www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-5, Issue-5, Oct 2017
Review Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Synthesis of Cryptography and Security Attacks

M. Arora[1*], S. Sharma[2]

[1*]Department of Computer Science and Applications, Khalsa College, Amritsar, India
[2]Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, India

**Corresponding Author: bedimani.arora@gmail.com*

Received 29th Jul 2017, Revised 11th Aug 2017, Accepted 24th Aug 2017, Online 30th Aug 2017

Abstract- In the era of digital media safeguarding of a mechanized orientation system in order to accomplish the applicable objectives of conserving the uprightness, possibility and discretion plays an essential role. There is compilation of tools intended to guard data and to prevent hackers but still there is a peril of multifarious attacks on information. This document brings into light the aspects of security and attack on cryptographic techniques. In it we have examined diverse types of attacks feasible on cryptography. In due course, I have gauged some eminent contemporary cryptographic algorithms in search for the finest compromise in security.

Keywords- Attack, Attacks Analysis, Ciphers, Cryptography, Information security, Performance and Security, Symmetric algorithms

I. INTRODUCTION

In the present time, information security is an up- coming field as digitization is mounting in all spheres of life. Information security is the protection offered to information automated systems. It is restricted to computer system as well as to information in an electronic or machine comprehensible form. It concerns to all phases of preserving or conserving information or data in no matter what form or media. The resources of information comprise of hardware, software, firmware, information / data and telecommunicationS. Recently there has been a transformation in the information security requirements and this is offered by physical and administrative mechanisms. The subsets of information security are

1. Computer and network security
2. Information technology security
3. Information system security
4. Information and Communications technology security(ICT)

Each of these has diverse importance but the universal concern is the security of information. For sustaining the security there is a requirement to ensure a check on security attacks. The security against attacks incorporates anticipation of attacks and exposure of attacks in the system. In this document we have done qualitatively analysis of attacks feasible on cryptography.

II. TYPES OF ATTACKS ON CRYPTOGRAPHY

Attacks due to information known to Cryptanalyst (Cryptanalytic Attacks)

The peril of abundant attacks on cryptography depends on what access the cryptanalyst has to the plain text, cipher text or other aspects of the cryptosystem. This type of attack takes advantage of the features of the algorithm to endeavour and assume an explicit plaintext or to presume the key being used.

Sr.No.	Information known to cryptanalyst	Possible Attacks				
		Cipher text only	Known Plaintext	Chosen Plaintext	Chosen cipher text	Chosen text
1.	Encryption Algorithm	✓	✓	✓	✓	✓
2.	Cipher text to be decoded.	✓	✓	✓	✓	✓
3.	One or additional plaintext-cipher text pairs created with the secret key.		✓			
4.	Plaintext message chosen by cryptanalyst, collectively with its corresponding cipher text generated with the secret key.			✓		✓
5.	Purported cipher text chosen by cryptanalyst, mutually with its corresponding decrypted plaintext created with the secret key				✓	✓

Attacks due to communication channel properties known to cryptanalyst(also called network based attacks)

These attacks divergent from the above attacks in perspective to that it mingle decepting individuals into renouncing their keys.

Sr.No.	Type of attack	Criteria
1.	Man in the middle attack	The cryptanalyst coherent him in the channel connecting two parties and counters back with each party. The heading parties consider that they are restoring keys with each other.
2.	Timing/differential power analysis	This technique is approved by launching unsystematic turmoil into the computations or altering the categorization of the executable.
3.	Side channel attack	This assault clouts additional information such as time taken (or CPU cycles used), to carry out a calculation, voltage used and so on. It presumes cryptanalyst has right to use to the plaintext or cipher text and perhaps the cryptographic algorithm.
4.	Birthday attack	It is a scuffle attack that can muzzle out the blow in lashing out around algorithms. It is most often used to observe its impact in hash functions such as MD5 and SHA1

Attacks possible on block ciphers

Sr. No	Type of Attack	Criteria
1.	Brute force Attack	In this outlook initially we force down provision all the probable amalgamation of keys, and then try each key to cipher text to recuperate plaintext.
2.	Differential Cryptanalysis	It considers on an investigation of the innate process of the divergence linking the two correlated plaintexts as they are encrypted on the bottom of the identical key. By examining precisely, analysis of the accessible data, probabilities can be credited to each of the possible keys, and in due course the most apparent key is recognized as the accurate one.
3.	Linear Cryptanalysis	It makes use of a linear estimation to illustrate the performance of the block cipher. Specified adequate pairs of plaintext and matching cipher text, speck of information about the key can be attained.
4.	Algebraic Attacks	Algebraic attacks are a kind of techniques that reckon on for their accomplishment on block ciphers displaying a high degree of mathematical structure
5.	The Exploitation of weak keys	Insubstantial keys would lay an impact on the security of the block cipher. These are the uncertain keys with a existing value for which the block cipher in question will exemplify assured regularities in encryption or, in optional cases, an impoverished level of encryption.

Attacks possible on stream ciphers

Sr.No.	Type of Attack	Criteria
1.	Correlation Attack	The correlation attack was projected by Siegenthaler in 1985 [1]. The correlation attack takes advantage of the survival of a statistical dependence involving the key stream along with the output of a single constituent linear feedback shift registers (LFSR), " [2]
2.	Fault Attack	The fault attack is a dominant cryptanalytic tool. It is extensively applied in cryptosystems which are not exposed to direct attack. This attack in stream cipher was developed by Hoch and Shamir [3].In this attack, the attacker can affect some bit flipping faults to either the RAM or the internal register of the cryptographic device. Nevertheless, he had only a biased control over their number, location and timing. This model endeavours to reveal a situation in which the attacker has the ownership of the physical device, and the faults are transient rather than eternal [3].
3.	Distinguishing Attack	The distinguishing attacks in stream ciphers were pioneered by Coppersmith et al [4]. In a *linear distinguishing attack* one can monitor a key stream of some length (known plaintext attack), and presents an answer: whether the stream make steps towards the considered cipher, or certainly from a random source. Distinguishers are generally positioned on statistical analysis of the specified stream.
4.	Cube Attack	It has been set up by Dinur and Shamir [5] in 2009. "The attack makes use of the subsistence of low degree polynomial representation of a particular output bit (as a function of the key and plaintext bits) with the intention to recuperate the secret key. With the purpose of obtaining the secret key, the attacker sums this bit by and large possible values of a subset of the plaintext bits. The summations are used in order to obtain linear equations in the key bits which can be economically solved, " [6]
5.	Guess and Determine Attack	As stated by Ahmadi and Eghlidos [7] the Guess and Determine Attack is defined as:" In GD attacks, the attacker first speculates (the values of) a set of state elements of the cryptosystem, called a basis; hence, the name. The beginning can keep in touch with diverse elements of dissimilar states (multiple times). Subsequently, she concludeS the remaining state elements and running key sequence, and compares the consequential key progression with the pragmatic key sequence. If these two sequences are identical, then the estimated values are accurate and the cryptosystem has been broken, if not the attacker should replicate the above situation with other presumed values. " [7]. Foremost work with GD attack was created by Pasalic [8]. He commenced the GD attacks on LFSRs for stream ciphers.

III. ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS WITH RESPECT TO ATTACKS

The reason of attack is to explore the key used in the course of ciphering and deciphering. Each attack has a process to endeavour to ascertain the key that was used. At this juncture, in this segment we have talked about some frequently used cryptography algorithms and their vulnerability toward attacks.

A. Data Encryption Standard: It encrypts and decrypts 64 bit data at a time. The 56 bit cipher key is employed mutually for encryption and decryption [9] It is by and large used for conservative algorithm. The most practical attack on it to date is a **brute force attack**— demanding every possible key in turn, also three theoretical attacks are probable that can break the full 16 rounds of DES with theoretical convolution not as much as a brute-force attack however they call for an improbable number of recognized or selected plaintexts to bring about, and are not interested in practice. These three attacks are:

Differential cryptanalysis: It was revived in the late 1980s by Eli Biham and Adi Shamir. To rupture the full 16 rounds, differential cryptanalysis wants 2^{49} chosen plaintexts. DES was intended to be resistant to DC.

Linear cryptanalysis: It was presented by Mitsuru Matsui, and needs 2^{43} known plaintexts [10], the process was executed [11], and was the primary experimental cryptanalysis of DES to be expressed. There is no confirmation that DES was modified to be opposed to this type of attack.

Improved Davies' attack: Linear and differential cryptanalysis are universal techniques and can be useful to a number of schemes, Davies' attack is a specified technique for DES, initially recommended by Donald Davies in the eighties, and improved by Biham and Biryukov (1997)[12]. The biggest influential form of the attack needs 2^{50} known plaintexts, has a computational complexity of 2^{50}, and has a 51% accomplishment velocity

B. 2DES: Double DES is primarily perfection over DES. It is the algorithm in which DES is used twice, with two diverse keys. It is undoubtedly a superior adaptation of DES, however still it is not protected in opposition to Meet-In-the-middle attack. This attack involves discerning a few plaintext/cipher text pairs .The plain text is encrypted by means of all 2^{56}possible keys and results are stored. The stored results will include all possible encryptions. Then cipher text is decrypted using all 2^{56}possible keys. After decrypting with each key, check for a match with the stored outputs of the possible encryptions is done. When we have a match, we have located a possibly correct pair of keys. Now, perhaps more than one pair of keys will result in a match, but the number of pairs of keys that return matches should be small. We could try each possible pair of keys. If more than one plain text/cipher text correspondence is known (for the key pair), then other correspondences could be used to check which of the keys is correct.

*C. 3DES:*3DES was developed in 1999 by IBM – by a team led by Walter Tuchman. 3DES prevents a meet-in-the-middle attack. It acquires 64 bit block of plain text and key of 112 bits as input and generates cipher text of 64 bits. Permutation and substitution functions are applied in 48 rounds. Merkle and Hellman requires 2^{56} chosen-plaintext plaintext-ciphertext pairs[13] to defeat algorithm using 2^{56} operations and 2^{56} words of memory using a **chosen-plaintext attack** . Afterwards C. van Oorschot and Michael J. Wiener presents a known-plaintext attack on two-key triple encryption[14]

D. 3DES: Triple DES with two keys undergo meet in the middle attack so triple DES with three keys move towards subsistence. Despite the fact that it is more safe and sound but time-consuming than DES .It is applied by Fedral organizations to protect receptive data. It captures 64 bit plaintext in addition to 168 bit key to produce cipher text of 64 bits in 48 rounds. Triple DES with a "triple length" (168-bit) key is vulnerable to a meet-in-the-middle attack in 2^{56} space and 2^{112} operations[15]

E. Blowfish: Blowfish Algorithm was formulated peculiarly by Bruce Schneier. Encryption algorithm acquires a 64-bits block of plaintext and an inconsistent length key as input and produces a 64-bits block of cipher text as output [16]. Blowfish is known to be susceptible to attacks on contemplatively feeble keys.[17] Four rounds are vulnerable to second order differential attack[18]

F. CAST 128: CAST 128 Encryption algorithm is initiated by Carliste, Adams and Stafford Tavared of Entrust Technology in 1996[19]. It has a subtle impediment to peculiiar cryptanalysis, linear cryptanalysis as well as interrelated key cryptanalysis. It devises the consumption of key size inconsistent from 40 bits to 128 bits in extension to 8 bits each. It marks on 64-bits block of plaintext to produce 64-bits block of cipher text in 16 rounds. Known-plaintext attack was disclosed on (reduced-round) CAST-128 and CAST-256 by Jorge Nakahara Jr, Mads Rasmussen[20]

G. RC2 : It is a conventional block encryption algorithm.It is effortless to make use of 16-bit microprocessor.It attains input of 64 bit stored in the 16 bit words and formulates an output of alike size i.e. of 64 bits.The inconsistent key size is taken one byte upto 128 bytes.It is prone to related key attack.

H. RC5 :RC5 encrypts blocks of plaintext of length 32, 64, or 128 bits into blocks of cipher text of the identical length. The key length varies from 0 to 2040 bits. It obtains three parameters as input.1). w (word size) 2). r (number of rounds) 3). b (number of bytes in encryption key K). 12-round RC5 (with 64-bit blocks) is subjected to a discrepancy attack using 2^{44} chosen plaintexts[21]

I. International Data Encryption Algorithm (IDEA): It gets hold of a 64-bits block of plaintext besides a 128-bit key as input in conjunction with it constitutes a 64-bits block of cipher text as output [22]. The central differential attack involves at most 2^{29} chosen plaintext pairs and a workload of about 2^{49} additions modulo $2^{16} + 1$ to find two sub keys or their additive inverses modulo $2^{16} + 1$

Comparison table of cryptanalysis of various algorithms

Sr. No.	Name of Algorithm	Cryptanalysis
1.	DES	Brute Force Attack
2.	2DES	Meet in Middle Attack
3.	Triple DES(2)	A known plaintext attack
4.	Triple DES(3)	Meet in Middle attack
5.	Blowfish	Four rounds are subjected to second order differential attack
6.	CAST 128	Known plaintext attack
7.	RC2	Related key attack
8.	RC5	12-round RC5 (with 64-bit blocks) is liable to a differential attack using 2^{44} chosen plaintexts
9.	IDEA	Differential linear attack

IV. CONCLUSION

We have crypt figured out a variety of symmetric algorithms to facilitate the parameters which engage in a significant role in conniving a new security algorithm as an experienced cryptanalyst can design only a superior cipher. Till date every cryptography algorithm is susceptible to some attack so there is a want to extend extra security algorithms by dispensing emphasis on to other parameters in addition to transmission time of encrypted data, size of initiated cipher text, number of keys used to encrypt and decrypt data, size of keys etc. As stated by us there is requirement of security algorithm which makes use of multiple and independent keys with the aim of encrypt data also the size of cipher text should be less important than the size of plain text so that memory utilization can be condensed.

REFERENCES

[1]. T. Siegenthaler, "*Decrypting a class of stream ciphers using ciphertext only. Computers*", IEEE Transactions , Vol.C-34 Issue.1pp.81–85, 1985.

[2]. A. Canteaut, "*Correlation attack for stream ciphers*", Encyclopedia of Cryptography and Security, pp. 261–262. Springer US, 2011.

[3]. J. Hoch and A.Shamir, *"Fault analysis of stream ciphers*", In Chryptographic Hardware and Embedded Systems CHES 2004, Lecture Notes in Computer Science, pp. 240–253. Springer-Verlag, 2004.

[4]. D.Coppersmith, S. Halevi, and C.Jutla, "*Cryptanalysis of stream ciphers with linear masking*",. In Moti Yung, editor, Advances in Cryptology CRYPTO 2002, Vol. 2442 of Lecture Notes in Computer Science, pp. 515–532. Springer- Berlin Heidelberg, 2002.

[5]. I.Dinur and A.Shamir , "*Cube attacks on tweakable black box polynomials*", In Antoine Joux, editor, Advances in Cryptology – EUROCRYPT 2009, Vol. 5479 Lecture Notes in Computer Science, pp. 278–299. Springer- Berlin Heidelberg, 2009.

[6]. I.Dinur and A. Shamir, "*Applying cube attacks to stream ciphers in realistic scenarios",* Cryptography and Communications, Vol.4 Issue.3 pp.217–232, 2012.

[7]. H. Ahmadi and T. Eghlidos, "*Heuristic guess-and-determine attacks on stream ciphers*" Information Security, IET, Vol.3 Issue.2 pp.66–73, 2009.

[8]. E.Pasalic, "*On guess and determine cryptanalysis of lfsr-based stream ciphers*", Information Theory, IEEE Transactions , Vol.55 Issue.7 pp.3398–3406, 2009.

[9]. Kaliski, Burton S., M. Robshaw, "*Linear Cryptanalysis Using Multiple Approximations*" CRYPTO 1994: pp26–39

[10]. D. Bhowmik, A. Datta, A. Sinha, "*A New Perspective of Inferring from the output of Linear Cryptanalysis Attack*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.2, pp.38-42, 2017.

[11]. M.Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard", *Lecture Notes in Computer Science* Vol.839 pp. 1–11,1994.

[12]. E.Biham, A.Biryukov, "*An Improvement of Davies' Attack on DES*". J. Cryptology Vol.10 Issue.3 pp. 195–206, 1997

[13]. Sachin sharma and Jeevan Singh Bisht, "*Performance Analysis of Data Encryption Algorithms*", International Journal of Scientific Research in Network Security and Communication, Vol.3, Issue.1, pp.1-5, 2015.

[14]. Paul *C. van Oorschot and Michael J. Wiener*, "A Known-Plaintext Attack on Two-Key Triple Encryption", Advances in cryptology, proceedings of EUROCRYPT'90, LNCS 473, pp 318-325,1990

[15]. L.R. Mathew, "*A Survey on Different Cryptographic Techniques",* International Journal of Computer Sciences and Engineering, Vol.5, Issue.2, pp.27-29, 2017.

[16]. Schneier B, "*The Blowfish Encryption Algorithm", Dr. Dobb's Journal*,Vol.19,Issue 4, pp .38-40,1994.

[17]. O. Kara and C. Manap, *"A New Class of Weak Keys for Blowfish"* , (PDF). FSE 2007.

[18]. V. Rijmen *"Cryptanalysis and Design of Iterated Block Ciphers" Ph.D thesis*,1997

[19]. M. Adams. "*Constructing Symmetric Ciphers Using the CAST Design Procedure", Designs, Codes, and Cryptography* (12), pp283–316,1997

[20]. J.Nakahara Jr, M. Rasmussen, " *Linear Analysis of Reduced-Round CAST-128 and CAST-256"*SBSEG,pp 45-55,2007

[21]. A. Biryukov and E. Kushilevitz. " *Improved Cryptanalysis of RC5*" EUROCRYPT 1998.
[22]. Mewada S, Sharma P, Gautam SS., "*Exploration of efficient symmetric algorithms*". 3rd International Conference on Computing for Sustainable Global Development (INDIACom), India, pp. 663-666, 2016.

Author Profiles

Mani Arora has done MCA from Guru Nanak Dev University in year 2003 and M.Tech (IT) from GNDU in year 2006. She recently completed her Ph.D. in 2017 and currently working as Assistant Professor in Department of Computer Science and Applications, Khalsa College, Amritsar. She has published 08 research papers in reputed international journals including (Scopus & Elsevier) and conferences and it's also available online. Her main research work focuses on Cryptography Algorithms, Data Security. She has 12 years of teaching experience.

