Review of Various Algorithms Used in Hybrid Cryptography

[1]Veerpal Kaur, [2]Aman Singh

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

[2]Assistant Professor, Department of Computer Science Engineering, Lovely Professional University
Phagwara, Punjab, India

Abstract - Cryptography is a technique used today for hiding any confidential information from the attack of an intruder. The study of hybrid cryptography going to present is based on the study of hybridization. Study has been performed from 1993 to 2013. All the concepts related to hybrid cryptography have been analyzed and reached at the conclusion that the use of RSA is quite expanding. Near about 200 papers have been searched related to the problem and 55 have been considered in this review based on filtering. Tabular survey has been provided for ease of use. Major scope of work has been done using RSA. Diffie-Hellman is a today's choice for algorithm implementation in any network. Another point of view is that very less use of DES is there due to some of its limitations such as less Avalanche effect. RSA, AES, SHA-1, MD5 are some of the most widely used algorithms for hybrid cryptography. The main aim of this review paper is to provide more and more information to the naïve researchers. Other objectives of this review paper are to emphasize on better performance, maximum speed of an algorithm, checking effectiveness, its efficiency and comparison with other related works.

Keywords- *RSA, ElGamal, hybrid of various algorithms, hybrid cryptography*

1. Introduction

Cryptography enables the user to transmit confidential information across any insecure network so that it cannot be used by an intruder. Cryptography is the process that involves encryption and decryption of text using various mechanisms or algorithms. A cryptographic algorithm is a mathematical function that can be used in the process of encryption and decryption. Encryption is the process of converting the plain text into an unreadable form called a cipher text. This unreadable form cannot be easily understood by an intruder and sent across the insecure media. Decryption is the process of converting this unreadable form back into its original form, so that it can be easily understood by the intended recipient. Many algorithms exist for encryption that can be categorized into symmetric and asymmetric encryption. In symmetric-key cryptography, also called conventional cryptography or secret-key encryption, one key is used both for encryption and decryption. Examples include DES and AES. But symmetric-key cryptography has some limitations. One major limitation is the key distribution problem. If in case key, while sending through the channel, get compromised, whole communication will get vulnerable to attacks.

1.1 DES (Data Encryption Standard)

The Data Encryption Standard is one of the first commercially developed ciphers. DES is the result of efforts done by IBM (International Business Machines) corporation, NBS (National Bureau of Standards) and NSA (National Security Agency). DES is a block cipher that encrypts 64-bit data blocks and encryption of the data is performed using a 56-bit secret key [4]. DES consists of sixteen rounds and two permutation layers. DES uses a shared key both to encrypt and decrypt the message. The decryption process is the reverse of encryption process. DES possesses strong Avalanche effect and is flexible as it works in CBC, ECB, CFB and OFB modes. DES easily falls pray to Brute Force attack and relatively slow in software.

1.2 AES (ADVANCED ENCRYPTION STANDARD)

The algorithm was invented by Joan Daemen and Vincent Rijmen. AES can process 128 bit data block and uses key lengths of 128, 192, or 256 bits. For the key length of 128,192 and 256 bits, AES may be referred to as AES-128, AES-192 and AES-256 respectively. Unlike DES, AES is not a fiestel structure. Number of rounds in AES depends on key length i.e. for a key length of 128, number of rounds is 10 and similarly for 192 and 256 bit keys, it is 12 and 14 respectively. AES provides resistance against all known attacks, simple in design and good speed of computation.

The problems of key distribution are solved by public key cryptography. Some examples of public-key cryptosystems are: Elgamal, RSA, Diffie-Hellman and DSA.

1.3 RSA (Rivest, Shamir and Adleman)

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. It widely used in electronic commerce protocols, and is believed that its security depends on the difficulty of decomposition of large numbers. RSA is secure because it is able to resist concerted attack.

1.4 Diffie-Hellman

Whitfield Diffie and Martin Hellman discovered Diffie-Hellman (DH) algorithm in 1976 was the first public key algorithm ever invented. Diffie–Hellman establishes a shared secret key that can be used for secret communications by exchanging data over a public network. Diffie–Hellman algorithm does not need any known key before communication begins and Discrete Logarithm Problem makes it extremely difficult to crack. Diffie–Hellman algorithm easily falls pray to man-in-the-middle attack.

1.5 Elgamal Algorithm

El Gamal algorithm was invented by Taher El-Gamal which is based on Discrete Logarithm Problem and Diffie-Hellman key exchange [19]. Elgamal can be used for encryption as well as digital signature. Each time when the same plaintext is encrypted, it gives a different ciphertext. Elgamal has the disadvantage of having ciphertext twice the size of the plaintext.

1.6 DSA (Data Signature Algorithm)

Data Signature Algorithm as an approved signature scheme was invented by David Kravitz. DSA is a variant of the ElGamal and Schnorr algorithms. Digital Signature Standard (DSS) used DSA proposed by National Institute of Standards and Technology (NIST) in 1991. Security of DSA is based on the difficulty to solve discrete logarithms. DSA has been accepted widely. DSA is more efficient and faster than RSA.

was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key encryption. It is still

In practice, the symmetric key algorithms and public key cryptography algorithms are generally combined together. Combining the features of two algorithms for the sake of better efficiency and performance and for combating the problems with the already existing algorithms, the process occurs is known as **Hybrid cryptography**. Hybridization of algorithms is a useful scheme that provides solutions to some major problems in the communication networks or any other means. Numerous ways have been made available by the study to carry hybridization. Deploying the positive points of an algorithm such as RSA into other less efficient algorithms will result in new hybrid cryptographic algorithm.

For this literature survey, the period of interest begins in the year 1993. For the period from 1993 to 2013, 500 IEEE papers were found. Topic filtering reduced this number to 49 which were related to the keyword, ‘‘Hybrid Cryptography’’. Some papers are also included that are not related to hybrid cryptography but those papers are very beneficial for the researchers to view which algorithm in comparison to others can be used in their studies. The remaining part of the paper is organized as follows. Section II provides the details of the literature survey been performed, results and discussions are available in Section III and Section IV contains the conclusion of the paper.

2. Literature Review

We have already mentioned that the aim of this paper is to provide the survey for various algorithms used for hybrid cryptography and papers available that used the hybrid cryptography. All the search is purely based on IEEE explore using appropriate keywords. After finding near about 500 papers related to the survey, topic filtering conducted, that results in a bundle of 55 papers that have been used in this review paper.

Table 1: Review of literature between 1993-2013

Author	Year of publication	Cryptography algorithm and other technical details	Advantages	Limitations
Huang et. al. [3]	2013	Se4GE	New scheme presented provides secure data transmission, privacy preservation and reduced processing time for key exchange. It also enhances key exchange security and provided a new method for message digest calculation.	

Mohanty et. al. [1]	2013	Discrete Logarithm, CDH	In the presented scheme, signer's anonymity is fully preserved, secure in case of any kind of signature leakage and no member of the group is able to produce a valid signature on behalf of one another. Number of group members has no role to play in the length of group signature and confidential documents will be sent effectively.	
WANG et. al. [2]	2013	RSA , Euclidean and its extension theorem, square multiply algorithm	Key transmission problem is solved and MATLAB implementation results show simulation of RSA to take 0.140176s.	
Bansod et. al. [13]	2012	DES, RSA	Two levels of security i.e. hybrid cryptography and stegnography are combined together, modified BPCS approach is used to decide embedding byte positions, so useless for any intruder to make attempts to steal data and degradation in image quality will not get reflected to normal human eye after the cipher text is embedded.	
Chitra and Sheeba[11]	2012	Asymmetric RSA, symmetric SEA, Montgomery multiplication algorithm	Maximum digital security is provided and memory and power consumption is quite low.	
Dhakar et. al. [9]	2012	RSA	As compared to RSA, MREA is more secure in combating mathematical and brute force attacks, time required to break MREA is more than RSA as it works on *dual* modulus and used for both signing and encryption.	The length of private key increases because of DUAL modulus used.
Gutub and Khan [15]	2012	DES(56 bit key) AES(128 bit key) RSA	Before key exchange, key encryption is performed with RSA, Data encryption with DES and AES.	

			Faster in execution, the user is free to use a number of encryption keys without any worry for their transfer and provides maximum security.	
Kumar et. al. [4]	2012	DES (56 bit key) AES (128,192 or 256 bit key)	AES and DES performance evaluation results that DES is most widely used in financial applications; memory requirement for DES is high. Avalanche effect for AES is high. AES is very effective for anything that involves monetary transactions and an ideal method for encryption in chat-channels.	
Kumar et. al. [6]	2012	DES	Rather than providing plaintext and encryption key directly to DES algorithm, various binary codes are used for mapping input plaintext and encryption key; provide measurable increase in Avalanche effect of DES.	
Markku-Juhani O. Saarinen [12]	2012	Rabin public key encryption algorithm, Shamir's randomized multiplication technique	Bluejay is used for achieving sensor data acquisition, intended for RFID authentication, and many secure logging applications, working space required is less.	
Nagar et.al. [10]	2012	RSA-Key Generations Offline	RSA-key generations offline speedup the RSA algorithm, and generated keys get saved in tables within the database, anyone who knows the exchanged values between gateways will face difficulty due to new method of keys exchange proposed in the paper.	
Rasmi P S et. al. [8]	2012	RSA, Discrete logarithms, Factoring	Design of a new paired cipher text public key system is provided that incorporates two mathematical hard problems for making algorithm more secure that	

			are discrete logarithm and factoring.	
Shilpi Gupta and Jaya Sharma [14]	2012	RSA and Diffie Hellman	Provides communication security, avoid attacks in the network and confidential messages and files are easily sent and received by a user.	Algorithm works only for encryption and decryption. No revised time complexity.
Zhang and Jin[5]	2012	DES (Triple DES with 168 bit key) with RSA and SHA-1 with DSS (digital signature standard)	Wide range of practicality for the system, triple DES used for data encryption and RSA for key management and SHA-1 for validating data integrity.	
Zodpe et.al. [7]	2012	DES (56 bit), FPGA	Implementation of iterative and loop unrolled DES architecture is presented to make cryptanalysis faster and better; results of experiments provided that for four instances of key search in single FPGA, iterative architecture requires less area and searching entire solution space requires less time.	
Ahmed and Ali [19]	2011	RSA, Elgamal	Provides solutions for two famous hard problems and increases the computation speed for asymmetric cryptosystem.	Public key's execution time and its complexity are trade-off problem and the execution time of the proposed method doesn't differ significantly as compared to original methods.
Dubal *et. al.* [16]	2011	ECC, dual RSA, Hash algorithms	Authentication, integrity and confidentiality are provided by single algorithm, provides lower power consumption with high speed of efficient computation and greater storage efficiency.	
Jailin *et. al.* [18]	2011	public key cryptography, ECC,	Significant increase in computational speed as	

		AES, MD5	well as security, reduced memory usage and lifetime of nodes has also been increased using aggregation.	
L.Smolinski [21]	2011	DES	A modification scheme is provided for the cryptographic hardware accelerators that allow adding new functionality that further allows dynamic changes in the number of rounds and required registers.	
Lin *et. al.* [24]	2011	Backward hashing, Filtering, Virus scanning	Virus scanning in open-source ClamAV by partitioning the signatures into long and short ones and WM and traditional AC algorithm benefits can be efficiently combined using this hybrid approach.	Some of the techniques such as packing, polymorphism, and metamorphism escape detection of anti-virus. So more processing is required to handle such techniques and such a processing will be time-consuming and provides an overhead.
Mukherjee *et. al.* [20]	2011	WEP, RSA	Proposed scheme makes WEP more secure as compared to existing WEP key process and tags read rate of RIFD system is much faster than the barcode system.	An overhead is there to the existing protocols and overall WEP communication process slows down due to the overhead.
Sharma *et. al.* [22]	2011	Elgamal cryptosystem	Encryptions of long messages get enhanced, secured against the brute force attack, low modulus, mathematical and known-plaintext attack.	Because of the use of one-way function, MECA cannot be used for authentication; it slows down the execution process of Elgamal cryptosystem.

Thomas and Chaudhari [17]	2011	NP complete, RSA, public key	Enhances the security bleach of existing hybrid cryptosystem, provides illustration for the threats existing on the available cryptosystem and also provides information about 3SAT such as the attacks that can happen by the use of polynomial solvable algorithm.	
Wang and Zhang[23]	2011	RSA cryptography	Transformation of personal information from plaintext to cipher text can be done and clients' privacy is preserved.	
BAI *et. al.* [31]	2010	conic curve, digital signature, Elgamal, elliptic curve	Provides advantages of conic curve simple operations as well as improved security, expected functionality is being achieved, effective in improving system security and its operating efficiency and easier to implement.	
Jun *et. al.* [33]	2010	ElGamal, Digital Signature	Problem in Elgamal digital signature algorithm is provided with a solution that random numbers can be repeatedly used, overcomes any attack on random number and security of the algorithm is checked.	
Junru and Ding Yi [27]	2010	BLS signature scheme	Provides an efficient signcryption scheme having short length of ciphertext, high data rate as well as communication performance.	
Li *et. al.* [29]	2010	BEARSA and BEAMRSA	Speed up the decryption process of Batch RSA.	
Li *et. al.* [25]	2010	RSA	Provides improved performance of signature generation and decryption, easy implementation, high speedup as well as security.	
Park *et. al.* [28]	2010	White box cryptography	With the use of dynamic and static tables, a technique of key updation	Practical use of white box cryptography

			is provided along with the solutions for performance slowdown and static table synchronization problems.	results in performance degradation because of the use of too many lookup tables.
Ren and Miao[32]	2010	DES and RSA algorithms	More secure data transmission, easier to achieve and provides safety in data transmission between Bluetooth devices.	Overcome only few shortcomings of E0 stream cipher used in Bluetooth communication.
Shao *et. al.* [26]	2010	AES	Improved the performance of AES algorithm, increased the efficiency of encryption and provides faster implementations.	
Songsheng and Xianzhen [30]	2010	DES(56 bit) and AES(128 bit)	Study provides the results that the security of AES encryption algorithm is higher as compared to DES. Since DES faced problems of been cracked, with some improvements, DES algorithm still has great scope of use.	
WU and MING [34]	2010	IDEA and RSA	High efficiency of IDEA algorithm and effective key management features of RSA are combined and effective working of encrypted database system has shown.	
Xiang Li et. al.[54]	2010	Improved AES and ECC	Along with the advantages of high operatability, high security, wider usability, high computational speed, greater performance, increased data encryption and decryption speeds, the proposed scheme also provides a solution for the problem of key distribution and authentication.	
Sarkar *et. al.* [37]	2009	VSS Scheme, Asmuth-Bloom Secret Sharing Scheme	For participating nodes, it is a secure technique for generating consistent shares of the secret and combining shares in reconstruction phase.	In case of regular RSA-TC when key sizes get doubled, the time required

				for signature generation and signature verification increases. RSA-TC scheme is of not much use in MANETs.
Sattar J Aboud [36]	2009	RSA	Provides an algorithm for attack on RSA scheme which is more efficient, faster and consumes less time as compared to the existing one.	
Wang and Hu[35]	2009	DPSK, SPDK, AES, DES, RSA	Study resulted that AES is about several hundred times faster than RSA, and about three times faster than triple-DES and big size plaintext is a computational overhead in RSA. The increasing key length in case of RSA and triple-DES when projected against key length used in AES, results show significant increase in AVT factor.	
Aboud *et. al.* [40]	2008	RSA	Presented RSA scheme implemented in the linear group is scalable, efficient and dynamic.	
Hasib and Haque [42]	2008	AES (128, 192 or 256 bits keys), RSA cryptography	Besides analyzing different kinds of attacks on AES and RSA for security purpose, a solution for the limitations of AES and RSA is provided.	
Razi and Quamar [38]	2008	Seniority-Based trust model, PGP	Having benefits of ease of deployment, more security, reliability and efficiency, the presented scheme provides broad area of application.	Problem in certificate revocation for the presented scheme.
Vishnu and Tiong [41]	2008	AES and DES	Provides the weaknesses of AES and ways to minimize these.	Testing results of ECB mode of the presented algorithm

			Tests were conducted to access the performance of AES and hybrid AES-DES had persistent PNSR readings.	shows that when implemented into Joint Video Streaming process, its processing time is high, which is an overhead.
Wang *et. al.* [39]	2008	public-key cryptography; RSA, entity authentication scheme, one-way trap-door function	Proposed one-way trap-door function is quite feasible, efficient and more secure. One-way function is helpful in construction of public key encryption, key agreement and digital signature algorithms along with entity authentication.	
Sun *et. al.* [43]	2007	Dual RSA	Dual RSA can be used in blind signatures as well as for authentication purposes, reduced memory requirements and good security.	High time-complexity due to the increment in the size of unsafe exponents in Dual RSA. Dual RSA is useful only when there are reduced memory requirements.
CHU and SIMA [46]	2006	NOIS processor, Montgomery Modular Exponentiation and Multiplication.	New custom instruction is provided for incorporating the MME unit into NOIS processor and provides a speedup range of 5x to probably 20x.	
Jung and Rao [45]	2006	XTR and Elgamal	With reduced key length, easy calculation and execution, suggested scheme fasten the computational speed.	For each session, user has to select a different random number through which protocol encrypts and transmits a message.
Mathew and Jacob [47]	2006	MAJE4 (128-bit key or a 256-bit key), RSA	Along with the benefits to preserve confidentiality and authentication, and	

			reduced memory requirement, the proposed scheme has good speed of encryption and decryption.	
Cilardo *et. al.* [48]	2005	radix-2 Montgomery technique, radix-4 MSD-first approach	The architecture structure provided is bit-sliced, highly regular, scalable and quite modular. Results for a 1024-bit modular exponentiation, implementation takes just 27.36 ms.	Comparison done between base paper i.e. Montgomery Modular Exponentiation reconfigurable hardware and the presented hybrid but with different hardware used.
Farouk *et. al.* [44]	2005	Stegnography, FPGA	Observes the drawbacks of existing micro architecture and provides an improved micro architecture that overcomes those drawbacks. Proposed micro architecture has 106 Mbps of throughput and it is quite sufficient for most high speed networks. Allows the user to choose stegnography or encryption without any change in the hardware, hence bridges the gap between stegnography and cryptography.	Variations in various security levels are excluded.
Khan and Singh [49]	2005	IDEA-RSA algorithm and RSA digital signature algorithm.	The proposed scheme provides hybrid encryption method for security and digital signatures for authenticity. A speed of 2.8 Mbps is provided by the scheme with more security.	
Eberle *et. al.* **[51]**	2004	FPGA technology	To support the emerging elliptic curve cryptosystem in addition to the traditional RSA cryptosystem, a dual-field multiplier is needed that supports operations for both fields $GF(p)$ and fields $GF(2m)$.	

			Proposed technique shows such support by providing a standard integer multiplier simply by rearranging the carry-save adder tree. The resulting modifications do not add any gate delay to the critical path of the multiplier and only require a modest amount of additional chip resources. The performance analysis shows a clear performance advantage for ECC over RSA.	
Sami Harari [50]	2004	RSA and TTP	"Man-in-the-middle" attack is resisted, almost impossible to attack and guarantees the identity of the user.	
Mohammed *et. al.* [52]	2000	Elgamal signatures, RSA blinding	Proposed scheme is used to generate blinded as well as normal Elgamal digital signatures with advantage of being efficient, faster, and simpler than RSA and offers privacy enhancement.	
El-Hadidi *et. al.* [53]	1995	DES, Diffie-Hellman, RSA	It enhances the system security in Ethernet LAN.	It is believed that by using hardware implementation for certain parts of the proposed encryption scheme, a much faster operation could be obtained.
Shand *et. al.* [55]	1993	RSA, Chinese remainders, Modular exponentiation, Hensel's odd division, Modular product.	Techniques that can be used in the design of fast hardware for RSA cryptography are analyzed. RSA having those techniques delivers a decryption rate about 600 Kb/s for 512 b keys and 165 Kb/s for 1 Kb keys and is quite faster than any of the previous implementations.	

Se4GE: Security system with RSA and Diffie-Hellman algorithms for a 4G environment; CDH: Computational Diffie-Helmann; RSA: Rivest, Shamir, Adleman; DES: Data Encryption Standard; SEA: Scalable Encryption Algorithm; BPCS: Bit Plane Complexity Segmentation; MREA: Modified RSA Encryption Algorithm; AES: Advanced Encryption Standard; SHA: Secure Hash Algorithm; WEP: Wired Equivalent Privacy; RFID: Radio Frequency Identification; MECA: Modified Elgamal Cryptographic Algorithm; NP: Non-deterministic Polynomial complete; BLS: Boneh, Lynn and Shacham signature; BEARSA: Batch Encrypt Assistant RSA; BEAMRSA: Batch Encrypt Assistant Multi-Prime RSA; GPU: Graphic Processing Unit; IDEA: International Data Encryption Algorithm; ECC: Elliptic Curve Cryptography; VSS: Verifiable Secret Sharing Scheme; DPSK: Different Plaintexts in Same Key; SPDK: Same Plaintext in Different Keys; AVT: Average Time-consuming; PGP: Pretty Good Privacy; Electronic Codebook: ECB mode; PNSR: Peak Signal to Noise Ratio; MSD: Most Significant Digit; FPGA: Field Programmable Gate Array; MD5: Message Digest; LAN: Local Area Network; TTP: Trusted Third Party

3. Results and Discussion

An overview of different cryptographic algorithms is presented in this paper. The IEEE database search has been done to obtain the papers dealing with hybrid cryptography. The search is mostly done on the basis of IEEE papers survey. According to all search results Tables 2, 3 and 4 have been prepared. Table 2 summarizes the Figs. 1 and 2, and gives the number of papers available for study on a yearly basis. Fig.-1 shows the percentage of papers used in the study from a particular year. By analyzing Fig.-1, it can be noticed that more efforts have been put to improve the performance of different algorithms during the years 2011-2013 i.e. 43%. Fig.-2 depicts the comparison of the number of papers published between the years 1993-2013 that has been used in this review paper. It can be clearly visible that the use of hybrid cryptography is going on increasing day by day.

Table 2: Number of papers available

Year	Papers
1993-95	2
1996-98	0
1999-2001	1
2002-04	2
2005-07	7
2008-10	19
2011-13	24
Total	55

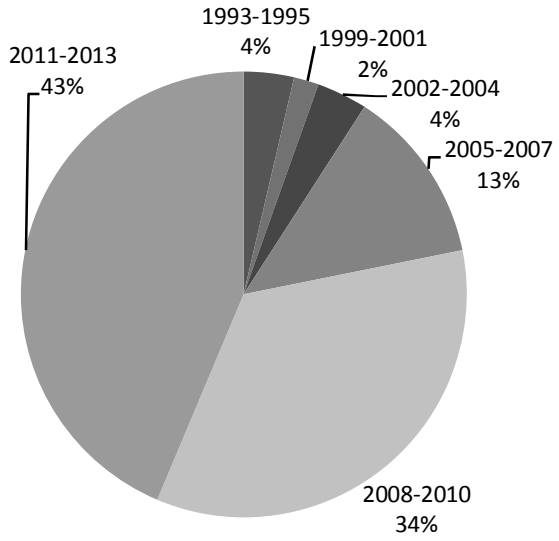

Fig 1: Percentage of papers used in the study

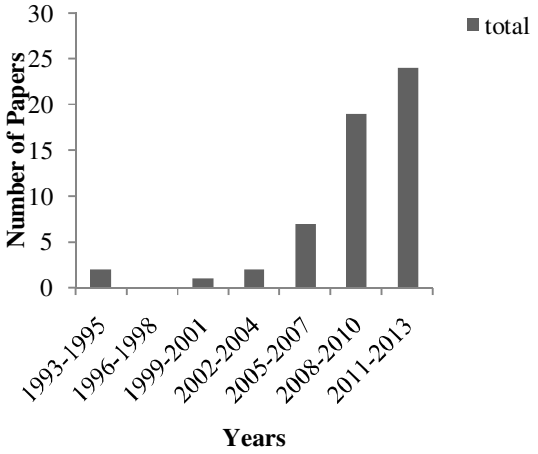

Fig 2: Comparison of number of papers published between years 1993-2013

Table 3 summarizes the number of papers that uses cryptographic algorithms solely as well as algorithms that have been used along with some other algorithms like in case of hybrid cryptography. It can be noticed that hybrid cryptography is a demanding approach for today. Hybrid cryptography is gaining its strength as the naïve researchers laid more emphasis on combination of different cryptographic algorithms for better results as shown in the table 3.

Table 3: Comparison of the number of papers using cryptographic algorithms on single and integrated basis

Year	Single	Integrated	Total
1993-1995	1	1	2
1996-1998	0	0	0
1999-2001	1	0	1
2002-2004	2	0	2
2005-2007	4	3	7
2008-2010	14	5	19
2011-2013	12	12	24

Fig 3 is showing the use of hybrid cryptography in the past 20 years. Between the years 2005-2007, the combination of different algorithms has been performed with RSA and the results show great deal of computational speedup and security. Then from 2008-2010, there is a peak rise in the use of hybrid cryptography for integration of various techniques and algorithms which continues till present.

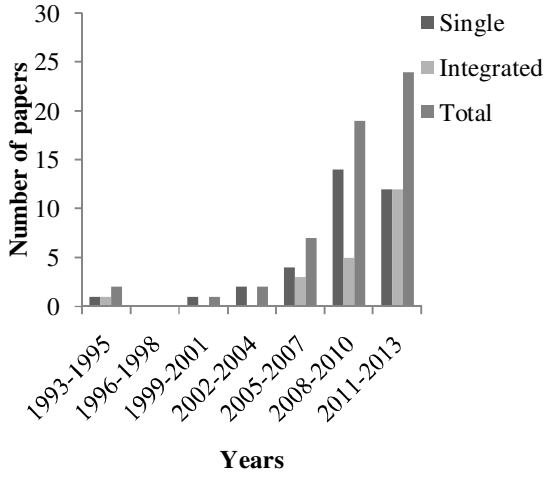

Fig 2: Comparison of the number of papers using the combination of algorithms and single algorithms usage

As elaborated in Table 4 that summarizes fig. 4 and 5, the RSA has become the most common standard of encryption in the information security world. The RSA is now the most widely used public-key system. The reason is the fact that the RSA is based on Integer Factorization problem (IFP) and now used by various web browsers such as Netscape for E-mail encryption programs. RSA is the first algorithm that can be used for signing as well as encryption and was known to be one the greatest achievements of public key cryptography.

From fig. 4, it can be easily analyzed that at an early stage, RSA has been used less frequently. But in duration of 2008-2010, RSA usage has been found to be 10% and then made an elevation of 48% from 2011-2013. The uses of RSA are increasing till now and hope to be increased further.

f RSA papers available in the past

Table 4: Number of papers used RSA in the study

Years	RSA Papers	Total Papers
1993-95	2	2
1996-98	0	0
1999-2001	1	1
2002-04	1	2
2005-07	3	7
2008-10	9	19
2011-13	15	24
Total	31	55

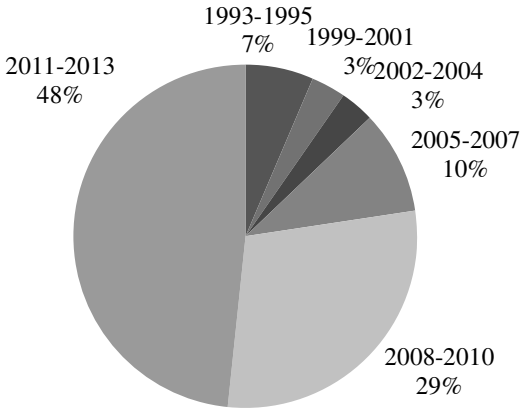

Fig 3: Percentage of RSA used in hybrid cryptography

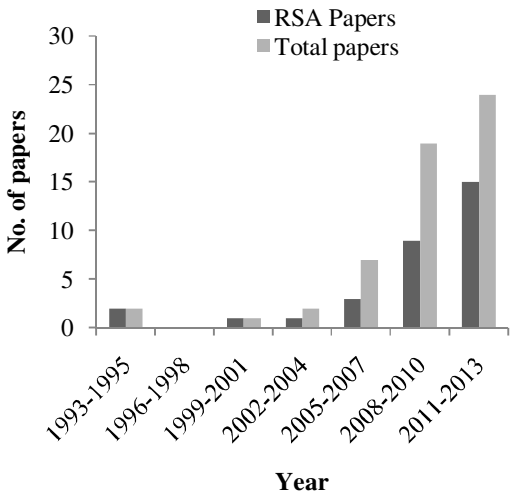

Fig 4: Bar representation o

4. Conclusion

With the results of increased efficiency, speed and throughput of various algorithms by the combination of various algorithms and techniques, hybrid cryptography has a great scope in the near future. Hybrid cryptography has been creating various opportunities for the naïve researchers and allows them to work upon various challenging limitations of algorithms in their original forms. Hybrid cryptography is easy to work upon and a great number of chances for improvement are there.

A number of different useful techniques and algorithms have been prescribed in this paper that can be used for providing security in the insecure media. This paper has been providing the study of past 20 years in the search for hybrid cryptographic algorithms that may help researchers to orientate their study areas and to choose various cryptographic algorithms for their studies. The study indicates the maximum use of RSA in the hybridization of various algorithms because of its Integer Factorization Problem. Diffie-Hellman being very secure is the prior choice for eliminating various limitations of cryptographic algorithms. AES and DES have limited scope of use because of the problem of key management. No doubt, the number of cryptographic algorithms presented here is neither complete nor exhaustive but a sample of papers that demonstrates the advantages and limitations of used cryptographic algorithms.

References

[1] S. Mohanty, B. Majhi, and V. Iyer, "A Strong Designated Verifiable Group Signature", Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on 22-23 March 2013, page(s): 518-523.

[2] H. WANG, Z. SONG, X. NIU, and Q. DING, "Key Generation Research of RSA Public Cryptosystem and MATLAB Implement", Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on 18-19 May 2013, page(s): 125-129.

[3] Y. L. Huang, F. Y. Leu, Y. K. Sun, C. C. Chu, and C. T. Yang, "A Secure Wireless Communication System by Integrating RSA and Diffie-Hellman PKDS in 4G Environments and an Intelligent Protection-key Chain with a Data Connection Core", Industrial Electronics (ISIE), 2013 IEEE International Symposium on 28-31 May 2013, page(s): 1-6.

[4] A. K. Mandal, C. Parakash, and Mrs. A. Tiwari, "Akash Kumar Mandal, Chandra Parakash, Mrs. Archana Tiwari", 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012.

[5] J. Zhang, and X. Jin, "Encryption System Design Based on DES and SHA-1", Distributed Computing and Applications to Business, Engineering & Science (DCABES), 2012 11th International Symposium on 19-22 Oct. 2012, page(s):317-320. [6] A. K. Mandal, and Mrs. A. Tiwari, "Comparative study of avalanche effect in DES using binary codes", Computing and Communication Systems (NCCCS), 2012 National Conference on 21-22 Nov. 2012, page(s): 1-4.

[7] H. D. Zodpe, P. W. Wani, and R. R. Mehta, "Design and Implementation of Algorithm for DES Cryptanalysis", Hybrid Intelligent Systems (HIS), 2012 12th International Conference on 4-7 Dec. 2012, page(s): 278-282.

[8] P S Rasmi, and Dr. V. Paul, "An Implementation of a New public key System based on RSA which leads hackers solve multiple hard problems to break the cipher", Intelligent Systems Design and Applications (ISDA), 2012 12th International Conference on 27-29 Nov. 2012, page(s): 656-661.

[9] R. S. Dhakar, A. K. Gupta, and P. Sharma, "Modified RSA Encryption Algorithm (MREA)", 2012 Second International Conference on Advanced Computing & Communication Technologies, 2012, page(s): 426 - 429

[10] S. A. Nagar, and S. Alshamma, "High Speed Implementation of RSA Algorithm with Modified Keys Exchange", 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012, page(s): 639 – 642.

[11] A Chitra, and T. B. Sheeba,"A Hybrid Reconfigurable Cryptographic Processor with RSA and SEA", Recent Trends In Information Technology (ICRTIT), 2012 International Conference, page(s): 428-433.

[12] M. O. Saarinen, "The BlueJay Ultra-Lightweight Hybrid Cryptosystem", IEEE Symposium on Security and Privacy Workshops, 2012, page(s): 27-32.

[13] S. P. Bansod, V. M. Mane, and L. R. Ragha, "Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity", 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India, 2012, page(s): 1-6.

[14] S. Gupta, and J. Sharma, "A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman", Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference, page(s): 1-4.

[15] A. A. Gutub, and F. A. Khan, "Hybrid Crypto Hardware Utilizing Symmetric-Key & Public-Key Cryptosystems", 2012 International Conference on Advanced Computer Science Applications and Technologies, 2012, page(s): 116-121.

[16] M. J. Dubal, T. R. Mahesh, and P. A. Ghosh, "Design Of New Security Algorithm Using Hybrid Cryptography Architecture", Electronics Computer Technology (ICECT), 2011 3rd International Conference (Volume:5), page(s): 99-101.

[17] J. Thomas, and N. S. Chaudhari, "Polynomial Solvability of Satisfiability and its Implication to Hybrid Cryptosystem Security", Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference, page(s): 52-54.

[18] S. Jailin, R. Kayalvizhi, and V. Vaidehi, "Performance Analysis of Hybrid Cryptography for Secured Data Aggregation in Wireless Sensor Networks", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT, MIT, Anna University, Chennai. June 3-5, 2011, page(s): 307-312.

[19] J. M. Ahmed, and Z. Md Ali, "The Enhancement of Computation Technique By Combining RSA and El-Gamal Cryptosystems", 2011 International Conference on Electrical

Engineering and Informatics,17-19 July 2011, Bandung, Indonesia, page(s): 1-5.

[20] S. Mukherjee, M. Hasan, B. Chowdhury, and M. Chowdhury, "Security of RFID Systems - A Hybrid Approach", 2011 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2011, page(s): 58-63.

[21] L.Smolinski, "Maintaining uniformity in the processes of encryption and decryption with a variable number of encryption rounds", Design & Test Symposium (EWDTS), 2011 9th East-West, page9s): 131-135.

[22] P. Sharma, S. Sharma, and R. S. Dhakar, "Modified Elgamal Cryptosystem Algorithm (MECA)", International Conference on Computer & Communication Technology (ICCCT)-2011, page(s): 439-443.

[23] L. Wang, and Y. Zhang, "A New Personal Information Protection Approach Based on RSA Cryptography", IT in Medicine and Education (ITME), 2011 International Symposium (Volume:1), page(s): 591-593.

[24] P.C. Lin, Y. D. Lin, and Y. C. Lai, "A Hybrid Algorithm of Backward Hashing and Automaton Tracking for Virus Scanning", IEEE Transactions On Computers, VOL. 60, NO. 4, APRIL 2011, page(s): 594-601.

[25] Y. Li, Q. Liu, and T. Li, "Design and Implementation of two Improved Batch RSA Algorithms", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference, page(s): 156-160.

[26] F. Shao, Z. Chang, and Y. Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU", 2010 Second International Conference on Communication Software and Networks, page(s): 588-590.

[27] H. Junru, and D. Yi, "An Efficient Signcryption Scheme with Shortened Ciphertext", 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), Page(s): V12-404 - V12-407

[28] J. Park, O. Yi, and J. Choi, "Methods for Practical Whitebox Cryptography", Information and Communication Technology Convergence (ICTC), 2010 International Conference, page(s): 474-479.

[29] Y. Li, Q. Liu, and T. Li, "Design and Implementation of an Improved RSA Algorithm", 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies, 2010, Page(s): 390 - 393

[30] T. Songsheng, and M. Xianzhen, "Research of typical block cipher algorithms",2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE), 2010, Page(s): 319 – 321.

[31] B. Chen-Xi, S. Rui, S. Shi-Lei, and H. Xin, "A New Digital Signature Scheme of ElGamal Type on Conic Curve over the Ring Zn",2010 International Conference on Computer Application and System Modeling (ICCASM 2010), Page(s): V11-378 - V11-381.

[32] W. Ren, and Z. Miao, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", 2010 Second International Conference on Modeling, Simulation and Visualization Methods, 2010, Page(s): 221 - 225 .

[33] Z. Jun, Z. H. Ying, and J. W. Dong, "ElGamal Digital Signature Scheme With a Private Key Pairs", Information Engineering and Computer Science (ICIECS), 2010 2nd International Conference , Page(s): 1 – 5.

[34] W. Xing-hui, and M. Xiu-jun, "Research of the Database Encryption Technique Based on Hybrid Cryptography", 2010 International Symposium on Computational Intelligence and Design, 2010, Page(s): 68 – 71.

[35] Y. Wang, and M. Hu, "Timing evaluation of the known cryptographic algorithms", 2009 International Conference on Computational Intelligence and Security, 2009, Page(s): 233 – 237.

[36] S. J Aboud, "An Effiecient Method For Attack RSA Scheme", Applications of Digital Information and Web Technologies, 2009. ICADIWT '09. Second International Conference, Page(s): 587 - 591 .

[37] S. Sarkar, B. Kisku, S. Misra, and M. S. Obaidat, "Chinese Remainder Theorem-Based RSA-Threshold Cryptography in MANET Using Verifiable Secret Sharing Scheme", 2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2009, Page(s): 258 – 262.

[38] M. Razi, and J. Quamar, "A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET", Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium, Page(s): 1 – 7.

[39] D. Wang, H. Bai, Q. Liu, and Z. Tong, "A Public-key Cryptography and A Entity Authentication Scheme Based on Improved Hyperbolic Function", Service Operations and Logistics, and Informatics, 2008. IEEE/SOLI 2008. IEEE International Conference, Page(s): 530 – 533.

[40] S. J Aboud, M. A AL-Fayoumi, M. Al-Fayoumi, and H. S Jabbar, "An Efficient RSA Public Key Encryption Scheme", Fifth International Conference on Information Technology: New Generations, 2008, Page(s): 127 – 130.

[41] M.B. Vishnu, and S.K. Tiong, "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm", Communications, 2008. APCC 2008. 14th Asia-Pacific Conference, Page(s): 1 – 5.

[42] A. Al Hasib and A. A. Md. M. Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography", Third 2008 International Conference on Convergence and Hybrid Information Technology, 2008, Page(s): 505 - 510 .

[43] H. Sun, M. Wu, W. Ting, and M. Jason Hinek, "Dual RSA and Its Security Analysis", IEEE Transactions On Information Theory, Vol. 53, No. 8, August 2007, Page(s): 2922 – 2933.

[44] H. A.Farouk, and M. Saeb, "An Improved FPGA implementation Of The Modified Hybrid Hiding Encryption Algorithm (MHHEA) For Data Communication Security", Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE'05) IEEE, 2005, Page(s): 76 - 81 Vol. 3.

[45] K. Jung, and I. A. Rao, "Design of User Authentication Protocol based on XTR-ElGamal",

2006 International Conference on Hybrid Information Technology (ICHIT'06), Page(s): 677 – 683.

[46] A. CHU, and M. SIMA, "Reconfigurable RSA Cryptography for Embedded Devices", Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference, Page(s): 1312 – 1315.

[47] S. Mathew, and K. P. Jacob, "A Novel Fast Hybrid Cryptographic System: MARS4", India Conference, 2006 Annual IEEE, Page(s): 1 – 5.

[48] A. Cilardo, A. Mazzeo, N. Mazzocca, and L. Romano, "A Novel Unified Architecture for Public-Key Cryptography", Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE'05) IEEE, 2005, Page(s): 52 - 57 Vol. 3.

[49] M.Ayoub Khan, and Y.P.Singh, "On the security of Joint Signature and Hybrid Encryption", Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication., 2005 13th IEEE International Conference (Volume:1).

[50] S. Harari, "A Session Key Establishment Protocol Using Trust", Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference.

[51] H. Eberle, N. Gura, S. C. Shantz, V. Gupta, and L. Rarick, "A Public-key Cryptographic Processor for RSA and ECC", Proceedings of the 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'04) 2004 IEEE, Page(s): 98 – 110.

[52] E. Mohammed, A. E. Emarah, and Kh. El-Shennawy, "A Blind Signature Scheme Based On ElGamal Signature", Radio Science Conference, 2000. 17th NRSC '2000. Seventeenth National, Page(s): C25/1 - C25/6.

[53] Dr. Mahmoud T. El-Hadidi, Dr. N. H. Hegazi, H. K. Aslan, "Implementation of a Hybrid Encryption Scheme for Ethernet", Computers and Communications, 1995. Proceedings., IEEE Symposium, Page(s): 150 – 156.

[54] X. Li, J. Chen, D. Qin, and W. Wan, "Research and Realization based on hybrid encryption algorithm of improved AES and ECC", Audio Language and Image Processing (ICALIP), 2010 International Conference, Page(s): 396 – 400.

[55] M. Shand, and J. Vuillemin, "Fast Implementations of RSA Cryptography", Computer Arithmetic, 1993. Proceedings., 11th Symposium , Page(s): 252 – 259.