TEJAS Thiagarajar College Journal ISSN (Online):2456-4044 June2018, Vol 3(2), PP 62-69

COMPARATIVE STUDY ON CRYPTOGRAPHIC ALGORITHMS VS QUANTUM CRYPTOGRAPHY

M. Yogeswari[1] R. Chandrasekar[2]

[1]Assistant Professor, Department of Computer Science, Thiagarajar College – Madurai.
[2]Assistant Professor, Department of Computer Science, Thiagarajar College – Madurai.

ABSTRACT*:* This paper classifies the Cryptographic Algorithms versus Quantum Cryptographic Methods and presents a comparative survey. Cryptographic protocols can be classified by the type of security against eavesdropping which they provide. There exist mathematically secure schemes whose security relies on mathematical proofs or conjectures about the complexity of deciphering the message without possessing the correct key. The majority of current secure public Internet connections rely on such schemes. Alternatively, a cryptographic setup may provide a physically secure method for communicating. In these setups the security is provided by the physical laws governing the communication protocol. This paper presents a comparative study of three quantum key distribution protocols with two, three and four-state systems, respectively. Starting with the same dimension of input data, the percentage of errors is analysed by comparison with the dimensions of the cryptographic keys obtained in the case of each protocol.

KEYWORDS: Cryptography, AES, DES, RSA, BLOWFISH, DIFFIE HELLMEN, qubits, qutrits, ququarts, quantum cryptography

1. INTRODUCTION:

Cryptography, a word with Greek origins, means "secret writing" is the science of devising methods that allow for information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient. The message to be sent through an unreliable medium is known as plaintext, which is encrypted before sending over the medium. The encrypted message is known as cipher text, which is received at the other end of the medium and decrypted to get back the original plaintext message. Hence a cryptosystem is a collection of algorithms and associated procedures for hiding and revealing information.

Quantum information theory describes the communication and processing of information with symbols encoded in quantum mechanical systems, that is, as quantum signs, which by their nature are subject to physical constraints differing from those on classical signs. The development of quantum information theory has involved the replacement or generalization of traditional information-theoretic concepts so as to describe situations involving such signs, something that is necessary because quantum mechanical systems are described by non-standard probability distributions. This paper presents a comparative study of five cryptographic algorithms and three quantum key distribution protocols: two, three, and four-state quantum systems.

2. Cryptographic Algorithms:

2.1 Data Encryption Standard (DES) Algorithm Data Encryption Standard (DES) is a symmetric key block cipher algorithm which was developed by IBM in 1977. It uses a block size of 64-bits and a key size of 56-bits (where 8bits are the parity bits) to encrypt the plain text which is 64bit in size. It consists of a fiestal network which divides a block into two equal Halves where the right half passes through a function. DES has series of S boxes and P-boxes. After passing through the initial permutation and substitution box the cipher text is obtained by the EX-or operation which takes place within the set of rounds. Decryption is just the reverse process. Since DES is vulnerable to brute force attacks therefore it is proven inadequate in terms of security. In the DES algorithm has been modified (called M-DES) to improve the Bit Error Rate(BER)rate caused due to avalanche effect and is made more secure so that it can be used in wireless communication. To carry out this modification the authors have made use of S-box mapping tables. The second modification has been done from the work in where the authors have shown that DES can be cracked from the differential cryptanalysis attack if 247 pairs of Plain text and Cipher text are present. observed that BER rate is much better than DES because there is no Avalanche effect in MDES and as expected the algorithm came out with good results. After plotting and comparing the values of throughput obtained, it was observed that the proposed algorithm outperforms the use of the fixed 256-AES algorithm. It proved be powerful when the channel conditions were worst. Apart from BER rate throughput of the Encryption Algorithm must also be kept in mind.

2.2 Triple Data Encryption Standard (3DES) It uses block size of 64-bits with a key length of 56bits. As the name suggests it performs the same DES algorithm 3 times to each data block. Although the algorithm is vulnerable to brute force attack but it is comparatively more secure than DES. We tried a round addition attack

in Triple DES using Differential analysis .The secret key extracted by the attack can easily obtain one correct Cipher text and two incorrect Cipher text. Since triple DES is used in many applications today counter measures must be taken to implement a modified algorithm. the application of the triple DES has been discussed in the implementation of VLSI. Three different hardware implementations have been proposed where the first two are related to pipeline techniques and the third one is used for consecutive iterations for data transformations. T-DES has been implemented by look up tables and ROM blocks providing information regarding throughput and design area. With these implementations simulation was done to check out for the correct functionality. It was found that the result was validated by the know answer test vector mentioned in [8]. The authors have shown that ROM blocks provide better performance and throughput results as compared to the look up tables.

2.3 Advanced Encryption Standard (AES) Algorithm AES Algorithm is comparatively more secure and has a strong avalanche effect. Attackers cannot easily decrypt the encrypted text by the brute force attack. Therefore AES has been used in many applications. The implementation of AES for PDA secure communication has been described. The author introduces a linear complexity in the design of AES to make it more secure. There are many attacks the AES algorithm has undergone. An attack which is a combination of boomerang and rectangle attack with related key differentials introduced. This attack can break the round versions of AES. short cut attacks have been defined which are dangerous to the three AES block ciphers. There are attacks which occur due to the vulnerability of S-box in AES algorithm. We tried a new way of generating S box which can help from the algebraic attack. Authors also added their contribution to make up for the weakness of S-box and introduced an iterated hill climbing algorithm for the design of S-box. After further discussions new Algorithms were proposed to overcome the weakness in S-box design. We the security that AES Algorithm provides in accounting information where (Accounting Information Security System) AISS protect the accounting information data. The design of AISS based on AES is made which provides security from both internal and external attacks. Data security with Steganography and AES. Since AES algorithm is secure, it is used in hybrid form with other encryption algorithm, forming an onion layered structure and providing more security. A modified version of AES was introduced to carryout MPEG video encryption. The algorithm was modified just to overcome calculations and computer overhead. A drastic improvement in the speed and encryption performance has been observed.

2.4 Blowfish Encryption Algorithm Out of all the symmetric key algorithms, Blowfish Encryption Algorithm has a variable key length upto 448 bits. It has a block size of 64-bits. Blowfish algorithm consists of two phases. In the key expansion phase, 448 bit key is converted into number of sub keys totaling 4168 bytes. In encryption phase, a function is iterated 16 times and the encrypted text is obtained using EX-OR operation. Blowfish is a strong encryption algorithm so it has been used in many applications. In the author has shown nested watermarks which are embedded in a main image and these watermarks are encrypted before

embedding using blowfish algorithm. Results show a remarkable embedded capacity and security in the watermarks. Tests were done to check the performance of blowfish algorithm by increasing the file size and the key length. The equations derived from the result are kept for evaluating future performances. The design and implantation of Password Management System is also based on Blowfish Algorithm. The algorithm has also been used in bitmap image plotting instead of using secret algorithm like Skipjack algorithm in the Clipper and Capstone chips. Blowfish Algorithm has been used with other encryption Algorithms in hybrid form to enhance security and performance. Performance was also evaluated by modifying its function which brought up subsequent impressive results. In the next section, different asymmetric algorithms available for the cryptography along with their applications are discussed in detail.

3. Asymmetric key algorithms

3.1 Rivest Shamir Adlemen (RSA) It is a public key algorithm because it uses two keys pairs to encrypt and decrypt the message. Public key is used by the sender to encrypt the text and is known to all. However, to decrypt the encrypted text private key of the receiver is used. This private key, as the name suggests is known only to the receiver. No one else in the network has any knowledge about the key. The RSA consists of some mathematical operations through which one can calculate the encryption and decryption keys (e and d), after that one can easily calculate the cipher text and the plain text by the following formulae

$$C= M^e \bmod(n) \quad (1)$$

$$P= M^d \bmod(n) \quad (2)$$

Where in (1) and (2) M is the original message, e and d are public and private keys and n is a value obtained from mathematical operations in RSA. To carry outperformance analysis RSA was modified. In, the author has introduced an improved version of RSA which is based on complex numeric operation resulting in comparatively low computational power. The authors have proposed a mechanism to speed up large mathematical calculations by implementing the numeric operation on the array resulting in a low computational power. With this the loop time is decreased and the calculation speed is improved greatly. Although RSA is a secure algorithm, but in an experiment was done in the application of low private exponent attack in RSA where the author found out that there can be some new weak keys in RSA. Therefore, digital signature concept was introduced in combination with RSA. Keeping all the flaws in mind, in an algorithm implementing Digital Signature with RSA Algorithm was proposed to double the security of the algorithm. The RSA has been used in various applications like in electronic commerce trade which ensures integrity, confidentiality, authentication and non-repudiation. This algorithm is also used in the construction of mercurial commitments and with this it has shown its contribution in zero knowledge databases as well . In the next section, a comparative analysis of different algorithms is given.

3.2 Diffie–Hellman key exchange (DH) is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols. secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that

have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. Diffie–Hellman is used to secure a variety of Internet services.

FACTORS	AES	DES	Blowfish	RSA	DH
Key used	same key for encryption & decryption	same key for encryption & decryption	same key for encryption & decryption	different key for encryption & decryption	different key for encryption &decryption
Algorithm	symmetric	symmetric	symmetric	asymmetric	asymmetric
Key length	128,192 or 256 bits	56 bits key	Fastest Except when changing keys	1024 bits	Key exchange management
Speed	Fast	Fast	fast	Fast	Slow
Tunability	No	No	No	Yes	Yes
Power Consumption	low	low	high	high	high
Security	Excellent security	not secure enough	Secure enough	least secure	less secure than RSA
Cost	cheaper	costly	costly	costly	depends on key

Table 1 – Comparative analysis of Cryptographic Algorithm

4. The Quantum Key Distribution Protocols

4.1 The Quantum Key Distribution protocol with Two-State Systems. Using quantum bi-dimensional systems (qubits) realized the first quantum distribution key protocol. The quantum bi-dimensional systems are represented by states of photon polarization, forming two orthonormal bases: linear and diagonal.

Nr crt	initial qubits = 160		initial qubits = 320		initial qubits = 640		initial qubits = 1280		initial qubits = 2560	
	Final bits	QBER (%)	Final bits	QBER (%)	Final bits	QBER (%)	Final bits	QBER (%)	Final bits	QBER (%)
1	81	50	166	49	298	54	669	48	1312	49
2	86	47	160	50	327	49	664	49	1338	48
3	91	44	157	51	319	51	617	52	1267	51
4	70	57	181	44	309	52	652	50	1331	49
5	78	52	169	48	317	51	640	50	1344	48
6	75	54	149	54	314	51	645	50	1234	52
7	82	49	158	51	316	51	644	50	1300	50
8	84	48	176	45	329	49	626	52	1294	52
9	91	44	159	51	317	51	633	51	1288	50
10	81	50	162	50	313	52	641	50	1317	48
	81.41	49.20	163.21	49.13	315.68	51.06	642.75	50.17	1299.44	49.60

Fig 1 – Two State System

4.2 The Quantum Key Distribution protocol with Three-State Systems. The quantum key distribution protocol for the three-state systems, the so-called qutrits. For qutrits, bases called Mutually Unbiased Bases (MUB) are used, obtained by the application of transformed Fourier discrete. For the protocol BPP, four measurement bases are used, each having three individual vectors.

No. crt	initial qutrits = 160		initial qutrits = 320		initial qutrits = 640		initial qutrits = 1280		initial qutrits = 2560	
	No. final trits	QTER (%)	No. final trits	QTER (%)	No. final trits	QTER (%)	No. final trits	QTER (%)	No. final trits	QTER (%)
1	40	75	84	74	162	75	336	74	639	76
2	39	76	77	76	170	74	353	73	641	75
3	38	77	75	77	170	74	353	73	661	75
4	41	74	77	76	161	75	335	74	648	75
5	40	75	79	76	154	76	332	75	681	74
6	38	77	91	72	171	74	341	74	681	74
7	40	75	85	74	156	76	330	75	667	74
8	39	76	91	72	154	76	332	75	659	75
9	41	74	85	74	158	76	356	73	668	74
10	42	73	81	75	149	77	358	73	636	76
	39.76	75.18	82.15	74.56	160.17	75.29	342.28	73.89	657.91	74.70

Fig 2 – Three State System

4.3 The Quantum Key Distribution protocol with Four-State Systems. Using quantum systems with four-dimensions (ququarts). The Quantum Key Distribution protocol with Four-State Systems uses twelve orthogonal states in a four-state quantum system. Hilbert space associated to these systems has four-dimensions, and the three mutually unbiased bases (MUB), each with four eigenvectors.

No. crt	initial ququarts = 160		initial ququarts = 320		initial ququarts = 640		initial ququarts = 1280		initial ququarts = 2560	
	No. final bits	QQqER (%)	No. final bits	QQqER (%)	No. final bits	QQqER (%)	No. final bits	QQqER (%)	No. final bits	QQqER (%)
1	92	72	240	63	384	70	840	68	1692	67
2	96	70	216	67	400	69	816	69	1696	67
3	88	74	232	65	408	69	816	69	1692	67
4	100	70	212	68	404	69	860	67	1648	68
5	104	68	200	69	412	68	864	67	1676	68
6	84	75	188	71	428	67	876	66	1702	67
7	104	69	208	68	412	68	816	69	1652	68
8	108	67	224	66	444	66	872	66	1640	68
9	92	72	188	71	404	69	844	68	1656	68
10	100	70	200	69	396	69	852	67	1660	68
	96.23	70.62	209.49	67.61	408.60	68.38	845.02	67.58	1671.12	67.60

Fig 3 – Four State System

5. COMPARATIVE ANALYSIS

The Table 1 shows the comparative analysis between Cyptographic algorithms at different settings of key algorithms such as the key length, block size, rounds, power consumption, avalanche effect, processing time resource consumption and many other platforms.We have made many comparisons between the algorithms of the same type and reached to a conclusion that AES is faster and efficient than all other encryption algorithms. We have encrypted files with different contents and sizes. The results proved that Blowfish showed a good performance than the other encryption algorithms and therefore the processing time of the blowfish algorithm was high. AES performance was better than DES and 3DES and it took less time in encryption and decryption. Next property, Avalanche effect is a property of block ciphers in which the output bits change significantly on a slight change of the input bits. Blow fish has a maximum avalanche effect due to the number of EX-or operations which changes the output drastically. DES has avalanche lower than AES. RSA also has high avalanche effect as it involves the mathematical calculation of two large prime numbers. Now, talking about cryptanalysis resistance, authors have explained differential cryptanalysis for each of the algorithm. It was observed that DES is highly vulnerable to linear and differential cryptanalysis. It was also found that 3DES and Blowfish were vulnerable to brute force attacks whereas in case of RSA brute force attack was difficult. AES proved to be strong against differential, linear interpolation and square attacks. Therefore the crack to AES algorithm has not been found yet. Comparing with the other algorithms only DES is the most insecure algorithm as it has already been declared

inadequate to use. Fig 1, Fig 2, Fig 3 notifies the Comparative analysis of all the three quantum key distribution protocols respectively. Quantum Bit (Trit) Error Rate consists in the calculation of the percentage of errors from the key, obtained at the end of the quantum transmission, after the step of communication of the measurement bases from the public channel. Quantum Bit (Trit) Error Rate method may be applied to most of the key distribution systems, for detection of the enemy. Each system has its own accepted error rate, and exceeding it means the intervention of an enemy. By quantum key distribution [1,2], two entities, *the Sender and the Receiver*, establish together a unique and secure key, which may be used with a secure encryption algorithm, like *one-time pad* [3,4].

A classical scheme of quantum key distribution uses two communication channels, a classical one, and a quantum one, and it has the following main steps:

1. *The Sender and the Receiver* generate random and independent sequences of bits/trits

2. *The Sender and the Receiver* use a quantum key distribution protocol to compare the sequences of bits/trits, and to establish together a unique and secret key;

3. *The Sender and the Receiver* perform a procedure of error correction.

4. *The Sender and the Receiver* appreciate (according to the error rate) if the transmission was intercepted by *theenemy;*

5. *The Sender and the Receiver* communicate through a public channel and perform a procedure called *privacy amplification* [5,6];

6. *The final secret unique and secure key* is obtained.

We tested the applications on a variable number of input data (quantum systems), and studied how the quantum errors varied. The first important step of the protocol is when *the Receiver* measures the quantum systems received from *the Sender*. Taking into account that the Receiver chooses the measurement bases randomly, we may speak of the appearance of significant errors in the protocol.

5. CONCLUSION

This paper presents a comparative study of different key algorithms like, AES, DES, 3DES, Blowfish and RSA, Diffie Hellman. Each algorithm has been compared on different set of parameters. AES and Blowfish, are the most secure and efficient algorithms among the cryptographic algorithms. The speed and power consumption of these algorithms are better compared to the others. In case of asymmetric encryption algorithm, RSA is secure and can be used for application in wireless network because of its good speed and security. Quantum Key Distribution (QKD) protocols are also compared based on its performance and efficiency in protecting the data.

6. References

[1]. T. Bala and Y. Kumar, “Asymmetric Algorithms and Symmetric Algorithms: A Review,” International Journal of Computer Applications (ICAET), pp.1-4, 2015.

[2]. W. Stallings, Cryptography and Network Security, 4th Ed, pp. 58-309, Prentice Hall,2005.

[3]. W. Y. Zibideh and M. M. Matalgah , “Modified-DES Encryption Algorithm with Improved BER Performance in Wireless Communication,” IEEE Radio and Wireless Symposium (RWS) Phoenix, pp.219-222 , Jan 2011.

[4]. H.Yoshikawa, M. Kaminaga, A. Shikoda, and T.Suzuki, “Round addition DFA for microcontroller implemented the Triple DES,” IEEE Consumer

Electronics (GCCE) Tokyo, pp. 538-539,October2013.

[5]. W.Y Zibideh. and M. M. Matalgah , "An OptimizedEncryption Framework based on the Modified-DES Algorithm: A Trade-Off between Security and Throughput in Wireless Channels," IEEE Radio and Wireless Symposium (RWS) CA , pp.419-422, Jan 2012.

[6]. E.Biham and A.Shamir, "Differential Cryptanalysis of the Full 16- Round DES,"

Proceedings of Crypto'92,vol. 740, Santa

[7]. Barbara, CA, December1991

[8]. . P. Kitsos, S. Goudevenos and O. Koufopavlou, "VLSI implementations of the triple-DES block cipher," IEEE Electronics Circuits and Systems, Vol. 1, pp.76-79, December 2003.

[9]. NIST Special Pubilication 800-20, "Modes of Operation Validation System for the Triple Data Encryption Algorithm," National Institute of Standard and Technology, 2000.

[10]. LIU Niansheng , G. Donghui, and H.

Jiaxiang, "AES Algorithm Implemented for PDA Secure Communication with Java," IEEE Anti-counter. Sec. Ident. Fujian, pp. 217-222, April 2007.

[11]. E.Biham, O. Dunkelman, and N. Keller, "Related-Key Boomerang and Rectangle Attacks," Lecture Notes in Computer Science, vol. 3494, pp. 507-525, Berlin: Springer Verlag,2005.

[12]. Y. A. Zhang and D.G. Feng,

[13]. "Equivalent Generation of the S-box of Rijndael," Chinese J. Computers, Vol. 27, no.12, pp.1593-1600, December 2004.

[14]. W. Millan, "How to Improve the Nonlinearity of Bijective S-boxes," Lecture Notes in Computer Science, Vol. 1438,pp.181 - 192, Berlin: Springer-Verlag, 1998.

[15]. Chen and D. G. Feng, "An Evolutionary Algorithm to Improve the Nonlinearity of Self-inverse S-Boxes," Lecture Notes in Computer Science, vol. 3506, pp.352- 361, Berlin: Springer-Verlag, 2005.

[16]. J. M. Liu, B. D. Wei, and X.G. Cheng,"An AES SBox to Increase Complexity and Cryptographic Analysis, " IEEE Proc. of the 19th InternationalConference on Advanced Information Networking and Applications China, Vol. 1, pp. 724-728, March2005.

TEJAS Thiagarajar College Journal ISSN (Online):2456-4044 June2018, Vol 3(2), PP 62-69