International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 1 Issue 3, November 2013

Study of Various Cryptographic Algorithms

Mini Malhotra[1], Aman Singh[2]

[1, 2]Department of Computer Science, Lovely Professional University, Punjab, India

Abstract: ***Cryptography is used to make secure data transmission over networks. The algorithm selected for cryptography should meet the conditions of authentication, confidentiality, integrity and non-repudiation. Cryptographic algorithms covered in this paper include AES, DES, RSA, Diffie-Hellman, RC4, Blow Fish, El-Gamal, MD5 and Miller-Rabin. Recent years have witnessed the phenomenal growth of RSA and most of the research in cryptography is done in the year 2010. The aim of this paper is to provide a study of the research work done in the cryptography field and various cryptographic algorithms being used, through a literature survey between the years 2008 and 2013. This paper represents the published knowledge from IEEE online database. 270 papers were concerned and after doing content filtering, 50 best suited papers were taken into consideration. Key word indices were used to identify the significant papers. This paper will provide a direction to the naive users and will allow many new future applications.***

Keywords: AES, Blow Fish, Circle Cipher, DES, Diffie Hellman, El Gamal, Euclid, Miller Rabin, MD5, RC4, RSA.

1. Introduction

Cryptography is an ancient art developed in 1900 B.C. [64]. It is a field of computer networks which transforms (encrypts) the information (plain text) into an unreadable form (cipher text). And this cipher text can be decrypted only with the help of a secret key. Cryptography acts as a method of keeping the information secret. Cryptography protects the information by using mathematics in science.

Electronic security is a major issue as various forms of electronic media and internet are becoming more prevalent. Cryptography is used to secure the data and to prevent the data from various attacks. Cryptography is necessary when communicating over any untrusted medium. Authentication, digital signatures, e-commerce are major applications of cryptography.

Broadly, Cryptographic systems provide us three types of cryptographic algorithms namely, Secret Key Cryptography (SKC), Public Key Cryptography (PKC) and Hash Functions. The Secret Key Cryptography (SKC) uses a single (same) key for the process of encryption and decryption.

The most commonly SKC algorithms used now-a-days include:

1.1 Data Encryption Standard (DES)

It was designed in 1970's by IBM and was ratified in 1977 by the National Bureau of Standards (NBS) for commercial use. It is a block cipher that operates on 64-bit blocks employing a 56-bit key and 8 rounds [51]. Although DES has been around long back but no real weakness has been identified. The biggest disadvantage of DES is the 56 bit key size.

1.2 Advanced Encryption Standard (AES)

It was designed by Vincent Rijmen and Joan Daemen and was introduced in 1998. The algorithm can use fickle key length and block length. The key length can include 128, 192, or 256 bits and block length can be of 128, 192, or 256 bits [52].AES is a highly efficient and secure algorithm. The drawback lies in its processing as it requires more processing.

1.3 Rivest Cipher (RC)

Ronald Rivest developed this algorithm and thus, the name of the algorithm was put after Ronald's Rivest name. It provides a series of RC algorithms including RC1, RC2, RC3, RC4, RC5 and RC6 [53].

1.4 Blowfish

It was developed by Bruce Schneie and was first published in the year 1993. This block cipher has 8 rounds, having the block size is of 64 bits and the key length can vary from 32 to 448 bits. Blowfish was proposed as a substitute was DES [54]. This algorithm is significantly faster than other algorithms and the key strength is excellent. Blowfish algorithm is apt only for applications where the key mostly remains the same.

The Public Key Cryptography (PKC) uses one (public) key for encryption and another (private) key for decryption.

The PKC algorithms that are in use today are :

1.4 RSA

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. RSA was named after the mathematicians who invented it. RSA was first published in 1997 [55]. Variable size key and encryption block is used in RSA. Main advantage of RSA algorithm is enhanced security and convenience. Using Public Key Encryption is also an advantage of this algorithm. RSA lacks in encryption speed [56].

1.5 Diffie-Hellman

This algorithm was introduced in1976 by Diffie-Hellman. The Diffie-Hellman algorithm grants two users to establish a shared secret key and to communicate over an insecure communication channel [57]. One way authentication is free with this type of algorithm. The biggest limitation of this kind of algorithm is communication made using this algorithm is itself vulnerable to man in the middle attack [61].

1.6 ElGamal

It was developed in the year 1984 by Taher Elgamal. It is an asymmetric key algorithm and is based on Diffie-Hellman key exchange. ElGamal encryption can be described over any cyclic group G. The security rely upon the issue of a problem in G related to computing discrete logarithms [58]. Fast generalized encryption for long messages and data expansion rate are the two biggest advantages of this algorithm [59]. The chief drawback of ElGamal is the requirement for randomness and its slower speed [60].

Hash Functions, also known as message digest, are the algorithms that do not use any key. Based upon the plain text, a fixed length hash value is generated.

Hash algorithms that are commonly used today include:

Message Digest (MD) algorithms

It produces a hash value of 128 bit from an arbitrary length message. The MD series includes MD2, MD4 and MD5 [61].

1.7 MD5 algorithm

The MD5 algorithm was developed by Rivest in 1991 and is an extension of the MD4 message-digest algorithm and is bit slower than MD4. This algorithm results in a 128 bit hash value. It is mostly used in security based applications. MD5 is more secure than MD4 [62]. It is suitable to use for standard file verifications but it has some flaws and therefore, it is not useful for advanced encryption applications [63].

The remaining part of the paper is organized as follows. Section 2 represents the literature review; Section 3 represents results and discussion. Finally, Section 4 represents a brief conclusion.

2. Literature Review

As stated earlier that the main purpose of this paper is to study the use of cryptographic algorithms in the field of computer networks and to provide navigation to the naive users. Searches are based on IEEE online database. The candidate papers of this survey are filtered using appropriate keywords. The searches were checked and examined several times to find their appropriate areas. The keywords used to search includes cryptography, DES,AES,RSA, Diffie Hellman, Blow Fish, Circle Cipher, RC4, Miller Rabin, MD5 and Euclid. These keywords were suitable to find the appropriate cryptographic algorithms. The search results depict the popularity and applicability of the cryptographic algorithms.

Table 1: Summary of previous findings

Author	*Year of Publication*	*Cryptography Algorithm and other technical details*	*Advantages*	*Limitations*
A.Ramesh, et.al. [45]	2013	DES: 64 bit plain text, 56 bit cipher key for encryption & decryption, 16 rounds. AES : Data block 128bits Rounds : 10,12 or 14 Cipher key size : 128,192 or 256 Key Length : 16,24 or 32 bits Round key : 128bits Blowfish : Key size 32 bits Block size : 64 bits Rounds : 16	Blowfish takes less execution time, produces high throughput, speeds the performance by approximately 4 times than AES and 2 times than DES. AES and DES consume more memory than blowfish algorithm.	
Datta,et.al. [50]	2013	Reversible logic, AES : Key size : 128 bits Rounds : 10	Power synthesis is low.	More reversible gates are required than the traditional CMOS designs.
Isaac,et.al. [46]	2013	Reverse Circle Cipher. Block size : elastic Same key for encryption & decryption.	Key length is not fixed; unlike in AES or DES Key size does not affect the algorithm speed.	Only text based files are dealt. The complete file can be erroneous if any change is

		Cipher, Frequency Distribution.	Whole text file can be considered as a key. Confusion and Diffusion adds security. Cost effective.	done to the ciphertext.
Mandal, et.al. [40]	2013	Merging : RSA algorithm and Diffie-Hellman Algorithm KI, IR, PKC, DDH, PSS	Increased throughput.	More power is consumed.
V. Suresh, C. Saraswathy [42]	2013	Image encryption; image recovery; reversible data hiding RC4 algorithm. Variable length key from 1 to 256 bit Encryption key : 128bit Pseudo-random sequence : 128 bit.	Original images are obtained efficiently.	Lossy compression on integrating image encryption and data hiding.
Chia-Long Wu and Chen-Hao Hu [30]	2012	Methods used : Square-and-Multiply Binary Signed-Digit Recoding Montgomery's Reduction, RSA cryptosystem, exponentiation.	Improved efficiency and decreased computational complexity of modular exponentiation.	The modular exponentiation requires more time if the length of the operators are minimum of 1024 bits.
Dewangan, et.al. [24]	2012	Avalanche Effect, AES : Data block 128bits Rounds : 10,12 or 14 Cipher key size : 128,192 or 256 Key Length : 16,24 or 32 bits Round key : 128bits	Improved security level through high Avalanche Effect.	Cannot carry out experiments on image.
Li Dongjiang [23]	2012	RSA,Miller-Rabin algorithm;Stain algorithm	Prime number generation is improved. Reduced encryption and decryption time.	
Mandal,et.al. [20]	2012	Avalanche Effect, DES : 64 bit plain text, 56 bit cipher key for encryption & decryption, 16 rounds. AES : Data block 128bits Rounds : 10,12 or 14 Cipher key size : 128,192 or 256 Key Length : 16,24 or 32 bits Round key : 128bits	High avalanche effect in AES.	High memory requirement in DES.
Mohammed M. Alani [22]	2012	Cryptanalysis, Algorithm Used : DES Key Size: 56 bits Block size: 64 bits Structure: Balanced Fiestel network Rounds : 16	Improvement in cryptanalysis of DES. Enhanced attack in terms of known-plaintexts needed and the time needed to perform the attack.	The cryptanalytic attack cannot be implemented in hardware.
Dhakar,et.al. [19]	2012	Encryption, Public key, Private key, Security, RSA.	Communication can be done with other parties by requiring only a single pair of keys. MREA is highly secure than RSA.	The original key also cannot decrypt the message if the decryption key corresponding to the encryption key is not known.
Tarik Gad [31]	2012	Stream cipher, linear span, hamming correlation, RC4 : Input : 256 bits Output : 128 or 256 bits Rounds : 256	Enhanced speed of RC4, high interference level.	Sensitive to cryptanalytic attacks.

Xuewen Tan, Yunfei Li [21]	2012	RSA; BS1PRSA,decryption; improved; parallel; multi-core.	Improved decryption performance. BS1PRSA can run side by side on multi-core devices,can be implemented in parallel effectively and efficiently.	
Yu,et.al. [37]	2012	RC4 Based Hash Function; RC4 Stream Cipher; Cryptanalysis; Collision Resistance Input : 256 bits Output : 128 or 256 bits Rounds : 256	RC4-BHF is better than the known hash functions. Collision resistant, preimage resistant, and second preimage resistant are fulfilled by RC4-BHF and is dominated by hash function attacks.	Limited computing and power resources.
Ambedkar,et.al. [15]	2011	Public Key Cryptography; RSA Scheme; Factorization Problem	Easy and scalable algorithm. Reduced prime factorization elapsed time.	Decryption is independent of N.
Dubal,et.al. [32]	2011	ECC, Dual RSA; Message Digest 5; ECDH; ECDSA Encryption algorithm : Dual RSA, Key generation algorithm : ECC, Derived cipher text and digital signature appending algorithm : ECDSA, Decryption algorithm : Dual RSA	Less computation cost and memory requirements, improved cyptosystem strength and security, reduced power consumption and improved bandwidth,	The original message can be hacked from the encrypted message.
Dursun caliskan [6]	2011	Semi-Hybrid Cryptosystem, RSA for Data Transfer, Private exponent : d Public key (n, e) Encryption = m^e (mod n) Decryption = c^d (mod n) Round(s) : 1	Proposed algorithm is more efficient and secure.	Cipher text, encryption and decryption process may be greater than the RSA-DT plain text. Problem may occur in implementation because the number of symbols, ASCII representation is not mentioned in the table.
Jassim Mohammed Ahmed, ZulkarnainMd Ali [18]	2011	Cryptography,RSA algorithm, El-Gamal algorithm.	Efficiency of proposed system is higher.	No significant difference in execution time as compared to the original process.
Moh'd, et.al. [29]	2011	AES,FPGA, Enhanced Security, Input block size : 512 bits Key Size : 512 bits Rounds : 10	Proposed system has high security and increased throughput as compared with the original AES-128 system.	Increased chip area.
Qian Yu and Chang N. Zhang [34]	2011	RC4; RC4 State; Secure Protocol; Secure Data Transmission; Hash Function; Input : 256 bits Output : 128 or 256 bits Rounds : 256	Highly secure, simple and efficient. Various levels of security is supported and is applicable in various network applications. Independent hash function.	Less supply of power, bandwidth is low, memory size is small and restricted calculations.
Rui,et.al. [5]	2011	RSA, kth power residue; k-RSA; Public key : triple (e, n, S ') Private key : triple (d,n, S ')	Increased flexibility of parameters, encryption and decryption speed, improved security. Speed & space is balanced.	Parallel implementation is low.

Shi,et.al. [17]	2011	AES; Avalanche Effect; S Box; Inverse S Box Data block 128bits Rounds : 10,12 or 14 Cipher key size : 128,192 or 256 Key Length : 16,24 or 32 bits Round key : 128bits Structure : Substitution-permutation network	Nonlinearity and the security is provided by the S-box and high avalanche effect.	
Suli Wang, Ganlai Liu [41]	2011	RSA algorithm; file encryption and decryption, Portable components; Private exponent : d Public key (n, e) Encryption = m^e (mod n) Decryption = c^d (mod n) Round(s) : 1	Development aspects are wide, efficient and reusable. Communication is easy with environment demanding high security.	Requires more cost.
Boldyreva,et.al. [16]	2010	Cryptography standards, encryption, provable security, RSA-OAEP	Highly secure. Long messages can be encrypted easily and changes can be implemented easily.	Increased implementation time.
Dr. Mohammed M. Alani [12]	2010	DES, encryption, des-variant, encryption, cryptanalysis DES96 Key Size : 96 bits Block size : 48 bits Structure : Balanced Fiestel network Rounds : 16	Proposed system brute-force attack, differential cryptanalysis, and linear cryptanalysis. Strikes down the weak-keys and complement keys of DES and improved avalanche effect.	
Hongwei Si, Youlin Cai, Zhimei Cheng [8]	2010	Digital signature; Complex Numeric Operation Function; RSA Algorithm Private exponent : d Public key (n, e) Encryption = m^e (mod n) Decryption = c^d (mod n) Round(s) : 1	Effective generation of arbitrary length RSA public and private key pair. Highly secure and requires less computational power.	Lot of time is required.
Jian Xie, Xiaozhong Pan [35]	2010	Improved RC4, confused S-box, Number of secret keys : 2 S-boxes : 2	Proposed system is more secure and fast than RC4 and parallelism is increased.	Many loop holes of the RC4 are not tested.
Jianqin Zhou [14]	2010	RSA, Euclid & Extended Euclid Algorithm.	Improved new system by removing the negative integer operation and reduces complexity of RSA.	
Joao Carlos Leandro da Silva [43]	2010	Factorization, semiprimes, modulus, RSA. Private exponent : d Public key (n, e) Encryption = m^e (mod n) Decryption = c^d (mod n) Round(s) : 1	New method is easy and scalable, supports parallel processing and less memory requirement.	Single system cannot deal with the large number of relations for very large semi primes.

Khan,et.al. [28]	2010	Cryptanalysis, BACO, Heuristic, Fitness Function. 4 Rounded DES Plain text: 64 bits Key size : 56 bits Cipher Text : 64 bits Rounds : 4	Optimum technique for block cipher cryptanalysis.	For obtaining other findings, the search space structure and calculation of the heuristic value may be changed.
Li Ming-xin, Kang Feng [13]	2010	Rich Internet Application, RSA Private exponent : d Public key (n, e) Encryption = m^e (mod n) Decryption = c^d (mod n) Round(s) : 1	Improved system security, reduces system load and server load. Industrial efficiency is good.	Middle man attack cannot be solved.
Li,et.al. [11]	2010	Batch RSA, Modular Exponentiation, Decryption.	Improved decryption.	Performance and security parameters are not optimized.
Li,et.al. [27]	2010	Batch RSA, BMRSA and BEARS.	Improved performance without compromising the security of Batch RSA.	Performance and security parameters are not optimized.
Liu, et.al. [44]	2010	RSA; Multi-Power RSA; acceleration; modular exponentiation; parallel; Round(s) : 1	Improved performance, high security and effective parallel implementation.	Parallel RSA system cannot be implemented in multi-core platform.
Nie, et.al. [26]	2010	Performance Evaluation; DES; Blowfish. DES : 64 bit plain text, 56 bit cipher key for encryption & decryption, 16 rounds Blowfish : Key size 32 bits Block size : 64 bits Rounds : 16	Running performance of Blowfish algorithm is faster than DES.	High energy consumption.
Park, et.al. [49]	2010	Whitebox Cryptography, PCBC mode, AES, DES	Speeds up the performance of the new system.	Look up tables reduces the performance. Key updation on dynamic scenario is comparatively tough than in black box cryptography an intermediate values can be seen by the attacker.
Raman Kumar, Harsh Kumar Verma [3]	2010	Proxy Signature, RSA, Secret Sharing, Non repudiation, Time constraint and known signers.	The proposed system stands efficiently and is secure against various attacks, less time and space complexity, reduced communication overhead. Non repudiation is achieved and proxy signature cannot be imitated.	
Sakshi Dhall, Saibal K. Pal [9]	2010	Block cipher, symmetric key, rounds, computational efficiency, avalanche effect, cryptanalytic attacks. Proposed scheme uses : Block size = 128 bits Key size = 128 bits	High security is ensured by using nonlinear operations and data conditional processing, computational cost is less and is suitable for the encryption of data with high bandwidth.	Differential cryptanalysis. Currently, cannot handle larger key/ block size. S-box is key independent.

		Rounds : 8		
Sami A. Nagar and Saad Alshamma [33]	2010	RSA, RSA-Key Generations Offline, RSA Handshake Database Protocol, secret-key, private-key, public-key.	New generation keys method speeds up the performance of RSA and is secure. Optimum authentication method.	High computational cost.
Shao,et.al. [47]	2010	GPU; style of stream programming; AES algorithm AES : Data block 128bits Rounds : 10,12 or 14 Cipher key size : 128,192 or 256 Key Length : 16,24 or 32 bits Round key : 128bits	Improved computing efficiency encryption efficiency of the proposed algorithm.	The speed of the CPU cipher algorithms is determined by the standards of openssl command.
Tang Songsheng, Ma Xianzhen [48]	2010	Block cipher; DES algorithm; AES algorithm; security DES : 64 bit plain text, 56 bit cipher key for encryption & decryption, 16 rounds AES : Cipher key size : 128,192 or 256 Rounds : 10 Round key : 128bits	AES encryption algorithm is more secure than DES and stands by various differential Cryptanalysis. Space is utilized efficiently by DES encryption algorithm.	Due to short key size of the DES, it can be cracked easily.
Wenxue,et.al. [10]	2010	RSA Algorithm, quantitating security of keys; information security; secure key.	Enhanced RSA security.	Weak keys might be generated.
Yu,et.al. [1]	2010	RC4, Hash Function, Message Authentication, MA C, Ultra-Low Power Devices Input : 256 bits Output : 128 or 256 bits Rounds : 256	Proposed system is simple and exhibits improved efficiency and is immune to all the generic attacks that are possible. Secured hash function.	Requires more cost.
Zhang,et.al. [39]	2010	Crypto Stream Ciphers, RC4, Fault Tolerant, Error Detection Input : 256 bits Output : 128 or 256 bits Rounds : 256	The proposed scheme is flexible and has a general use, can be easily implemented on both hardware and software. Improved fault tolerant Capability and optimum range of the overhead.	At most three arbitrary errors can be identified and removed.
Huayin Ou, Baodian Wei [36]	2009	RSA, CRT-RSA, Multi-factor RSA, Rebalanced RSA-CRT.	Optimized key generation algorithms Scheme II and Scheme IV.	Extra computation cost is incurred on key generation algorithms for Scheme I and

			Highly suitable for applications involving low encryption and decryption costs.	Scheme III.
LIU Chang,YANG Chi [7]	2009	RSA cryptanalysis, LLL algorithm, Lattice basis reduction.	Asymptotic approach.	Propsed method is heuristic. Both of the reduced bases of L that are produced by LLL algorithm in the final step are not linearly related.
Mohammad Jabed Morshed, Tapas Pal [2]	2009	Encryption, Decryption, Symmetric Key Algorithms. New Symmetric Key Algorithm : Encryption : Input: M, a 64 bit value Output: E, a 32 bit value Decryption : Input: E, a 32 bit value Output: M, a 64 bit value	Data is transferred securely through unreliable channel. Reduced overhead as compared to PKC. Encrypted message of fixed size is produced in every case and reduced computational complexity and high confidentiality.	Less secure than public-private key algorithm, high precision is required while performing several floating point operations. Algorithm reliability is proportionate to the precision provided, without the effect any other factor. Round off error can be introduced by increasing the block size. Cannot be easily implemented on hardware.
Abdullah Al Hasib and Abul Ahsan Md. Mahmudul Haque [4]	2008	AES, RSA.	AES encrypts the data blocks faster than RSA Reduced encryption with large keys, resulting is less compromising of the keys. Limited damage if the key is compromised.	Distribution of the secret key is an issue with AES. High computational overhead is involved with RSA.
Aboud,et.al. [38]	2008	RSA Public Encryption Scheme, square matrices, general linear group, digital signature scheme	System is not rigid and is highly efficient and scalable. Range of the key is taken under consideration.	
Ying-yu Cao, Chong Fu [25]	2008	Algorithm used : RSA digital signature	Increased computational speed, security and efficiency.	Large integer library is required and created.

DES: Data encryption standard; AES: Advanced Encryption Standard; CMOS: Complementary metal–oxide–semiconductor; RSA: Ron Rivest, Adi Shamir and Leonard Adleman; KI: Key Insulation; IR: Intrusion Resilience; PKC: Public Key Cryptosystem; DDH: Decision Diffie Hellman; PSS: Probabilistic Signature Scheme; RC4: Rivest Cipher4; MREA: Modified RSA Encryption Algorithm; BS1PRSA: Batch RSA-S1 Multi-Power RSA; ECC: Elliptic Curve Cryptography, ECDH: Elliptic Curve Diffie Hellman; ECDSA: Elliptic Curve Digital Signature Algorithm; FPGA: Field Programmable Gate Arrays; OAEP: Optimal Asymmetric Encryption Padding; BACO: Binary Ant Colony Optimization; BMRSA: Batch Multi-Prime RSA; BEARSA: Batch Encrypt Assistant RSA; PCBC: Propagating Cipher-Block Chaining; GPU: Graphic Processing Unit; CRT: Chinese Remainder Theorem; LLL: Lenstra,Lenstra and Lovasz.

3. Results and Discussions

A review of various cryptographic algorithms is presented in this paper. The accomplishment of cryptography has been explored in almost every field of Computer Networks. Based on this study, RSA is being widely used. IEEE online database search has been done to obtain various papers in the field of cryptography. A thorough literature survey has been done on this. According to all survey results Table I, II and III have been prepared.

Table 2 summarize the figures 1 and 2 and represent the various cryptographic algorithms. The results show that RSA is the most frequently and widely used algorithm. RSA is used 43%, AES 18%, DES 13%, RC4 11%, BlowFish and Diffie-Hellman 3%, Miller-Rabin, El-Gamal, Euclid and MD5 are used 2% and Circle Cipher is used only 1%.

Table 2: Cryptographic algorithms based on published papers

Algorithm	*No of papers*
DES	8
AES	11
Blow Fish	2
Circle Cipher	1
RSA	27
Diffie Hellman	2
RC4	7
Miller Rabin	1
El-Gamal	1
Euclid	1
MD5	1

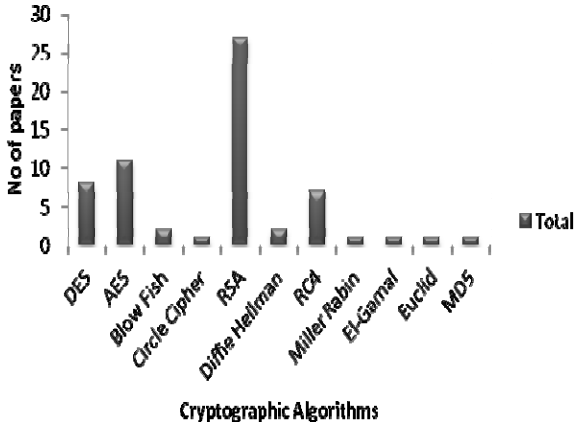

Figure 1: No. of cryptographic algorithms based on the published papers

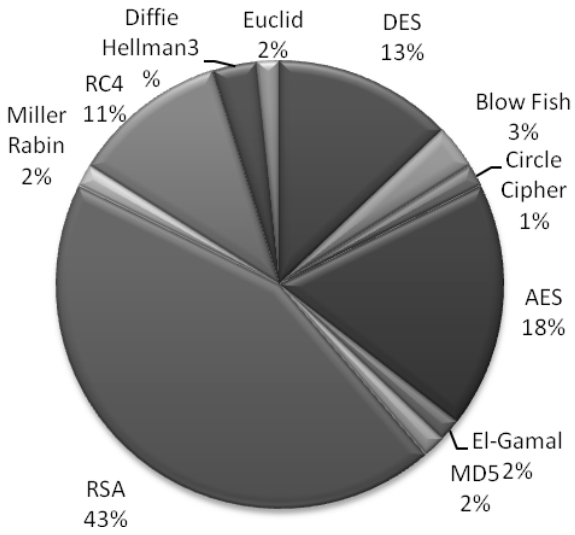

Figure 2: Proportion of cryptographic algorithms based on the published papers

Table 3 summarizes the figures 3 and 4 and depicts the number of papers developed from the year 2008 to 2013. The results show that most of the work is done in the year 2010. 18% of the research work is done in the years 2011 and 2012. In 2010 year, 42 % of the research work is done, which is more than 2 times higher than in the years 2011 and 2012. Research work is done 10% in the year 2013 and only 6% in 2008 and 2009. Figure 3 shows the distribution of the research work done on a yearly basis.

Table 3: Distribution of cryptographic algorithms in last 6 years.

Year	2008	2009	2010	2011	2012	2013	Total
No of papers	3	3	21	9	9	5	50

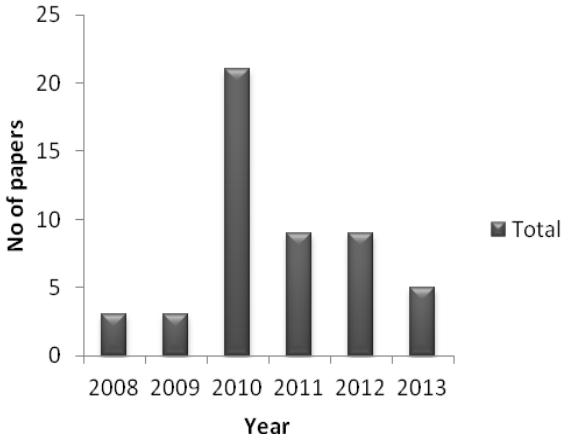

Figure 3: Number of cryptographic algorithms in last 6 years

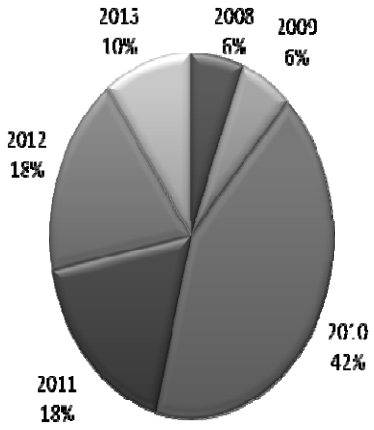

Figure 4: Proportion of cryptographic algorithms in the last 6 years

Table III summarizes figure 5 and depicts the number of single and integrated cryptographic papers on yearly basis.

Out of the total of 50 cryptography research papers, 43 are single and remaining 7 are integrated.

Table 3: The number of single and integrated cryptographic papers on a yearly basis

Year	2008	2009	2010	2011	2012	2013	Total
Single	2	3	19	7	8	4	43
Integrated	1	0	2	2	1	1	7
Total	3	3	21	9	9	5	50

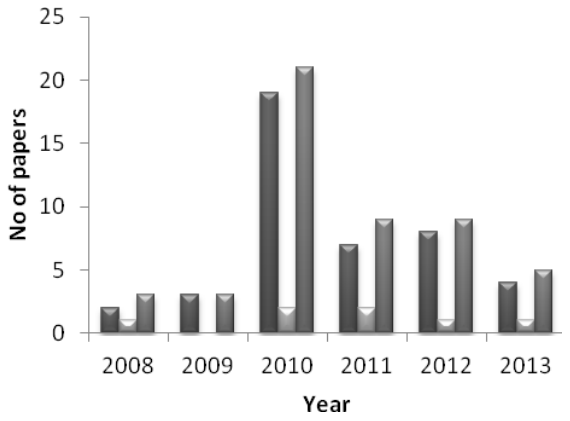

Figure 5: Comparison of the number of single and integrated cryptographic papers between the years 2008-2013

The number of various cryptographic algorithms used is addressed in Fig 1 and 2 on the basis of number of papers. In the graphics, RSA is at the peak and is used most commonly. On contrast, Circle Cipher, Miller Rabin, El-Gamal, Euclid and MD5 are used very less. Figure 3 and 4 depicts the cryptography research paper year wise, starting from 2008 to 2013. According to this survey, only 3 research papers on cryptography are there for the year 2008 and 2009. This number increases to 21 in the year 2010 but falls down rapidly to 9 in 2011 and 2012. In 2013, the number further falls to 5.

A message emerging from this survey is that Circle Cipher, Miller Rabin, El-Gamal, Euclid and MD5 algorithms have not been applied well enough to cryptography yet. Most of the researchers preferred to use RSA, AES and DES. These cryptographic algorithms are very old and this will be the reason of their excellent progress in the field of cryptography. The integrated papers show very weak progress.

Another point which we got from the search result is that Blow Fish, Diffie-Hellman, Circle Cipher, Miller Rabin, El-Gamal, Euclid and MD5 algorithms are not well used. Hybrid algorithms can be developed by combining two or more algorithms. A better understanding of these algorithms is essential for the cryptographic application.

4. Conclusion

This paper represents a review of literature concerned with cryptographic algorithms from the year 2008 to 2013. It is recapitulated that the RSA is used widely. Wide range of research is done in RSA. It used a search of keyword indices and article titles. This paper presents the current scenario and can provide a direction to naive users. According to the search conducted, the research work was at its peak in the year 2010 and then declined in the next 3 successive years.

A number of cryptographic algorithms have been used. As per the literature survey, very less work has been done in BlowFish, Diffie-Hellman, Circle Cipher, Miller Rabin, El-Gamal, Euclid and MD5 algorithms. It is suggested that researchers can direct their research in the above specified algorithms. Future work can be done in BlowFish, Diffie-Hellman, Circle Cipher, Miller Rabin, El-Gamal, Euclid and MD5 algorithms as these algorithms are less explored. The objective of this paper is to provide assistance to the new users in the filed of cryptography.

The main findings of the study are:

- RSA is most widely used algorithm.
- According to the survey, maximum research on cryptography is done in the year 2010.
- There is no remarkable improvement is the progress of integrated papers.
- Finally, through the better understanding of these algorithm's strengths and weaknesses further research can be conducted effectively.

References

[1] Qian Yu ; Zhang, C.N. ; Xun Huang , "An RC4-Based Hash Function for Ultra-Low Power Devices " ,Computer Engineering and Technology (ICCET), Page(s): V1-323 - V1-328, 2010
[2] Chowdhury, M.J.M. ; Pal, T.," A New Symmetric Key Encryption Algorithm based on 2-d Geometry", Electronic Computer Technology,Page(s): 541 – 544, 2009.
[3] Kumar, R. ; Verma, H.K., " An Advanced Secure (t, n) Threshold Proxy Signature Scheme Based on RSA Cryptosystem for Known Signers ", Advance Computing Conference (IACC) ,Page(s): 293 – 298, 2010.
[4] AlHasib, A. ; Haque, A.A.M.M.,"A Comparative Study of the Performance andSecurity Issues of AES and RSA Cryptography",Convergence and Hybrid Information Technology, 2008 , Page(s): 505 – 510, 2008.
[5] Wang Rui ; Chen Ju ; Duan Guangwen, "A k-RSA Algorithm ",Communication Software and Networks (ICCSN) , Page(s): 21 – 24, 2011.
[6] Caliskan,D. ,"An application of RSA in data transfer",Application of Information and

Communication Technologies (AICT), Page(s): 1 – 4, 2011 .
[7] LiuChang ; YangChi ,"Factoring RSA modulo N with high bits of p known revisited", IT in Medicine & Education, Page(s): 495 – 500,2009.
[8] HongweiSi ; YoulinCai ; ZhimeiCheng ,"An Improved RSA Signature Algorithm Based onComplex Numeric Operation Function",Challenges in Environmental Science and Computer Engineering (CESCE), Page(s): 397 – 400, 2010 .
[9] Dhall,S. ; Pal,S.K.,"Design of a New Block Cipher Based on ConditionalEncryption",Information Technology: New Generations (ITNG), Page(s): 714 – 718, 2010.
[10] Wenxue Tan ; Wang Xiping ; Jinju Xi ; Meisen Pan , "A mechanism of quantitating the security strength ofRSA key", Electronic Commerce and Security (ISECS), Page(s): 357 – 361, 2010.
[11] YunfeiLi ; QingLiu ; TongLi,"Design and implementation of two improved BatchRSA algorithms", Computer Science and Information Technology (ICCSIT) , Page(s): 156 – 160, 2010.
[12] Alani, M.M., " DES96 - Improved DES Security", Systems Signals and Devices (SSD), Page(s): 1 – 4, 2010.
[13] Li Ming-xin ; Kang Feng ," An improved sign-in scheme based on RSA cryptosystem",Computer Application and System Modeling (ICCASM), Page(s): V6-35 - V6-37, 2010.
[14] Jianqin Zhou ; Jun Hu ; Ping Chen , "Extended Euclid algorithm and its application in RSA", Information Science and Engineering (ICISE), Page(s): 2079 – 2081, 2010.
[15] Ambedkar, B.R. ; Gupta, A. ; Gautam, P. ; Bedi, S.S. , "An Efficient Method to Factorize the RSA Public KeyEncryption",Communication Systems and Network Technologies (CSNT), Page(s): 108 – 111, 2011.
[16] Boldyreva, A. ; Imai, H. ; Kobara, K. , "How to Strengthen the Security of RSA-OAEP",Information Theory , Page(s): 5876 – 5886, 2010.
[17] Hui Shi ; Yuanqing Deng ; Yu Guan, "Analysis of the avalanche effect of the AES S box",Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC) , Page(s): 5425 – 5428, , 2011.
[18] Ahmed, J.M. ; Ali, Z.M. , "The Enhancement of Computation Technique By Combining RSA and El-Gamal Cryptosystems", Electrical Engineering and Informatics (ICEEI) , Page(s): 1 – 5, , 2011.
[19] Dhakar, R.S. ; Gupta, A.K. ; Sharma, P., "Modified RSA Encryption Algorithm (MREA)", Advanced Computing & Communication Technologies (ACCT), Page(s): 426 – 429,2012.
[20] Mandal, A.K. ; Parakash, C. ; Tiwari, A., "Performance Evaluation of Cryptographic Algorithms: DES and AES", Electrical, Electronics and Computer Science (SCEECS), Page(s): 1 – 5, 2012 .
[21] Xuewen Tan ; Yunfei Li, "Parallel Analysis of an Improved RSA Algorithm", Computer Science and Electronics Engineering (ICCSEE), Page(s): 318 – 320, 2012.
[22] Alani, M.M., " Neuro-Cryptanalysis of DES ", Internet Security (WorldCIS),Page(s): 23 – 27, 2012.
[23] Li Dongjiang ; Wang Yandan ; Chen Hong, "The research on key generation in RSA public- key cryptosystem", Page(s): 578 – 580, 2012.
[24] Dewangan, C.P. ; Agrawal, S. ; Mandal, A.K. ; Tiwari, A. , "Study of avalanche effect in AES using binary codes", Advanced Communication Control and Computing Technologies (ICACCCT), 2012 IEEE International Conference, Page(s): 183 – 187, 2012.
[25] Chong Fu ; Zhi-liang Zhu, "An Efficient Implementation of RSA Digital SignatureAlgorithm",Wireless Communications, Networking and Mobile Computing, Page(s): 1 – 4,2008.
[26] Tingyuan Nie ; Chuanwang Song ; Xulong Zhi , "Performance Evaluation of DES and Blowfish Algorithms", Biomedical Engineering and Computer Science (ICBECS), Page(s): 1 – 4, 2010.
[27] Yunfei Li ; Qing Liu ; Tong Li ; Wenming Xiao, "Two efficient methods to speed up the Batch RSAdecryption", Advanced Computational Intelligence (IWACI), Page(s): 469 – 473, 2010 .
[28] Khan, S. ; Shahzad, W. ; Khan, F.A., "Cryptanalysis of Four-Rounded DES using Ant Colony Optimization",Information Science and Applications (ICISA) ,Page(s): 1 – 7, 2010.
[29] Moh'd, A. ; Jararweh, Y. ; Tawalbeh, L. , "AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evaluation", Information Assurance and Security (IAS), Page(s): 292 – 297, 2011.
[30] ChiaLongWu ; ChenHaoHu ,"Computational Complexity Theoretical Analyses onCryptographic Algorithms for Computer SecurityApplication", Innovations in Bio-Inspired Computing and Applications(IBICA), Page(s): 307 - 311, ,2012.
[31] Gad, T. ; El-Soudani, M. ; Youssef, A. ; Khalil, A., "Study of RC4 Over non-2m domain ", Computer Engineering Conference (ICENCO), Page(s): 7 – 12, 2012 .
[32] Dubai, M.J. ; Mahesh, T.R. ; Ghosh, P.A. , "Design of new security algorithm: Using hybridCryptography architecture",Electronics Computer Technology (ICECT), Page(s): 99 – 101, 2011.
[33] Nagar, S.A. ; Alshamma, S. , "High speed implementation of RSA algorithm withmodified keys exchange",Sciences of Electronics, Technologies of Information and Telecommunications (SETIT) , Page(s): 639 – 642 , 2010.
[34] Qian Yu ; Zhang, C.N., " RC4 State and Its Applications " ,Privacy, Security and Trust (PST), Page(s): 264 – 269, 2011.
[35] Jian Xie, Xiaozhong Pan, "An Improved RC4 Stream Cipher", Computer Application and System Modeling (ICCASM), Page(s): V7-156 - V7-159, 2010.

[36] Huayin Ou, Baodian Wei, "Multi-factor Rebalanced RSA-CRT Encryption Schemes", Biomedical Engineering and Informatics , Page(s): 1 – 5, 2009.
[37] Qian Yu ; Zhang, C.N. ; Orumiehchiha, M.A. ; Hua Li, "RC4-BHF An Improved RC4-Based Hash Function" Computer and Information Technology (CIT) , Page(s): 322 - 326, 2012.
[38] Aboud, S.J. ; Al-Fayoumi, M.A. ; Al-Fayoumi, M. ; Jabbar, H. , "An Efficient RSA Public Key Encryption Scheme", Information Technology: New Generations, Page(s): 127 – 130, 2008.
[39] Zhang, C.N. ; Qian Yu ; Xiao Wei Liu , "Multiple Dimensional Fault Tolerant Schemes for Crypto Stream Ciphers", Multimedia Information Networking and Security (MINES),Page(s): 406 – 412, 2010 .
[40] Mandal, B.K. ; Bhattacharyya, D. ; Bandyopadhyay, S.K. , "Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm ", Communication Systems and Network Technologies (CSNT), Page(s): 453 – 461, 2013.
[41] Wang, Suli ; Liu, Ganlai , "File encryption and decryption system based on RSA algorithm", Computational and Information Sciences (ICCIS), Page(s): 797 – 800, 2011.
[42] Suresh, V. ; Saraswathy, C. ,"Separable Reversible Data Hiding Using Rc4 Algorithm", Pattern Recognition, Informatics and Mobile Engineering (PRIME), Page(s): 164 – 168,2013.
[43] da Silva, J.C.L. ,"Factoring Semiprimes and Possible Implications for RSA", Electrical and Electronics Engineers in Israel (IEEEI), Page(s): 000182 – 000183, 2010.
[44] Qing Liu, Yunfei Li, Lin Hao, "On the Design and Implementation of an Efficient RSA Variant", Advanced Computer Theory and Engineering (ICACTE), Page(s): V3-533 - V3-536, 2010.
[45] Ramesh, A. ; Suruliandi, A. , "Performance Analysis of Encryption Algorithms for Information Security, Circuits, Power and Computing Technologies (ICCPCT), Page(s): 840 – 844, 2013.
[46] Isaac, E.R.H.P. ; Isaac, J.H.R. ; Visumathi, J. , "Reverse Circle Cipher for Personal and Network Security", Information Communication and Embedded Systems (ICICES), Page(s): 346 – 351,2013 .
[47] Fei Shao, Zinan Chang, Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU", Communication Software and Networks, Page(s): 588 – 590, 2010.
[48] Tang Songsheng, Ma Xianzhen,"Research of typical block cipher algorithm", Computer, Mechatronics, Control and Electronic Engineering (CMCE), Page(s): 319 – 321, 2010.
[49] Jong-Yeon Park, Okyeon Yi, Ji-Sun Choi, "Methods for Practical Whitebox Cryptography", Information and Communication Technology Convergence (ICTC) , Page(s): 474 – 479, 2010.
[50] Datta, K. ; Shrivastav, V. ; Sengupta, I. ; Rahaman, H. , "Reversible Logic Implementation of AES Algorithm", Design & Technology of Integrated Systems in Nanoscale Era (DTIS), Page(s): 140 – 144, 2013.
[51] http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard
[52] http://www.truecrypt.org/docs/aes
[53] http://en.citizendium.org/wiki/Rivest_ciphers
[54] https://www.schneier.com/blowfish.html
[55] http://searchsecurity.techtarget.com/definition/RSA
[56] http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/advantages-and-disadvantages.htm
[57] http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange
[58] http://www.princeton.edu/~achaney/tmve/wiki100k/docs/ElGamal_encryption.html
[59] http://markus-jakobsson.com/papers/jakobsson-asiacrypt00.pdf
[60] http://x5.net/faqs/crypto/q29.html
[61] http://technet.microsoft.com/en-us/library/cc962033.aspx
[62] http://www.accuhash.com/what-is-md5.html
[63] http://pcsupport.about.com/od/termsm/g/md5.htm
[64] http://searchsoftwarequality.techtarget.com/definition/cryptography

Author Profile

Mini Malhotra received the degree of BCA from Uttar Pradesh Technical University in 2010. Presently, pursuing MCA-M.Tech (CSE) from Lovely Professional University, Punjab, India.

Aman Singh, Assistant Professor, Computer Science and Engineering department, Lovely Professional University, Punjab, India.