryptography is up and running. First packets of data across the Quantum Net were transmitted by the leader of the quantum engineering team at BBN Technologies in Cambridge, Chip Elliott. In April 2004, two Austrian banks tested the

first money transfer encrypted by quantum keys.[9][10][11]

IV. SOME LATEST TESTS ON QUANTUM CRYPTOGRAPHY

4.1 24 August 2015

A research team led by Ronald Hanson, Delft University of Technology reports the both detection and the communication loopholes of first Bell experiment. The team used "entanglement swapping" which is a cunning technique to combine the benefits of using light and matter both. Theytook two untangled electrons sitting in diamond crystals which held 1.3 kilometers apart in different Delft campus labs. Each electron was individually entangled with a photon, and both of those photons were then rushed to a third location. There, the two photons were entangled with each other and which caused the entanglement of both their associate electrons too. This did not work every time. In total 245 entangled pairs of electrons over the course of nine days were managed to be generated by the team. Besides, the experiment closed both loopholes immediately, as the electrons were easy to monitor, the detection loophole was not an issue, and they were separated far enough apart to terminate the communication loophole. A loophole-free Bell test also has crucial implications for quantum cryptography, says Leifer. To block eavesdroppers companies has already sold some systems that use quantum mechanics. The systems produce entangled pairs of photons and from this pair one photon in each pair is send to the first user and the other photon to the second user. Then turn these photons into a cryptographic key by those two users that only they know. Observing a quantum system interrupt its properties, an alarm will be set off as someone tries to eavesdrop on this process it will make a noticeable effect.[7]

4.2 16 October 2015

The record was broken for securing high bandwidth data transmission in Toshiba Research Europe's Cambridge lab and Adva Optical Networking at Adastral Park tech hub BT. This trial showed a system with a 200Gbps bandwidth applying quantum cryptography on a single fiber up to 100 km in length. The new system at Adastral Park makes higher bandwidth transmissions possibleby filtering the light to extract quantum signals from background and remove the need for dedicated fibers.[8]

V. CONCLUTION

It has been observed that algorithms like DES failed in providing security to electronic data in modern times. But an algorithm such as AES which is an extension to the concept of DES has been quite successful. So, cryptography is the field which will keeps on innovating and modernizing. Data security is that problem which will never be solved as some or ther way there are the loopholes will be brought to surface and hacked. As quantum cryptography is the most modern technique which scientists are working on. It is limited by distance so not usable for general or public sector, so it should be made more efficient. Cryptography has long way to cover and it's hard to see its upper limit.

REFERENCES

[1]. "A NEW APPROACH TOWARDS ENCRYPTION SCHEMES: BYTE – ROTATION ENCRYPTION ALGORITHM" SunitaBhati , Anita Bhati , S. K. Sharma, World Congress on Engineering and Computer Science 2012 Vol II WCECS 2012, October 24-26, 2012, San Francisco, USA.

[2]. "A STUDY ON MODERN CRYPTOGRAPHY AND THEIR SECURITY ISSUES" Jyotirmoy Das, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 10, October 2014.

[3]. "HISTORY OF CRYPTOGRAPHY AN EASY TO UNDERSTAND HISTORY OF CRYPTOGRAPHY" 2013 Thawte Inc.

[4]. "ENCRYPTION TECHNIQUES: A TIMELINE APPROACH" T Morkel , JHP Eloff, issa 2004.

[5]. "Elliptic Curve Cryptography and Its Applications to Mobile Devices" Wendy Chou, University of Maryland, College Park.

[6]. "An overview of new trends in cryptography" S.Tamilselvan, R. SoundaraRajan and S.Tamilenthi. ISSN: 2076-5061.

[7]. http://www.nature.com/news/quantum-spookiness-passes-toughest-test-yet-1.18255 .

[8]. http://www.telecompaper.com/news/bt-announces-quantum-cryptography-breakthrough--1108132 .

[9]. "Quantum Cryptography: Realizing next generation information security" Miss. Payal P. Kilor ,Mr.Pravin.D.Soni, Volume 3, Issue 2, February 2014, ISSN 2319 – 4847.

[10]. "Quantum Cryptography" Richard J. Hughes D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer, LA-UR-95-806.

[11]. "Quantum cryptography" Bennett, C. H., Brassard, G., and Ekert, A. K, Sci. Am. 267, 4 (Oct.1992), pp. 50.