THINK INDIA JOURNAL

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

A Study of Various Security Threatsin RSA

Sartaj Singh*, Ashok Sharma, Sandeep Kaur

**PhD Scholar, School of Computer Science and Engineering, LPU, Phagwara*

Associate Professor, School of Computer Science and Engineering, LPU, Phagwara

Assistant Professor, Guru Nanak College for Women, CharanKanwal, Banga

Abstract:

Data Security has been concern for all stakeholders no matters the customer types, organisations. Securing data in rest in cloud or somewhere else and even during the communication is always not trustworthy. The entire research in data security deals in these two cases only and no matter we claims a lot but very next moment leads us to another threats. In this paper we have examine the various threats found by various researchers in most adopted RSA algorithm.

Introduction

Cryptographic algorithm is deemed very important in cryptosystem for, as well as, maintaining authentic and confidential message. Encryption and decryption are the primary necessity for privacysecurity on the internet [18]. Creating secret keys Sk, is important to encrypt and decrypt the message. The size of the key depends on the number of bits in a message. Therefore, the key size must always be greater than the number of bits in the message. A ciphertext C, can be decrypted back into original message only by using the correct key K. A comprehensive key search, which may be called ‘brute-force’ also, is the rudimentary technique used for identifying the concept K. Many a time, it has been seen that a weakness of the key schedule of the cipher happens to better the efficiency of a comprehensive key-search-attack. With a sea-change in the improvement of technology, the computing performance of technology, the computing performance always tend to make the comprehensive key-search-attack a better practice against keys having a fixed length. At the time of the designing of DES, it was deemed very secure, as compared to a comprehensive key-search, apart from being a less costly hardware.

It is also possible that comprehensive key-search may be employed on desktop work stations or personal computer. Whereas comprehensive search of DES 56 – bit key space is likely to require a thousand years on the best available computer of the day, the development of internet made the utilization of thousands of gadgets in a speed-out-search possible by dividing the key-space. The search is executed by partitioning it and dividing small portions to each of a large number of computers. As a result, some specifically designed ultra-modern computer was need of the hour. In such computer a DES key was actually split into 22 hours during the month of January, 1999. The existing rate of growth in computer power is about 80-bit key, which is likely to offer a reasonable amount of security for say about 12-15 years more. It seems impossible that 128-bit keys, which are employed in International Data Encryption Algorithm (IDEA) will be broken by the comprehensive search in the near future. Same may be the case with the forth coming AES. In this research, to enhance the security and to reduce the size of M in RSA, Huffman Compression technique and DES are considered as proof of concept. The security factor is decided by the size of modulus in RSA algorithm, with the actual use of RSA cryptosystem.

RSA modulus is the result of two large primes; and the primes tend to become larger. As a result, an attack will necessitate far greater time-span to factor it. A number with bigger prime factors with specified properties is going to make it easier to factor. For instance, this will happen, if the prime factors are quite close to each other. To enhance the security and for compression, several authors have proposed different methods which are illustrated in a few publications. This review highlights some important techniques of the said algorithms that has been carried out already. They are presented in the following subsections.

Literature Review of Encoding, Compression and Encryption approaches

According to the origin – Shannon's coding theorem, log bp is the optimal length of code for a symbol. Here b is the number of symbols used to render output codes, while p is used for the input symbol likelihood.But there is a shortcoming of arithmetic coding in it. The update operation is slow; and so is the model look up. In this method, at least one multiplication per event is needed for fully precise form of arithmetic coding; whereas in some cases of implementations up to two divisions and two multiplications are needed, per even. Both, Lempel-Ziv coding as well as, Huffman coding are much faster, so far so, speed is concerned. It is because this method is represented straightway in the data structure. There is one more drawback of arithmetic coding – arithmetic codes. Resist poorly the occurring errors, when these are used with adaptive models. In a coded file, a single bit error, consequently makes the decoder's internal state show to be in error. As such, it makes the rest of the encoded file incorrect. Actually, this drawback is found almost in all the adaptive codes. Lempel-Ziv codes and adaptive codes of Huffman are no exception.

Huffman coding shows many useful and nice properties. It is widely used in many applications. However, there are also some significant limitations in it. The main drawback in this code is that any error in the coded sequence of bits is likely to propagate at the time of decoding. This issue is faced in many codes of varied length. The boundaries between code words cannot be ascertained beforehand, unlike fixed length codes. it can be found only while the process of decoding is in progress. The error moves into the succeeding codeword if the wrongly decoded sequence of bits does not occur at the end on the boundary of correct code word.

Tarek M Mahmoud presented a novel and efficient technique. It is a method comprising encryption for the security of SMS in the Symbian operating system. This technique is employed for the safe and secure sending of SMS from one mobile phone to the other. RSA based technique of encryption is also employed to dwindle the possibility of spying and eaves dropping. But here again, the problem arises that encryption enhances the length of text message. As such, the bandwidth is not utilized. Clemens Guhmann and Stephan Rein offered the method of data compression in mobiles. It offers less complicated arithmetic coding compression of the text transmitted through mobiles. Biham and Seberry bought in yet another method known as 'rolling arrays. This method comprises rotations and permutations. But this method is also not devoid of shortcomings. Its limitation is that the total 256 keystream KS does not depend on the M, which is to be encrypted.

Fenwick suggests the use of prevailing predefined variable length codes, as well as universal. They can also show satisfactory compression. It is also described as 'Sticky Move-to-Front' modification. It offers a quite useful and better compression of most files. The higher the compression ratio, the more efficient the algorithm is. But it does not mention about the security of the message while transmitting from one to the other.Data compression methodologies for loss free data presented by Porwal S et. al gives a comparative performance of Huffman and arithmetic encoding is greater and better as compared to that of Huffman's encoding. The time used and channel bandwidth is lowered and it is far better than Huffman encoding. When compared with Huffman coding, the compression speed is very low in arithmetic encoding.

Sreelaja and Pai suggest another method for the creation of KS, known as Ant Colony Optimization (ACO). This method is employed for the distribution of the characters for encryption in the M. An also Artificial Ants do not find their counterparts. At the same time, the encryption time grows higher. It is so because the phenomenon deposition depends on problem. It does not re-create real ants' performance. As per Imad Khaled Salah et. at analysis RSA cryptosystem cannot be broken by any attack algorithm in an effective and efficient way. Most attack seen the result of system'smisuse or wrong choice of parameters. Majid Bakhtiari and Mohd. AizainiMaarof created an effective and efficient stream cipher algorithm to produce 115 bits in a single round of the process randomly. At the same time, it enhanced the processes' resistance, in comparison to algebraic and correlation attacks of Berlekamp-Massey. However, some computers may be unable to create random bits effectively and efficiently.

IwanHandoyoPutro, Petrus Santoso suggested yet another novel technique for data compression. It is an arithmetic encoding-based technique. This method highlights the drawbacks of the length of the message. It showed a way-out for transmitting a message with more than 180 characters. Text compression, as well as, superfast searching has been shown by Khurana U and Koul. They demonstrated a better and efficient technique which provided higher compression ratios and speedier search through the text. In this way, if necessitates the development of mathematical models. In addition, increasing the speed of public key cryptographic algorithms and efficient implementation is also mandatory.

Various codes have been proposed in the literature for data compression and they are categorised as fixed length and variable length codes. Variable length codes use some statistical method in contrast with fixed length codes. Short codes are given to symbols or groups of symbols with a higher probability of occurrence in the variable length code.Longer codes are assigned to lower probability symbols or group of symbols.Individuals who design and implement variable-length codes will tackle these two problems, namely assigning unambiguously decodable codes and assigning codes with the very less average width. Huffman code[32] is one of the length codes of the function.It is a compression of loss-free data to represent a character in some other form. Using the known RSA public-key algorithm, the compressed code will be sent for encryption.

A symmetric block encryption algorithm translates a fixed length block of M data into a block of the same size of C data, while a stream cipher that works on smaller M units usually transforms bits or bytes.The block's flow ciphers are much faster than ciphers. The problem facing most stream ciphers is to produce one random bit in each process round as the output flow of the cryptosystem raises the risk of algebraic similarity with these cryptosystems[33].The one-time pad of Vernam is one of the stream ciphers that uses a randomly generated bits series. As the whole Ks is random, if he / she sees the P, even an adversary with infinite computational tools might guess the P.While the one-time pad of Vernam is perfectly safe, it is too hard to remember and store a K because the size of K is always taken as the size of M, so it is at least practical [34].

Abdul-Kader, Hadhoud, proved in [35]Minaam that DES fares better than 3DES. Muthumanickam T [36] proposed that the Rijndael‟s S-Boxes are the dominant element of the round function in terms of required logic resources. Each Rijndael round requires sixteen copies of the S-Boxes, each of which is an $8bit\times8bit$ look-uptable, requiring more hardware resources. In [37] MijanurRahaman, Md. Masudul Islam proposed how essentially quantum-based computation could change our conventional processing and communication in cloud system. They also described about the major advantages and major problem in progress of quantum computation. Erdem S SYanik Ko T [38] described a method for performing computations in a finite field GF(2N) by embedding it in a larger ring Rp. They proved that the multiplication operation is a product of convolution and the rearrangement of bits is the squaring operation. Multiplication operation in Rp has complexity N+1, which is approximately is doubly efficient than optimal normal basis multiplication (ONB).

In [39] Longa P and Miri A described an innovative methodology to create the composite operations of the form $dP+Q$ by applying the special addition with identical z-coordinate to the setting of generic scalar multiplications over prime fields.They showed that their methods offer the lowest costs, given by $1I+(9L)M+(3L+5)Sand\ 1I+(9L)M+(2L+6)S$, when using only one inversion. There are several drawbacks in symmetric-key algorithms. A novel approach in generating the K from the Ks for stream ciphers using the Primitive Pythagorean Triples (PPT) has been proposed by Gopinath Ganapathy and Mani K [40] proved that this method is used to reduce the number of keys to be stored and distributed.The requirement of storage space is minimized and the P is not taken as such. Instead, a code is generated based on Huffman code and also a mutation process is employed at various levels of the Huffman tree of each character. It is proved that the mutated code of each character is used for encryption with Ks, the corresponding ciphertext obtained from the encryption process is not easily predictable.

Md. Rubaiyat Hasan [41] presented a data compression using Huffman based LZW encoding technique for transmitting a digital image from a digital data source to a digital data receiver. He has proved that it improves better transmission speed and saves time. Rajan S Jamgekar et.al [42] implemented a file encryption and decryption using secure RSA. It shows that Modified RSA Encryption Algorithm (MREA) is used to encrypt files and transmit encrypted files to another end to be decrypted. It works for smaller file size whereas it takes more time for larger file size.[43] Monisha Sharma et.al described a novel approach of image encryption and decryption by using partition and scanning pattern. The author has proposed a loss free encryption of image and also accessing of variable lengths of the encryption keys.

Systematic Review of attacks on RSA

In 1998 Kocher P introduced, a new form of attack on smart cards and cryptographictokens, called power analysis. These attacks are based on monitoring the token's power consumption. An attacker can recover the secret information because the power consumption varies significantly during different steps of the cryptographic operation. Two types of attacks are defined namely.1. Simple Power Analysis (SPA) attacks work by directly observing a system's power consumption. 2. Differential Power Analysis (DPA) [44] attacks are more powerful using statistical analysis and error correction techniques to extract information correlated to private-keys. These attacks are very complex.It requires a high level of technical skill to implement these attacks.

In 2001, Boneh, DeMillo and Lipton [45] introduced an attack against RSA.This attack exploits possible errors on the RSA private operation in cryptographic devices. The RSA private operation is a very computer-intensive operation which consists of a modular exponentiation, using numbers typically in the range of 300 decimal digits and many of the implementations of RSA decryption. The Chinese Remainder Theorem (CRT) is based on working module$p$ and q (instead of module $n = pq$). It can affect a considerable improvement in the performance. They provided a technique for exploiting an error that occurs during decryption or signing and analysing the data, and an attacker could also factor the module and thus recover the private key of the device or the success of the attack, both input and output of the operation are needed. It only needs to cause an error in the system during the private operation to execute this type of attack (e.g. by voltage or clock speed variation). The main challenge of this is the primary duration freedom.

The success or failures of decryption operation indicates that the failure analysis exploits feedback. Failure analyzes used by attacks are typically ciphertext attacks chosen for adaptation. A decryption software tests the validity of the ciphertext transmitted. Bleichenbacher D launched this kind of attack in 1998. It's called the Attack of the Million Message[46]. This attack takes advantage of some implementations ' cryptographic message syntax.

Kocher P conducted timing attacks on RSA in 1995. Timing attacks take advantage of the private-key connection with the cryptographic process runtime.Personal RSA operations are serial exponentiation, using the personal-key d as an exponent.An algorithm called repeated squaring algorithm, in which the modular$m$, exponentiations are implemented using squaring algorithm. If the private-key is k-bits long and the loop running with bits of d and with $2k$ modular multiplications,the data is squared in each step and the execution of a modular multiplication if the current bit of the exponent is one. After measuring the runtime of the private operation on a large number of random messages, an attacker could recover bits of d one at a time, beginning with the least significant bit. While using a low public exponent, using this approach, the attacker only needs to find the first k/4 bits.

In 1996, Burt Kaliski [47] proved that the timing attacks potentially affect the implementations of the RSA and DSA algorithms in BSAFE and RSAREF which, like many other implementations, are optimized for performance and hence take an amount of time that can potentially be correlated with the input.

Burt Kaliski[48] addressed the decryption of RSA and the signing of computational complexity in 1997. It is directly proportional to private exponent size d and varies with length linearly. To increase computational efficiency, most low-power devices prefer to use small d.The limited d choice, however, may result in Michael Wiener's complete breakdown of the cryptosystem.He alsoshowed that if n is the modulus, d is the private exponent and then d< 1/3(n)¼ and the public-key(e,n), an attacker can efficiently recover d (Boneh and Durfee have recently improved the bound to d<n 0.292). In practical terms, a standard 1024-bit RSA module is recommended. It should be at least 300 bits long for the private exponent.Interestingly, if e is chosen e= 65,537 and then calculating, $dfromed$= 1 $mod\Phi$(n), then, it is guaranteed that the d of size is comparable to n and consequently preventing this attack from posing threat to the cryptosystem.

Review of Works Related to Weakness of Security on RSA

Many attacks seem to be the product of device abuse or bad parameter choice. Examination of the known attacks reveals that RSA has not proved to be unbreakable, although it has survived much cryptanalytic security in the last 30 years [49].

As per Fermat's little Theorem on the probable prime number if p is a prime and a is an integer co-prime to p, then ap-1-1 will be evenly divisible by p. Therefore, in the notation of modular arithmetic: ap-1=1 (mod p). Otherwise, p is composite number. RSA algorithm is working on the base of two prime numbers p, q. The Fermat"s theory could be expanded in some part of RSA algorithm as follows: $n=p\times q$, $\emptyset n=(p-1)(q-1)$.

Public-key and the secret-key on the basis of f should be generated.Therefore, for all ciphertexts, chosen prime for RSA cryptosystem has at least two identical Sk in n domain and infinite similar secret key exists from the "n" domain.It also indicates that the absolute level of safety of RSA is not equal to the bit-length. When comparing each of the two chosen prime numbers, the RSA cryptosystem's security level is significantly lower than the digit length. Apparently, different cryptosystems are not tested properly.RSA numbers (p, q) have 40 secret keys that can be encrypted by a single public key to decrypt all ciphertexts. It is important to note that finding p in such a way that p±1 and q±1 are not sufficient conditions to have a broad prime factor advised by RSA laboratories [50]. Because of the stated conditions, similarity keys in the "n" domain cannot be fixed and to that, the serious weakness in RSA has been tried for all ciphertexts, the RSA cryptosystem has at least two related domains of n; and that there are countless similar secret keys from n domain.Currently, it is not a correct evaluation between different cryptosystem and RSA proposed by Majid B and Mohd. A. Maarof [51].

Approaches of Generation of Keystream for Symmetric-key Encryption

EladBarkan, Eli Biham and Nathan Keller [52] in 2003 had demonstrated the attacks on A5/1 and A5/2, enabling hackers to access and decrypt Global Mobile Communication System (GSM) mobile phone conversations at any later date.The University of California at Berkeley's Alex Biryukov and Adi Shamir [53] in 2007 had published a weaker A5/2 algorithm analysis showing a work factor of 216, or around 10 milliseconds.EladBarkhan, Eli Biham, and Nathan Keller of Technion[52] described a cipher-text-only attack on A 5/2 that the off-the air encryption of only a few tens of milliseconds.

Timo Gendrulis[54] described a hypothesis to evaluate an attack on the A 5/1 stream cipher by running on the special purpose hardware device called COPACOBANA in 2008. Bluetooth has an E0 algorithm.Until now, numerous known attacks have been available on the E0 encryption scheme that could endanger Bluetooth's security. Algebraic attacks [55] and correlation attacks [56, 57] are the most well-known of them. With 4 shift registers with different lengths (25, 31, 33, 39 bits), E0 can generate a bit. Also, the last function that generates keystream in E0 such as A5/1 and A5/2 is simple XOR. Because of the linear XOR properties, the output Ks has a linear relationship with its inputs that can threaten the entire algorithm.This showed that the linear exit relationship can be reconstructed between the output sequence bits and the vast majority of the unidentified output bits[58].

The complexity of A5/2 should be 264, according to the GSM claim. Dorward and Quinlan [59] have proposed a robust data compression network packet with various compression algorithms to increase the packet network's efficiency. It is hypothesized that speed matters when condensing the network packets, particularly if there is a huge bandwidth relative to the computing power available.Shanmugasundaram and Lourdusamy[60] established various numerical compression algorithms as well as comparable standards. It has been concentrated on LZ77 and LZ78-based algorithms.

Many encoding, encryption and compression techniques were surveyed[61]. RC4[62] is a major software cipher for streaming. The first drawback of RC4 is that a small sub-set of main bytes can decide a large number of initial permutation bits.The insecurity of K is a second weakness if the attacker is exposed to a part of K. Baruah R, et.al [63] has shown that Burrows –Wheeler's Compression Algorithm (BWCA) performance analysis, the more effectivenessof thetransformation algorithms are rendered in combining different text files with different sizes and higher compression ratios with the proposed method.In the field of mobile communication, Anita Singhrova, Dr Nupur Prakash[64] provided a new technique. This technique has been proposed to analyse various security protocols in mobile devices. Different encryption and authentication techniques have been introduced that are necessary during mobile phone data transmission.

Conclusion

Various existing works related to encoding, compression and encryption, various attacks on RSA, enhancement of security, generation of keystream for symmetric key encryption algorithms and increasing the transmission speed of M have been studied. Their relevance to the existing cryptographic algorithms is also analysed. It is noted from the current literature that no one have suggested an integrated approach to the encoded compressed cryptosystem.Further PPT and U-matrix based key is not yet generated for symmetric-key encryption. These ideas motivate me to develop various mathematical models so that they could be stored as components in the proposed framework. Any user can use these components as methods for encoding and for enhancing the security of the cryptographic algorithms.

References

[18]Whitfield Diffie and Martin E. Hellman, “Exhaustive cryptanalysis of the NBS Data Encryption Standard”, Computer Magazine, pp. 74-84, 1977.

[19]Lenstra A K and Verheul E R, “Selecting Cryptographic Key Sizes”, The 2000 International Workshop on Practice and Theory in Public Key Cryptography (PKC2000), Melbourne, Australia, 2000.

[20]Shannon C E, “Certain Results in Coding Theory for Noisy Channels”, Information and control, Vol. 1, pp. 6–25, 1957.

[21]Tarek M Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed, “Hybrid Compression Encryption Technique for Securing SMS”, IJCSS, Vol. 3. Issue 6, 2010.

[22]Stephan Rein, Clemens Guhmann, Frank H. P. Fitzek, “Low-Complexity Compression of Short Messages”, IEEE, Data Compression Conference, 2006.

[23]Biham E, Seberry J, Py (Roo), “A fast and secure stream cipher”, Research Online: 2005.

[24]Fenwick P, “Burrows Wheeler Compression with Variable Length Integer Codes”, Software–Practice and Experience, Vol. 32, No. 13, pp. 1307–1316, Nov. 2002.

[25]Porwal S, Chaudhary Y, Joshi J, Jain M, “Data Compression Methodologies for Lossless Data and Comparison between Algorithms”, International Journal of Engineering Science and Innovative Technology (IJESIT), Vol. 2, Issue 2, Mar. 2013.

[26]Sreelajaa N K and Pai GAV, “Stream cipher for binary image encryption using Ant Colony Optimization based key generation”, Journal of Applied Soft Computing, Vol. 12, pp. 2879–95, 2012.

[27]Imad Khaled, Salah, Abdullah Darwish and Saleh Oqeilli, “Mathematical Attacks on RSA Cryptosystem”, Journal of Computer Science, Vol. 2, No. 8, pp:665-671, 2006.

[28]Majid Bakhtiari and MohdAizainiMaarof, “An Efficient Stream Cipher Algorithm for Data Encryption”, International Journal of Computer Science Issues (IJCSI), Vol. 8, Issue 3, No. 1, May 2011.

[29]IwanHandoyoPutro, Petrus Santoso and Maya Basoeki, “A Short Text Compression Scheme based on Arithmetic Coding”, 2007.

[30]Khurana U and Koul A, “Text Compression and Superfast Searching”, Thapar Institute of Engineering and Technology, Patiala, Punjab, India.

[31]Delfs H and Knebl H, Introduction to Cryptography Principles and Applications, Springer-Verlag, Berlin, Heidelberg, 2001.

[32]Data_Compression available at website: http://en.wikipedia.org/wiki/ Data_Compression.

[33]Meier W and Staffelbach O, “Nonlinearity Criteria for Cryptographic Functions, Advances in Cryptology”, EUROCRYPT ’89, J-J Quisquater and J V andewalle Editors, Springer Berlin / Heidelberg, pp: 549-562, 1990.

[34]Charles P fleeger and Shari Lawrence P fleeger, Security in computing, Fourth Edition, Prentice Hall of India Pvt Ltd., New Delhi, 2007.

[35]Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud, “Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types”, IJ Network Security, Vol. 11 (2), 2010.

[36]Muthumanickam T, “Performance Analysis of Cryptographic VLSI Data”, IRACST– International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 2, No. 1, 2012.

[37]MijanurRahaman and Md. Masudul Islam, “An Overview on Quantum Computing as a Service (QCaaS): Probability or Possibility”, International Journal of Mathematical Sciences and Computing (IJMSC), Vol. 2, No. 1, pp. 16-22, 2016.

[38]Erdem S S, Yanik T Ko C and C K., “Fast Finite Field Multiplication. In: C.K. Ko, c (ed.) Cryptographic Engineering”, Springer, 2009.

[39]Longa P and Miri A, “New Composite Operations and Precomputation Scheme for Elliptic Curve Cryptosystems over Prime Fields. In: PKC 2008”, LNCS, Vol. 4939, pp. 229-247, Springer, Heidelberg, 2008.

[40]Gopinath Ganapathy and Mani K, “Maximization of Speed in Elliptic Curve Cryptography Using Fuzzy Modular Arithmetic over a Microcontroller base Environment”, Lecture Notes in Engineering and Computer Science, World Congress on Engineering and Computer Science (WCECS), IAENG, San Francisco,USA, Vol. 1, pp. 328-332, Oct. 2009.

[41]Rubaiyat Hasan M D, “Data Compression using Huffman based LZW Encoding Technique”, International Journal of Scientific & Engineering Research, Vol. 2, No. 11, pp. 1-7, Nov. 2011.

[42]Rajan S Jamgekar and Geeta Shantanu Joshi, “File Encryption and Decryption Using Secure RSA”, International Journal of Emerging Science and Engineering (IJESE), Vol. 1, Issue 4, Feb. 2013.

[43]Monisha Sharma, Chandrashekhar Kamargaonkar and Amit Gupta, “A Novel Approach of Image Encryption and Decryption by using partition and Scanning Pattern”, International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 7, Sep. 2012.

[44]Jaffe J, “Introduction to differential power analysis. In: Summer School on Cryptographic Hardware, Side-Channel and Fault Attacks”, ECRYPT, pp. 42–45, 2006.

[45]Boneh D, DeMillo R A and Lipton R J, “On the Importance of Eliminating Errors in Cryptographic Computations”, Journal of Cryptology, pp:101–119, 2001.

[46]Bleichenbacher D, Kaliski B and Staddon J, “Recent Results on PKCS #1: RSA Encryption Standard”, RSA Laboratories, 1998.

[47]Kaliski B, Timing Attacks on Cryptosystems, RSA Laboratories, 1996.

[48]Kaliski B and Robshaw M, “Comments on Some New Attacks on Cryptographic Devices”, RSA Laboratories, 1997.

[49]Salah I K, Darwish A and Oqeili S, “Mathematical attacks on RSA cryptosystem”, Journal of Computer Science, Vol. 2, No. 8, pp. 665-671, 2006.

[50]Rivest R and Silverman R D, “Are strong primes needed for RSA”, Cite seer, 1997.

[51]Majid Bakhtiari and MohdAizainiMaarof, “Serious Security Weakness in RSA Cryptosystem”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue. 1, No 3, Jan. 2012.

[52]Barkan E, Biham E and Keller K, “Instant Ciphertext Only Cryptanalysis of GSM Encrypted Communication”, In Advances in Cryptology-CRYPTO 2003, Springer Berlin / Heidelberg, pp. 600-616, 2003.

[53]Alex Biryukov and Adi Shamir, “Real Time Cryptanalysis of the Alleged A5/1 on a PC”, Fast Software Encryption Workshop 2000, pp. 10-12, April 2000.

[54]Gendrullis T, Novotný M, and Rupp A, “A Real World Attack Breaking A5/1 within Hours”, Cryptographic Hardware and Embedded Systems –CHES 2008, 2008.

[55]Armknecht F and Krause M, “Algebraic Attacks on Combiners with Memory”, Advances in Cryptology - CRYPTO 2003, Springer Berlin/ Heidelberg, pp. 162-175, 2003.

[56]Hermelin M and Nyberg K, “Correlation Properties of the Bluetooth Combiner”, Information Security and Cryptology- ICISC’99, Springer Berlin / Heidelberg, pp. 17-29, 2000.

[57]Lu Y and Vaudenay S, “Faster Correlation Attack on Bluetooth Keystream Generator E0”, Springer, 2004.

[58]Petrovic S and Fuster-Sabater A, “An improved Cryptanalysis of the A5/2 Algorithm for Mobile Communications”, 2002.

[59]Dorward S and Quinlan S, “Robust data compression of network packets”, Bell Labs, 2000.

[60]Shanmugasundaram S and Lourdusamy R, “A Comparative Study of Text Compression Algorithms”, International Journal of Wisdom Based Computing, Vol.1, pp. 68–76, Dec. 2011.

[61]Devi A and Mani K, “A Survey on Various Encoding, Encryption and compression Techniques”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 7, Issue 1, Jan. 2018.

[62]RC4_Encryption-algorithm available at website: https://www.vocal.com/