Traditional and Hybrid Encryption Techniques: A Survey

Chapter · January 2018

DOI: 10.1007/978-981-10-4600-1_22

Avadhesh KUMAR Gupta
IMS Ghaziabad
36 PUBLICATIONS **156** CITATIONS
SEE PROFILE

(Dr.) Munesh Trivedi
National Institute of Technology, Agartala
135 PUBLICATIONS **1,930** CITATIONS
SEE PROFILE

Virendra Yadav
ABES Engineering College
30 PUBLICATIONS **424** CITATIONS
SEE PROFILE

Traditional and Hybrid Encryption Techniques: A Survey

Pooja Dixit, Avadhesh Kumar Gupta, Munesh Chandra Trivedi and Virendra Kumar Yadav

Abstract Information security is the process that protects its availability, privacy, and integrity. Access to stored information on computer databases has increased nowadays. Most companies store business and individual information in computer. Much of the information stored is highly confidential and not for knowing publicly. Data encryption is most traditional technique that secure highly confidential information by using some conventional algorithm, which already exist or prewritten. Most powerful part of encryption technique is key generation, which has two parts, one is symmetric key generation and another is asymmetric key generation. Nowadays hackers are easily capable to break the key with the help of modern high computing machines. Current need is strongly encrypted data which cannot be decrypt through cryptanalysis. Paper presented discusses some traditional as well as modern hybrid encryption techniques along with quantum approach such as RSA based on ECC with AVK, DES-RSA, RSA-based singular cubic curve, JCE, 3D chaotic map technique, Blowfish.

Keywords Information security • Symmetric encryption technique • Hybrid encryption • Double encryption • Certificate-based-encryption • Link encryption technique

P. Dixit · M.C. Trivedi · V.K. Yadav (✉)
Computer Science Department, ABES Engineering College, Ghaziabad, Uttar Pradesh, India
e-mail: virendrashines@gmail.com; virendra.yadav@abes.ac.in

P. Dixit
e-mail: pooja.dixit68@gmail.com

M.C. Trivedi
e-mail: muneshtrivedi@gmail.com

A.K. Gupta
IMS Engineering College, Ghaziabad, Uttar Pradesh, India

G.M. Perez et al. (eds.), *Networking Communication and Data Knowledge Engineering*, Lecture Notes on Data Engineering and Communications Technologies 4, https://doi.org/10.1007/978-981-10-4600-1_22

1 Introduction

In all over world, nowadays, biggest challenges are confidentiality; everyone wants confidentiality in business, in social media, etc. Cryptography provides encryption techniques to resolve this problem. Cryptography is the concept which allows information to be sent in a secure form in such a way that only receiver is able to retrieve this information. Presently, continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm; these algorithms must consider many factors such as security, features of algorithm, time complexity, and space complexity (Fig. 1).

1.1 Security Services

If thinking about security, then following information comes in mind [1]:

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (data has not been altered)
- Non-repudiation (the order is final)
- Access control (Authorized person who has permission to access)
- Availability (presence)

Figure 2 explains some algorithms that help in providing confidential data. There are many algorithms to encrypt text into code word, but these algorithms are not sufficient because encryption is a very common technique for promoting the information security. The evolution of encryption is moving toward a future of endless possibilities. Everyday new methods of encryption techniques are discovered. As simple encryption algorithms are very easy to break by unknown user once

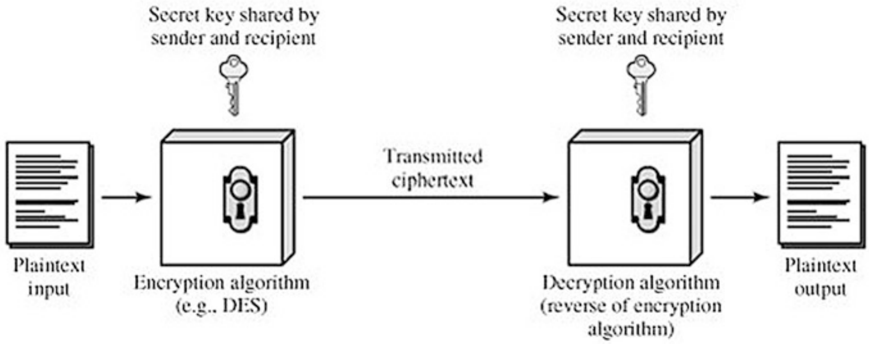

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig. 1 Conventional encryption

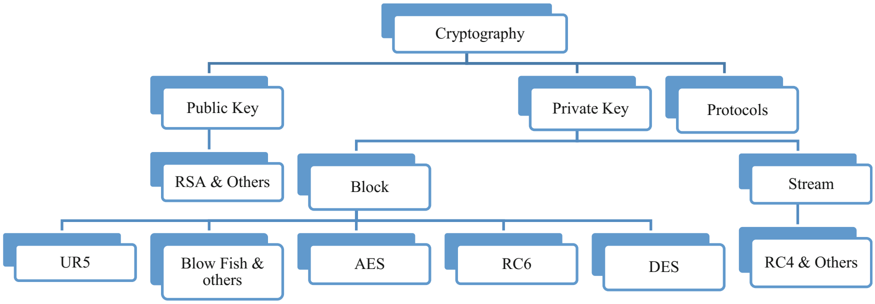


Fig. 2 Overview of most common encryption algorithm [1]

key or logic known. Paper presented discusses some cryptographic techniques under the heading “types of encryption technique,” researches in this domain under the heading “literature survey,” comparison of various techniques under the heading “Comparison,” and “Conclusion” contains the summary and future research directions.

1.2 Types of Encryption Technique

Commonly, three types of cryptographic techniques are symmetric cryptographic technique, asymmetric cryptographic technique, and hash function. In symmetric technique using single key encryption to encrypt or decrypt data. Data Encryption Standard (DES), Advance Encryption Standard (AES), Carlisle Adams and Stafford Tavares (CAST) algorithm, Blowfish, Two fish, International Data Encryption Algorithm (IDEA), and Secure and Fast Encryption Routine (SAFER) are some examples of symmetric encryption. In an asymmetric technique, two different keys are used, one (public) key for encryption and another (private) key for decryption, it may vice versa too. RSA, DSA, Elgama, and elliptic curve cryptography (ECC) are examples of asymmetric technique. The hash function uses a mathematical transformation to irreversibly “encrypt” information. This type of technique includes message digest (MD5), SHA-1, SHA-2. The RSA algorithm at present is the most successful in use for ciphering keys and password or counts [1].

2 Literature Survey

In 2015, Sourabh Chandra and Bidisha Mandalb proposed double encryption [2], which is content-based algorithm that implements folding method and circular bitwise operation. In this technique, encryption of plaintext occurs two times with secret key, providing cipher text by using circular bitwise binary addition operation. Algorithm of double encryption also exists. For better security, do double encryption of the text using secret key which is generated by a random number that is provided as an input. Encrypt a text by using a simple addition method on the ASCII value of each character with the length of corresponding word.

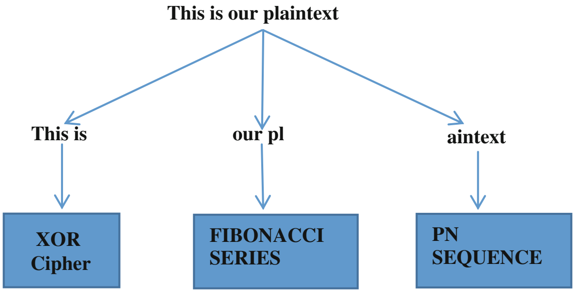
Hybrid technique, which has concept of combination of different-different algorithm. Each algorithm is unique having some strengths and weaknesses. In hybrid technique, use strength of technology and to overcome limitations use another technique together, so that will give best result in area of security. Lots of work have been done in hybrid technique such as AES-ECC [3], Fibonacci series-XOR bitwise-PN sequence [4], IDEA-RSA [5], and DES-RSA [1]. In this concept, plaintext is encrypted by an encryption technique using secret key and that secret key is encrypted by another technique. Then plaintext is encryptedusing encrypted secret key. But some of the algorithms use double encryption like AES-ECC, and this provides security for variety of multimedia data such as text document, images, audio, video. First, convert this data into base64 encoded version in text format [3]. At the initial level, generate key randomly by using AES, and then that key will be encryptedusing ECC public key. Then, encrypted AES key will be used to encrypt plaintext to generate cipher text. After do again encryption of AES encrypted text by using ECC public key. In Fibonacci-XOR logic-PN Sequence, still completed, divide input message into some blocks and all block contains equal number of characters. Every block is encrypted with the help of different types of techniques. For example, text is—"This is our plaintext" [4] (Fig. 3).

Another hybrid technique is DES-RSA, where DES algorithm is used to encrypt plaintext P with the help of session key (which is randomly generated) and give

$$C = E(k, P) \tag{1}$$

Cipher text as output [1]. Since DES is a secret key encryption/decryption model, this secret key has to be kept more secret and this is done by encrypting secret key with the help of public key encryption model which is RSA algorithm. DES's secret key is encrypted by public key, so this produces session key "u" [1].

Fig. 3 Split message into parts and apply three different techniques



$$\mathrm{u} = k^{e}(mod(n)) \tag{2}$$

Another encryption technique available is called RSAbased singular cubic curve with AVK [6], use to reduce time complexity. This technique is used to encrypt subpart of message rather than whole message.

Selective part of message will be encrypted with the help of RSA-based singular cubic curve, and rest of the part of message will be encrypted with the help of DES algorithm.

In this technique, first use data compression technique, that compress data, reduces the data size means it reduces space complexity and encrypt that compressed data by using AES algorithm to provide better security domain. This concept involves two types of procedure [7].

(1) Individual compression and encryption

- Compression followed by Encryption (CE): This technique provides more data security from access by unauthorized person, but size is more.
- Encryption followed by Compression (EC): This technique is not efficient due to decrease sequence in size, and this technique reduces space complexity. But in this technique hackers can access some clue regarding decryption of the cipher text.

(2) Joint Compression and Encryption (JCE): This method is faster and better than above two techniques. But this is very complicated for the implementation.

In encryption technique, one more name which is gaining attention of researchers is quantum encryption [8]. It is believed that when quantum computer will be built then every traditional algorithm will be break within few seconds. Every algorithm is based on key generation; if key is breakable, then unauthorized user can decrypt the cipher text. So, must be prepare for future challenges and try to make some quantum encryption technique. A lot of research is carrying out in this area. It is developed in 1994 by Peter Shor at AT&T Bell Laboratory. This technique uses principle of quantum cryptography which is Heisenberg uncertainty and photon of polarization principle. First prototype implementation of quantum cryptography in IBM, 1989 [8]'. In this paper most of the algorithm are discussed about encryption technique of text information only not for images, video, audio and graphics. In 2015, Pradeep H. Kharat proposed technique which is 3D chaotic map encryption technique. First time, Edward Lorenz used chaos theory in encryption system in 1963 [9]. All encryption technique is unique and effective to improve security domain. In 2014, Link Encryption Algorithm (LEA) used by Hadia M.S. El Hennawy, Alaa E.A. Omar, Salah M.A. Khaliah. In this chapter, proposed stream cipher algorithm that consists general structure of algorithm, key loading, and three types of layer: Linear Feedback Shift Register (LFSR) Layer, Bit Compression Layer, and Nonlinear Function F Layer.

3 Comparison

Literature survey discusses some common encryption algorithm which are combination of conventional (DES, 3DES, AES, Blowfish etc.) and public key (RSA, ECC etc.) algorithms. This section presents some comparison between symmetric key algorithm and comparison between some new techniques.

Table 1 mentions comparison between symmetric algorithms in terms of speed. According to Table 1, Blowfish gives better performance rather than other algorithms Table 2 compares performance of some algorithms. From Table 2, it is concluded that Blowfish give better result in comparison to techniques mentioned. In Table 2, LEA can be other preferred technique (Tables 3 and 4).

Table 1 Speed comparison of Block Cipher

Algorithm	Clock cycles per round	# of rounds	# of clock cycles per byte encrypted
DES	18	16	45
AES	14	12	40
IDEA	50	8	50
Blowfish	9	16	18

Table 2 Link Encryption Algorithm (LEA), performance comparison results [10]

Input size (bytes)	DES	3DES	AES	BF	LEA
20,527	2	7	4	2	2
36,002	4	13	6	3	4
45,911	5	17	8	4	5
51,200	6	20	10	5	6
69,545	9	26	13	7	8
79,776	10	31	15	7	8
87,968	11	34	17	8	8
96,160	12	37	18	8	8
103,056	13	40	19	10	12
Average time/sample	8	26	12	6	7
Bytes/s	7988	2663	5320	10,167	9285

Table 3 Encryption execution time of some technique in second

Bits	Hybrid	Compression and encryption	RSA-based singular cubic curve with AVK
256	0.004	0.003	0.004
512	0.005	0.002	0.005
1024	0.003	0.002	0.005
2048	0.004	0.002	0.011

Table 4 Comparison of various algorithms on the basis of different parameters [11, 12]

Parameter	Blowfish	Twofish	Threefish
Development	Bruce Schneier in 1993	Bruce Schneier in 1998	Bruce Schneier, Niels Ferguson, Stefan Lucks in 2008
Key length (Bits)	32–448	128, 192, 256	256, 512, 1024
Rounds	16	16	For 256, 512 key = 72 For 1024 key = 80
Block sizes (Bits)	64	128	256, 512 and 1024
Attack found	No attack is found to be successful against blowfish	Differential attack, related key attack	Improved related key Boomerang attack
Level of security	Highly secure	Secure	Secure
Possible keys	2^{32}, 2^{448}	2^{128}, 2^{192}, 2^{256}	2^{256}, 2^{512}, 2^{1024}
Time requires to check all possible keys	For a 448 bit 10^{116} year	Breaks 6 rounds out of 16 of the 256-bit key version using 2^{256} steps	For 512 bit and 33 round Time complexity is $2^{355.5}$
Parameter	Camellia	ECC	SAFER
Development	By Mitsubishi Electric and NTT in 2000	Victor Miller from IBM and Neil Koblitz in 1985	By Massey in 1993
Key length (Bits)	128, 192 or 256 bits	Smaller but effective key (example -512 bit)	For SAFER K-64, 64 bit For SAFER K-128, 128 bit
Rounds	18 or 24	1	4.75
Block sizes (Bits)	128 bits	Stream size is variable	64
Attack found	In future, algebraic attack, such as Extended Sparse Linearization	Doubling attack	Linear cryptanalytic attack
Level of security	Secure	Highly secure	Secure
Possible keys	2^{128}, 2^{192}, 2^{256}	2^{512}	2^{64}, 2^{128}
Time requires to check all possible keys	–	For 512 bit, 3 × 10^{4} MIPS-years	–

4 Conclusion

Data confidentiality is very important during transmission of information from client to server. Privacy is achieved with creating password of our file or generate code word of information (which ready to transmit), that easily understandable by those users who wants to share it. It is possible through information encryption. This paper presented explains encryption techniques available and used, which have strengths in term of security and computational performance. Like, Combined Concept of DES and RSA paper presented here but, can also use AES-RC4, SERPENT-RC4 and RC4-AES-SERPENT), using the same packet size of text data, sample ranging from (1 KB to 30 MB). But DSA-RSA hybrid technique is faster than other hybrid technique and in terms of throughput DSA-RSA is 54% better than RC4-AES-SERPRNT and 68% better than both AES-RC4 and SERPENT-RC4 [1]. In RSA-based singular cubic curve with AVK concept, reduces time complexity and provides comprehensive system functionality to be applicable in high-level security application domain. But in double encryption, this technique is best for small text or content. It is not suited for large content. The concept of AES-ECC technique reduces time complexity as expected and space complexity also less rather than other algorithm [3]. This hybrid methodology is more secure because ECC is robust technology which provides better security than others. Concept of compression of plaintext first and then encryption is good to provide more security, and it is best in term of file size and encryption execution time [7]. Quantum encryption concept mentioned in the presented paper is a better concept in terms of key distribution, unhackable, and less resources needed. Currently, signal is limited to 90 miles only comparison section evaluates some algorithms and techniques. From Table 1, it can be concluded that blowfish is good to encrypt data rather than AES, DES, and IDEA. And from Table 2 and Fig. 4, Compression then encryption technique is better than other current techniques in term of encryption execution time and performance of security. In future, more efficient algorithm can be developed, which uses both Compression and encryption (CE) technique along with quantum encryption concept which can withstand with modern high computing machines performing cryptanalysis (Fig. 5).

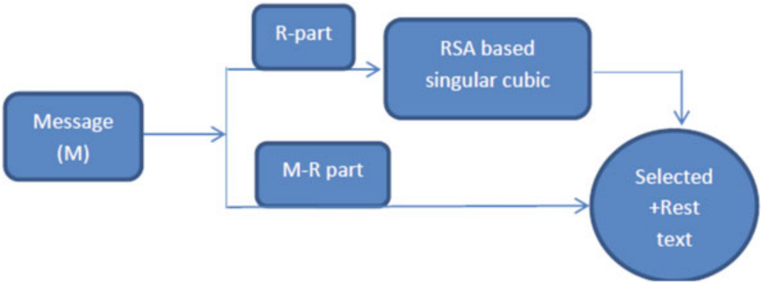


Fig. 4 RSA-based singular cubic curve with AVK [6]

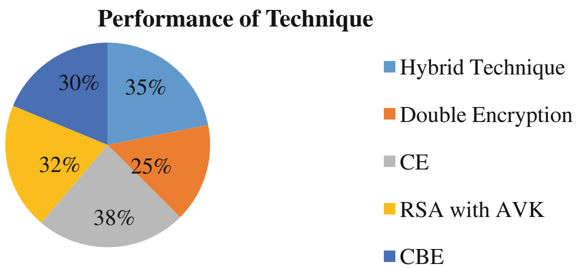


Fig. 5 Security performance of some technique

Acknowledgements I am thankful to my all professors who helped me to provide material regarding encryption technique and their valuable discussions hours.

References

1. Adedeji Kazeem B., Ponnle Akinlolu.: A New Hybrid Data Encryption and Decryption Technique to Enhance Data Security in Communication Networks: Algorithm Development. In: International Journal of Scientific & Engineering Research, Vol. 5, Issue 10, October (2014).
2. Sourabh Chandraa., Bidisha Mandalb., Sk. Safikul Alamc., Siddhartha Bhattacharyya.: Content based double encryption algorithm using symmetric key cryptography. In: International Conference on Recent Trends in Computing (2015).
3. Sridhar C. Iyera., R.R. Sedamkarb., Shiwani Gupta.: A Novel Idea on Multimedia Encryption using Hybrid Crypto Approach. In: 7th International Conference on Communication, Computing and Virtualization (2016).
4. Md. Atiullah Khan., Kailash Kr. Mishra., N. Santhi., J. Jayakumari.: A New Hybrid Technique for Data Encryption. In: Proceedings of 2015 Global Conference on Communication Technologies (2015).
5. WU Xing-hui.: Research of the Database Encryption Technique Based on Hybrid Cryptography. In: International Symposium on Computational Intelligence and Design. (2010).
6. Kalpana Singh.: Selective encryption technique in RSA based singular cubic curve with AVK for text based documents: Enhancement of Koyama approach. Deakin University, Dept. of Computer. Sci. & Eng., Motilal Nehru Nat. Inst. of Technol., Allahabad, India., DOI:10.1109/ICNIT.2010.5508497 Conference: Networking and Information Technology (ICNIT)., International Conference on Source: IEEE Xplore (2010).
7. Nur Nabila Mohamed., Habibah Hashim., Yusnani Mohd Yussoff.: Compression and Encryption Technique on Securing TFTP Packet. In: IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, April (2014).
8. Mehrdad. S. Sharbaf.: Quantum Cryptography: A New Generation of Information Technology Security System: http://ieeexplore.ieee.org/xpl/freeabsall?arnumber=5070885 (2009).
9. Pradeep H Kharat.: A secured Transmission of data using 3D chaotic map encryption and data hiding technique. In: International Conference on Industrial Instrumentation and Control (ICIC) College of Engineering Pune, India. May (2015).
10. Hadia M.S. El Hennawy., Alaa E.A. Omar b., Salah M.A. Kholaif.: LEA: Link Encryption Algorithm Proposed Stream Cipher Algorithm. In: 2014 Production and hosting by Elsevier B.V. on behalf of Ain Shams University (2014).

11. Milind Mathur, Ayush Kesharwani, “Comparison Between Des, 3DES, RC2, RC6, Blowfish And AES”. In Proceedings of National Conference on New Horizons in IT - NCNHIT 2013, ISBN 978-93-82338-79-6.
12. Rajdeep Bhanot, Rahul Hans, “A Review and Comparative Analysis of Various Encryption Algorithms”. In International Journal of Security and Its Applications, Volume 9, No. 4 (2015), pp. 289–306.