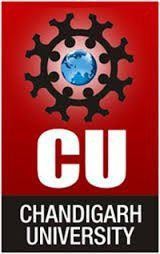
**HYBRID CRYPTOGRAPHY**

Submitted in partial fulfillment of the requirements for the award of degree of

**BACHELOR OF ENGINEERING** **IN**

**COMPUTER SCIENCE & ENGINEERING**

**IEEE FORM**



**Submittedto:**

**SHIKHA ATWAL**

**SubmittedBy:**

**YUKTI GOYAL 18BCS1838**

**SHUBHAM SHUKLA 18BCS1848**

**PRADIPTA SARKAR 18BCS1854**

**MIRTUNJAY GUPTA 18BCS1843**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**Chandigarh University, Gharuan**

**August 2019**

**IEEE FORM**

**IEEE FORM OF PROJECT Hybrid Cryptography**

**Abstract**:

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting health care information. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. The reader is advised, then, that the topics covered here only describe the first of many steps necessary for better security in any number of situations.

The proposed system is a cryptographic algorithm which accepts any kind of data for processing. In addition of that the simulation of the proposed methodology enables a user to send and receive data using the application. The proposed simulation first accepts the data from the user and then compresses it in order to reduce the data size. After doing that it uses the proposed cryptographic algorithm data to manipulate the data into cipher text. The generated cipher text is compressed again and using file splitter utility and then it is transmitted much efficiently on network. On the other end the receiver follows the same procedure in reverse direction to decrypt IT. Cryptographic algorithms have a good role in information security for wireless sensor networks. Now, various types of cryptographic algorithms provide security in networks, but there are still some problems. In this research, to improve the power of these algorithms, a new hybrid encryption algorithm for monitoring energy transmission lines and increasing the security of wireless sensor networks is proposed. The proposed hybrid encryption algorithm provides the security and timely transmission of data in wireless sensor networks to monitor the transmission pipelines. The proposed algorithm fulfills three principles of cryptography: integrity, confidentiality and authentication. The details of the algorithm and basic concepts are presented in such a way that the algorithm can be operational.

**Keywords:**

Advance hybrid cryptography, cryptography algorithm, hybrid cryptography, confidentiality, integration, authentication, DES , AES , RSA Diffie-Hellman , Elgamal Algorithm , DSA

**Introduction**

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

Security can be established in each layer of application, network, data link, and physical layer. Cryptographic algorithms play a significant role in information security systems, and can also meet security goals in wireless sensor networks. Encryption is the process of changing message or information so that only authorized people can read that information. Encryption does not prevent the attack, but the content of the message is protected by the attacker. In an encryption scheme, the information or message set to be transmitted using an encryption algorithm change so that it can only be read by decrypting. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. For a good design encryption scheme, computational resources and much more skills are required. An authorized recipient of the message can easily decrypt the message with a key and an encryption algorithm. Cryptography is a knowledge of hiding information and verification, and includes protocols, algorithms, and secure strategies to prevent unauthorized access to critical information. Encryption provides a mechanism for verifying each component of a communication. Encryption follows the three main goals include message confidentiality, message integrity and Sender authentication. In message confidentiality, only one authorized recipient must be able to extract the contents of the message from its encrypted form. Confidentiality includes a set of conventions or rules that limit the access to certain types of information, and hid information and stop free access to encrypted information. In message integrity, the recipient must be able to detect the message that has been tampered with. Data integrity, maintenance, and assurance of the integrity of data throughout its life, and is an essential aspect of the design, implementation and use of any system that stores, processes and retrieves data. Maintaining the accuracy of the data means ensuring that the information is accurate and does not change its original content during transmission. Changing the initial content of the information may be accidental due to sending or deliberate problems. In sender authentication, the receiver should be able to check the message, the sender’s identity, the source, or the send and confirmation path of the sender. Authentication is the correct confirmation of a feature of a single piece of data that is done by an entity. Authentication is a validation process and may involve verification of a person by using his identity documents or by checking his credentials using a digital certificate. An encryption algorithm is a component for secure electronic data transfer. Operational and mathematical stages develop cryptographic algorithms. Cryptographic algorithms prevent data frauds and unauthorized access to electronic information. Some cryptographic algorithms are faster than others. The designers and developers of the algorithms make the math background more complicated by the algorithms so that the attackers cannot penetrate. The power of an encryption algorithm usually depends on the length of the key. Cryptographic algorithms and functions used in cryptography are divided into symmetric, asymmetric, hashing, key exchange, key derivation and hybrid.

**Literature review**

This section provides the study on the recent contribution placed in the domain of hybrid cryptographic data models. According to Mohammad Reza Najaf Torkaman et al [6] exists a big demand for innovative secure electronic communications while the expertise level of attackers increases rapidly and that causes even bigger demands and needs for an extreme secure connection. An ideal security protocol should always be protecting the security of connections in many aspects, and leaves no trapdoor for the attackers. Nowadays, one of the popular cryptography protocols is hybrid cryptosystem that uses private and public key cryptography to change secret message. In available cryptography protocol attackers are always aware of transmission of sensitive data. Even non-interested attackers can get interested to break the ciphertext out of curiosity and challenge, when suddenly catches some scrambled data over the network. First of all, we try to explain the roles of innovative approaches in cryptography. After that we discuss about the disadvantages of public key cryptography to exchange secret key. Furthermore, DNA steganography is explained as an innovative paradigm to diminish the usage of public cryptography to exchange session key. In this protocol, session key between a sender and receiver is hidden by novel DNA data hiding technique. Consequently, the attackers are not aware of transmission of session key through unsecure channel. Finally, the strength point of the DNA steganography is discussed. Information protection is one of the most important issues in every domain, especially when we are talking about enterprises. Information safety can be translated into three key terms: integrity, availability and data protection. There is a great number of means used in order to achieve the three objectives simultaneously. The most popular is cryptography because it offers a lot of techniques which nowadays are impossible to fail. In this paper Georgiana Mateescu et al [7] want to prove their efficiency by comparing the different types of crypto algorithms and by presenting their weaknesses and strengths. In order to maximize the benefits of the crypto techniques, we propose a hybrid approach that combines three crypto algorithms. Mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client to overcome on the limitation of mobile devices and uses the main advantage of cloud computing. As mobile cloud computing continues to grow, so does the need for effective security mechanisms because data offloaded and moved from mobile to unknown destination. Encryption algorithms play good roles in information security systems (ISS). Those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. The present asymmetric encryption methods and symmetric encryption methods can offer the security levels but with many limitations. For instance key maintenance is a great problem faced in symmetric encryption methods and less security level is the problem of asymmetric encryption methods even though key maintenance is easy. To improve the strength of these algorithms, Hatem M. Abdul Kader et al [8] propose a new hybrid cryptographic algorithm in this paper. The algorithm is designed using combination of two symmetric cryptographic techniques and two Asymmetric cryptographic techniques. This protocol provides three cryptographic primitives, integrity, confidentiality and authentication. It is a hybrid encryption method where elliptical curve cryptography (ECC) and advanced encryption (AES) are combined to provide node encryption. (RSA) algorithm and (Blowfish) are combined to provide authentication and (MD5) for integrity. We applied this protocol on one type of wireless sensor network (Zigbee) to be evaluated and compared it with other four hybrid cryptography protocol. The results show that the proposed hybrid cryptographic algorithm gives better performance in terms of computation time and the size of cipher text. Satellite based communication is a way to transmit digital information from one geographic location to another by utilizing satellites. Satellite as communication medium to transfer data vulnerable various types of information security threat, and require a novel methodology for safe and secure data transmission over satellite. Omar M.Barukab et al [9] a methodology is proposed to ensure safe and secured transferred of data or information for satellite based communication using symmetric and asymmetric Cryptographic techniques. Cryptography is the technique to encrypt and decrypt the data for secure communication. The cryptographic mechanism enables the entities of network to transmit secure data through insecure channel. So that, only the intended users can access the transmitted data. Two public key cryptographic techniques are mostly used for secure transmission of data, namely Elliptic Curve Cryptography & RSA. Among this two cryptographic system, ECC is more first due to its small key size. DNA-cryptography is a new technique, which also used for secure data transmission in recent years. The DNA based cryptography technique, derived from DNA computing. It uses DNA nucleotide sequence for cryptographic purpose. To develop more secure and stable cryptography technique, Prokash Barman et al [10] propose a new hybrid DNA encoded Elliptic Curve Cryptography scheme in this paper. DNA encoded ECC cryptography uses smaller key size and less computation power with multilevel security. The main attraction of the proposed system is that it has two level of security. First is unknown DNA sequence based encoding and the second is Light weight ECC based encryption and decryption system.

The ECC algorithm has significant advantages over the RSA algorithm, which reduces the computation time as well as the amount of data transmitted. The RSA algorithm is a method for implementing a public key encryption system whose security depends on the complexity of the large prime numbers factoring. This method is suitable for data encryption and digital signature creation. The ECC algorithm is related to the algebraic structure of elliptic curves and its difficulty in elliptical curve size. The key advantage of this algorithm is the smaller key size, which reduces storage and transmission. For example, an elliptic curve algorithm can provide the same level of security in an RSA based system with smaller modules and keys. For current cryptographic purposes, an elliptic curve is a curved surface that contains points of the equation y2=x3+ax+b. Compared to the RSA, ECC has a smaller key and uses less memory, which is highly regarded by wireless sensor networks. ECC cryptography has recently been an important topic in cryptographic research, which provides a higher level of security with a smaller key size than other encryption methods .ASCII values match pairs of texts, and pairings are used as ECC encryption inputs. This proposed new method reduces the cost of the mapping operation and requires the sharing of the table between the sender and the receiver. The algorithm is designed to be used to encrypt or decrypt any type of text with the values of the ASCII. Many images are moving in the network daily. Most of these images are confidential and should be transmitted securely. Cryptography plays a significant role in the safe transfer of images. The exponential problem solving a discrete logarithm of an elliptic curve proportional to the size of the ECC

A Hybrid Encryption Algorithm for Security Enhancement .

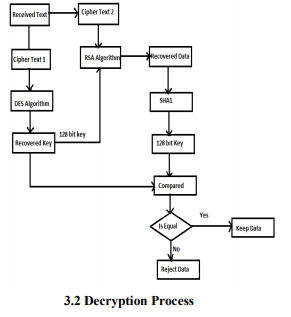
RSA is the foundation of many encrypted applications. Great progress is for public key encryption and is also used for digital signing. The algorithm process consists of three steps: key generation, encryption and decryption. The Diffie-Hellman key exchange method allows two entities that have no prior knowledge to share a common key through an unsecured connection channel. Diffie-Hellman has been involved in multi-protocol development, including SSL, SSH, and IPS. The RSA algorithm is used as one of the most efficient encryption algorithms and provides confidential, information integrity and privacy. The minimum overhead, increased throughput and privacy are its benefits. In this method, the user uses the RSA algorithm and generates encrypted messages that are categorized according to priority and then sent. The receiver decrypt messages using the RSA algorithm and according to their priority. Symmetric and asymmetric hybrid encryption algorithms provide integrated data transfer and concealment at higher speeds and play an important role in virtual private networks.Elliptic curve cryptography is an effective cryptography and has its own special advantages such as an efficient key relative to other key public infrastructures. In the article of Shahryar et al.The generation phase is based on a common key and a generator point of G, which is a generator of a curve to obtain a random sequence. The AES encryption is then applied to these sequences and the keys to the image encryption are obtained. Using AES, along with random allocation, offers a prominent encryption method. The image encryption is rapidly increasing with the increasing use of the Internet and media. Sharing important images on non-secure channels provides the ability to attack and steal. Encryption techniques are the best ways to protect images against attacks. Hill cipher algorithm is one of the symmetric cryptographic methods, with a simple structure and fast computing, but it has a weak security because the sender and receiver must share a private key on a non-secure channel. In the article of Dawahdeh et al.A self-inverse key matrix is used to create encryption and decryption keys so there is no need to find the reverse key matrix in the decryption process. A 4×4 hidden key matrix is used as an example in this study. The Internet in the world today is widely used to access information, which is why there is a need to send secure information. The main goal of Brindha et al. Encrypted text is decrypted using decrypt keys and AES. The application of the network and the Internet is growing at a high rate, thus increasing the need to protect such applications. The first way is to compress data in half, and the second method focuses on producing characters of encrypted text differently for the same text characters than the different events of the character in the text. The combined effect of using symmetric algorithms with the proposed algorithm creates a hybrid encryption scheme that makes it difficult for an attacker to learn from messages transmitted in an unsecured transmission environment. In this paper, encryption and decryption are described in detail in four sections along with the code. In the last section, the key generated is different for each character, which means that a single character in the text may have a different cipher character corresponding to the character position .A hybrid encryption system combines the convenience of a public key system with the efficiency of a symmetric key. In this article, two secure data encryption methods are provided that are important for confidential. The system uses two different encryption algorithms for the encryption and decryption process; one is public key encryption based on a linear block cipher, and the other is private key encryption based on a symmetric simple algorithm. This encryption algorithm provides more security is better than other existing hybrid algorithms. A computer network is an interconnected group of independent computing nodes that interact with each other by using a proper definition and a set of agreed rules and conventions known as protocols, and permitting the sharing of resources preferably in a way that can be Predictable and controllable. At the moment, various types of cryptographic algorithms provide high security for information in a controlled network. These algorithms need to specify the data security and authenticity of the user. In order to improve the strength of these security algorithms, a new security protocol for online transactions has been designed using the combination of symmetric and asymmetric encryption methods in Subasree et al. [Subasree and Sakthivel (2010)]. This protocol meets the three basic principles of encryption: integrity, confidentiality, and authentication. These basic principles can be met by using elliptic curve cryptography, Dual RSA and MD5. ECC for encryption, Dual RSA for authentication and MD5 for integrity. This new security protocol uses a combination of symmetric and asymmetric methods for better security and integrity. The text is encrypted using ECC. At the same time, the hash value is calculated using MD5. The resulting hash value is then encrypted with the Dual RSA algorithm. The process of decrypting is the inverse process of encryption.

A Hybrid Encryption Algorithm for Security Enhancement 329 A set of connected computers using communication channels requires security for the exchange of information. This field of work involves a specialist in network security with the network administrator that prevents and monitors unauthorized access, modifies, and disables the use of the network. To combat this growing problem, security professionals are looking for better protection. Attacks have endangered security; hence, various symmetric and asymmetric encryption algorithms are provided to achieve the appropriate security services such as identity, confidentiality, integrity and availability. These algorithms are designed to provide security and authenticate users. encryption methods. Wireless sensor networks consist of hundreds or thousands of low-cost, low-power and self-organized nodes that are highly distributed. Wireless sensor networks are growing and require effective security mechanisms, because sensor networks may interact with sensitive data. Cryptographic algorithms have a good role in information security systems. Currently, various types of cryptographic algorithms provide security in wireless sensor networks, but there are still some problems. At present, symmetric and asymmetric encryption methods can provide a level of security with some constraints. In Dhaliwal et al. One of the goals of wireless sensor networks is to transmit trusted information from one node to another in the network. In the paper by Bhave et al. In this article for exploring purposes, plain text is given with 16 bytes and a key is considered and the algorithm is implemented. Many key management schemes are provided in a wireless sensor network. Sensor nodes are provided with insufficient battery power, low memory, limited computing, and communication constraints. Energy in safe and efficient routing is a major issue for wireless sensor networks. SAERP is an approach in energy-efficient routing that is based on Some sensors use Bluetooth technology to communicate in wireless sensor networks. This encryption is broken down under certain conditions with the complexity of time O (264). In the proposed hybrid algorithm instead of E0 encryption, the DES algorithm is used for data transmission because it has higher efficiency in block encryption and uses the RSA algorithm to decrypt the DES key because it is superior to cryptographic key management. Under the protection of DES and RSA algorithms, the Bluetooth system is safer. It is clear that the whole encryption method is simple and efficient, and in addition, the confidentiality of the algorithm is high. Bluetooth features include wireless, short range and low power. Therefore, the use of AES and RSA algorithms makes it safer to transfer information in Bluetooth. In addition, the hybrid encryption algorithm is a convenient and easy way to encrypt data and enhance confidential. Security is one of the most important and fundamental issues for transmitting data in wireless sensor networks. Hence, innovative hybrid encryption algorithms for security have been developed. DNA cryptography plays a vital role in the fields of communication and data transmission. In DNA encryption, the biological concept of DNA is used not only to store data and information carriers, but also to perform computations. Encryption plays an important role in securing wireless sensor networks.

**Proposed method**

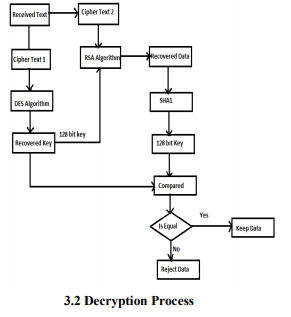
The proposed working hybrid model for data cryptography is given using figure 3.1 and figure 3.2. In figure 3.1 the encryption process of the system is described and the figure 3.2 reports the decryption process of the system. During the encryption process user need to encrypt the file using the hybrid cryptographic model, thus a input file is first produced to the system. The input file is first processed using SHA1 hash generation algorithm, the SHA1 algorithm generates the 128 bit hash code for the input data Input file.

The proposed working hybrid model for data cryptography is given using figure 3.1 and figure 3.2. In figure 3.1 the encryption process of the system is described and the figure 3.2 reports the decryption process of the system. During the encryption process user need to encrypt the file using the hybrid cryptographic model, thus a input file is first produced to the system. The input file is first processed using SHA1 hash generation algorithm, the SHA1 algorithm generates the 128 bit hash code for the input data Input file.



Input file: This is the input file to be sent over the network. SHA1: The compressed zip file is produced before the SHA1 algorithm to generate 128 bit hash. This hash is used to check the data validity at the receiver end. If the sender generated hash matched with the receiver end hash than the data is valid otherwise data is corrupt.

Key (16 bytes): This is SHA1 generated hash which is separately treated as key form encryption. Over the produced 128 bit hash key the bit discarding process is taken place, in this process the 128 bit hash code is converted into 16 blocks of the 8 bit data. In each block of data the first bit is removed and placed separately for further processing. Thus the 128 bit hash code is converted into 112 bit of code and 16 bit of separated code. Both the bits 112 and 16 bit data is produced into a key generator where the 16 bit data is divided into 2 blocks of 8 bit and 112 bit of data converted into 14 blocks of data both the newly generated are combined to generate the complete 128 bit of key. For securing the key more the DES algorithm is used to encrypt the key which generates the cipher 1 which the encrypted key for decryption process. On the other hand the input original data is produced over the RSA algorithm with a 128 bit key generated by the key generator. This process generates the cipher 2. In further steps the cipher text 1 and cipher text 2 is combined and ready to prepare the text for transmission.



The transmitted text to the network is received by the end user, this text is termed here as the received text. In first process the received text is divided into two different ciphers, cipher 1 which is outcome of key data and seconds the cipher 2 that contains the encrypted data for security. The cipher 1 is treated first to generate the key for data recovery, therefore first the cipher text 1 is produced to DES algorithm for the recovering the original key by which the data is recovered. After recovering key using decipher of cipher text 1 the key is produced to RSA algorithm with the cipher text 2. The RSA algorithm decipher the original text and can be used with the other application but for authenticating the recovered data on receiver end the integrity check is applied for the data. Therefore first the recovered data is processed through the SHA1 hash key and 128 bit obtained from the data. In further the comparer is implemented, the comparer has two functionalities first using the SHA1 128 bit, regenerate the original key by which the encryption performed. Thus the same operation is performed over the 128 bit to generate key and second the comparison among generated key and the obtained key from network. In further is both the keys are found similar the data is accepted by the system else the data can be rejected.

Input file: This is the input file to be sent over the network. SHA1: The compressed zip file is produced before the SHA1 algorithm to generate 128 bit hash. This hash is used to check the data validity at the receiver end. If the sender generated hash matched with the receiver end hash than the data is valid otherwise data is corrupt.

Key (16 bytes): This is SHA1 generated hash which is separately treated as key form encryption. Over the produced 128 bit hash key the bit discarding process is taken place, in this process the 128 bit hash code is converted into 16 blocks of the 8 bit data. In each block of data the first bit is removed and placed separately for further processing. Thus the 128 bit hash code is converted into 112 bit of code and 16 bit of separated code. Both the bits 112 and 16 bit data is produced into a key generator where the 16 bit data is divided into 2 blocks of 8 bit and 112 bit of data converted into 14 blocks of data both the newly generated are combined to generate the complete 128 bit of key. For securing the key more the DES algorithm is used to encrypt the key which generates the cipher 1 which the encrypted key for decryption process. On the other hand the input original data is produced over the RSA algorithm with a 128 bit key generated by the key generator. This process generates the cipher 2. In further steps the cipher text 1 and cipher text 2 is combined and ready to prepare the text for transmission.

The transmitted text to the network is received by the end user, this text is termed here as the received text. In first process the received text is divided into two different ciphers, cipher 1 which is outcome of key data and seconds the cipher 2 that contains the encrypted data for security. The cipher 1 is treated first to generate the key for data recovery, therefore first the cipher text 1 is produced to DES algorithm for the recovering the original key by which the data is recovered. After recovering key using decipher of cipher text 1 the key is produced to RSA algorithm with the cipher text 2. The RSA algorithm decipher the original text and can be used with the other application but for authenticating the recovered data on receiver end the integrity check is applied for the data. Therefore first the recovered data is processed through the SHA1 hash key and 128 bit obtained from the data. In further the comparer is implemented, the comparer has two functionalities first using the SHA1 128 bit, regenerate the original key by which the encryption performed. Thus the same operation is performed over the 128 bit to generate key and second the comparison among generated key and the obtained key from network. In further is both the keys are found similar the data is accepted by the system else the data can be rejected.

The purpose of this research is to develop it as an applied research. Initial information on wireless sensor networks, functions and security has been collected, studied and presented. Articles focusing on the operation of wireless sensor networks in the transmission of energy and enhancing the security of data transmission using a combination of encryption algorithms were developed and presented. Familiarity with the latest actions taken in the field of cryptography and diagnostic information in the area of energy transfer. In order to implement the solutions, several articles with the most recent release date were carefully reviewed at the level of implementation details. Throughout the description, details of the implementation of some of the cryptographic algorithms as well as how to combine them together to provide three principles of cryptography including integrity, confidentiality, and authentication were introduced. Some articles in the implementation area have not been fully implemented and only one has provided a hybrid algorithm. In the implementation of some of the algorithms, there were some limitations that arise from the definition of those algorithms. According to the studies, the lack of a hybrid cryptographic algorithm for transmitting diagnostic information in wireless sensor networks was considered to monitor and enhance the security of energy transmission pipelines, in such a way that three principles of cryptography include integrity, confidentiality and authentication Coverage, as well as the possibility of its operational implementation. Each of the examined algorithms fulfilled a part of the security needs, therefore, a comprehensive roadmap for increasing the security of data transfer using past studies is formulated and a general overview of the process of doing the work is determined.

**Comparison**

In the proposed algorithm, the advantages of symmetric and asymmetric encryption algorithms are combined to establish the three principles of confidentiality, authentication and integrity. Correspondingly, the limits of wireless sensor networks are considered in the exchange and transfer of information. The cryptographic process is performed using the Rijndael algorithm with 256-bit blocks. Rijndael algorithm is a high-speed symmetric encryption algorithm and variation in implementation.

Due to computational constraints on sensors, two principles of authentication and integration have been attempted in the form of a process so that their digital signatures also provide some kind of integration of the encryption system. Some of the features are tailored to the limitations of the benefits of the proposed algorithm. Some of them are referred to:

1. Using a variable length encoding system
2. Blocking with larger sizE
3. Using symmetric cryptography
4. Use asymmetric cryptography for key exchange
5. Use of two asymmetric encryption algorithms
6. Combining processes for authentication and integration
7. Using the SHA-256 hash algorithm
8. Implement a hybrid cryptographic system

**Conclusion and future work**

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.

This paper has briefly (!?) described how digital cryptography works. The reader must beware, however, that there are a number of ways to attack every one of these systems; cryptanalysis and attacks on cryptosystems, however, are well beyond the scope of this paper. In the words of Sherlock Holmes (ok, Arthur Conan Doyle, really), "What one man can invent, another can discover" ("The Adventure of the Dancing Men," in: The Return of Sherlock Holmes, 1903).

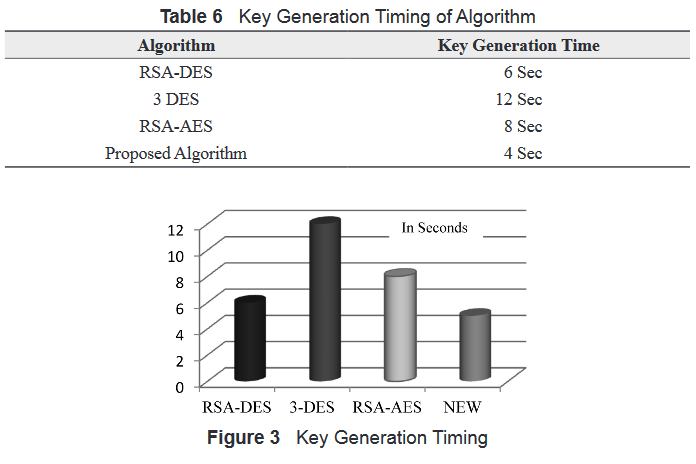
There are a lot of topics that have been discussed above that will be big issues going forward in cryptography. As compute power increases, attackers can go after bigger keys and local devices can process more complex algorithms. Some of these issues include the size of public keys, the ability to forge public key certificates, which hash function(s) to use, and the trust that we will have in random number generators. Interested readers should check out "Recent Parables in Cryptography" (Orman, H., January/February 2014, IEEE Internet Computing, 18(1), 82-86).

Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that secrecy is not the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also well-tested and well-studied! In fact, time is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys.

**Result & discussion**

The encryption/decryption algorithm is compared on the basis of time consumption check which pair of algorithms is more efficient for hybrid encryption/decryption of messages. We have taken various different message lengths are used and results are drawn as shown in the following Table 6. Figure 3 shows results of time consumed by the various pairs of algorithm in graphical form. It illustrates the execution time in milliseconds taken by each pair of algorithms to hybrid encrypt/decrypt the message of various different sizes mentioned in Table 7 and Figure 4. The graph shows that the combination of linear block cipher -- Symmetric key takes minimum time so it executes faster than RSA-DES and RSA-AES.

The overall performance evaluation of RSA-DES, RSA-AES and new proposed algorithm mentioned in Figure 5.



**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.

Bamford, J. (1983). The Puzzle Palace: Inside the National Security Agency, America's most secret intelligence organization. New York: Penguin Books.

Bamford, J. (2001). Body of Secrets : Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century. New York: Doubleday.

Barr, T.H. (2002). Invitation to Cryptology. Upper Saddle River, NJ: Prentice Hall.

Basin, D., Cremers, C., Miyazaki, K., Radomirovic, S., & Watanabe, D. (2015, May/June). Improving the Security of Cryptographic Protocol Standards. IEEE Security & Privacy, 13(3), 24:31.

Bauer, F.L. (2002). Decrypted Secrets: Methods and Maxims of Cryptology, 2nd ed. New York: Springer Verlag.

Belfield, R. (2007). The Six Unsolved Ciphers: Inside the Mysterious Codes That Have Confounded the World's Greatest Cryptographers. Berkeley, CA: Ulysses Press.

Denning, D.E. (1982). Cryptography and Data Security. Reading, MA: Addison-Wesley.

Diffie, W., & Landau, S. (1998). Privacy on the Line. Boston: MIT Press.