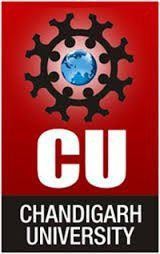
**HYBRID CRYPTOGRAPHY**

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

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

**COMPUTER SCIENCE & ENGINEERING**

**FINAL PROGRESS REPORT**



**Submittedto:**

**SHIKHA ATWAL**

**SubmittedBy:**

**YUKTI GOYAL 18BCS1838**

**PRADIPTA SARKAR 18BCS1854**

**MIRTUNJAY GUPTA 18BCS1843**

**SHUBHAM SHUKLA 18BCS1848**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

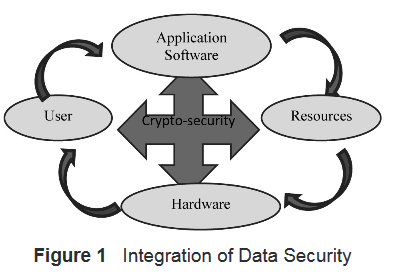
**Chandigarh University, Gharuan**

**April 2020**

**Introduction**

Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme. Hybrid encryption is achieved through data transfer using unique session keys along with symmetrical encryption. Public key encryption is implemented for random symmetric key encryption. The recipient then uses the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message. The combination of encryption methods has various advantages. One is that a connection channel is established between two users’ sets of equipment. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced. The result is the added security of the transmittal process along with overall improved system performance. The hybrid cryptosystem is itself a public-key system, who’s public and private keys are the same as in the key encapsulation scheme. In place of public key system we can use digital signature like message digesting function with symmetric key system to make hybrid crypto system. Note that for very long messages the bulk of the work in encryption/decryption is done by the more efficient symmetric-key scheme, while the inefficient public-key scheme is used only to encrypt/decrypt a short key value. For example, to encrypt a message addressed to user-1 in a hybrid technique user-2 does the following:

* Obtains user-1 public key.
* Generates a fresh symmetric key.
* Encrypts the message using the symmetric key.
* Encrypt the symmetric key using user-1 public key. And send both of these encryptions to user-1. To decrypt this hybrid cipher text, user-1 does the following.
* User-1 uses her private key to decrypt the symmetric key.
* User-1 uses this symmetric key to decrypt the message.



### Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between literally billions of people and is used as a tool for commerce, social interaction, and the exchange of an increasing amount of personal information, security has become a tremendously important issue for every user to deal with.

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.

This paper has two major purposes. The first is to define some of the terms and concepts behind basic cryptographic methods, and to offer a way to compare the myriad cryptographic schemes in use today. The second is to provide some real examples of cryptography in use today.

**Literature review**

Shaar, Saeb, Elmessiery and Badawi (2003). In this proposal, encryption algorithm that can be used for hardware-implemented applications to secure data communications, this encryption algorithm is based on hiding a number of bits from plain text message into a random vector of bits. The name demonstrates the two basic operations of this algorithm, these operations include inserting part of the plaintext bits into a cover to hide it from recognition, that is, there are no conventional operations on the ciphered text, just plain hiding in a random bit string, the name hybrid is used to show that the algorithm has built-in features that are inherited from data hiding techniques or steganography.

Ramaraj, Karthikeyan and Hemalatha (2009), design the new security protocol using hybrid encryption technique for on line transaction. The hybrid encryption technique is a combination of both symmetric and asymmetric cryptographic techniques. It provides all the three cryptographic primitives -- integrity, confidentiality and authentication. In this proposed design methodology, the new protocol design using Symmetric cipher (AES-Rijndael) and public key cryptography (RSA) with hash function. Tat Wi (2010) in this project, encryption will be implemented in information on a web that makes it hard to be readable and secure. In this encryption, it uses the substitution cipher in which each letter in the plaintext is replaced by some fixed number of position down the alphabet. This method is names after Julius Caesar who using this method to communicate with his generals.

The result from this project is a data which is encrypted and be decrypted to its readable form. As a conclusion, Caesar cipher algorithm can be implemented in hybrid encryption project to make data secure and better. Kuppuswamy and Chandrasekar’s (2011) paper deals with a new algorithm, which is based on linear block cipher. The concept of this new algorithm is based on modular 37 (alphabets and numerals) whereas existing algorithms are based only on modular 26 (only alphabets). We are naming this linear based algorithm as New linear block cipher or Nlbc. Kuppuswamy and Al-Khalidi (2012) proposed research main goal is to reflect the importance of security in network and provide the better encryption technique for currently implemented encryption techniques in simple and powerful method. In this research we have proposed a modular 37 and select any number and calculate inverse of the selected integer using modular 37. The symmetric key distribution should be done in the secured manner. Also, we examine the performance of our new SSK algorithm with other existing symmetric key algorithm.

**Research objectives**

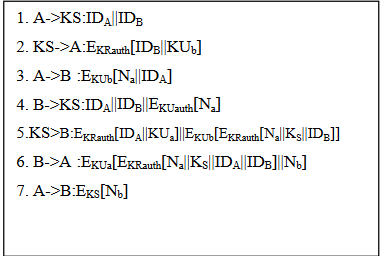
Privacy is one of the key issues addressed by information Security. Through cryptographic encryption methods, one can prevent a third party from understanding transmitted raw data over unsecured channel during signal transmission. The cryptographic methods for enhancing the security of digital contents have gained high significance in the current era. Breach of security and misuse of confidential information that has been intercepted by unauthorized parties are key problems that information security tries to solve. This paper sets out to contribute to the general body of knowledge in the area of classical cryptography by developing a new hybrid way of encryption of plaintext. DES algorithm is now considered insecure for many applications and has many weaknesses. This is mainly because its 56-bit key size is too small. Many attacks and methods that exploited the shortcomings of DES have rendered it an insecure block cipher. Triple DES which is an enhancement to DES was later proposed in which the original DES algorithm was applied thrice to increase the security. But it was found to be very slow. The most preferred algorithm is AES. It is considered to be the best encryption standard. Brute force attack is the only known possible attack against AES algorithm. Our proposed hybrid algorithm is found to be the best encryption standard and is given priority over other standards.

**Proposed Approach**

In our proposed approach, to manage the keys between the users using remote key servers. The key management and secure transaction will be done by hybrid encryption technique. In this approach, three steps will be followed.

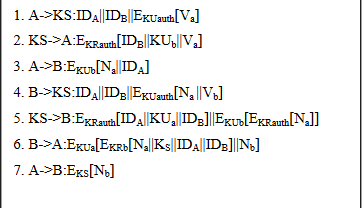
1. **Session Key Establishment Phase**

The identification of correct public key of proper person is more difficult without using any third party. In this phase the identification of correct public key of proper person using key servers. The following protocol proposed by Woo and Lam, makes use of nonce.



In the above protocol, in step 1, A informs the Key Server (KS) of its intention to establish a secure connection with B. The KS returns to ‘A’ copy of B’s public key certificate. Using B’s public key, A informs B of its desire to communicate and sends a nonce Na (step 3). In step 4, B asks the KS for A’s public key certificate and requests a session key; B includes A’s nonce so that the KS can stamp the session key with that nonce. The nonce is protected using KS public key. In step 5, the KS returns to B a copy of A’s public key certificate, plus the information {Na, KS, IDB, IDA}. This information basically says KS is the secret key generated by the KS on behalf of B and tied to Na. This information is encrypted using KS private key, to allow B to verify that information from the KS. It also encrypted using B’s public key, so that no other entity may use the information in an attempt to establish a fraudulent connection with A. In step 6, the information {Na, KS, IDB, IDA} still encrypted with KS private key, is relayed with A together with a nonce Nb, generated by B. All foregoing are encrypted using A’s public key. A retrieves the session key and uses it to encrypt Nb and return it to B. The last message assures B of A’s knowledge of the session key. Thus it is the pair {Na, IDA} that uniquely identifies the connection request of A.

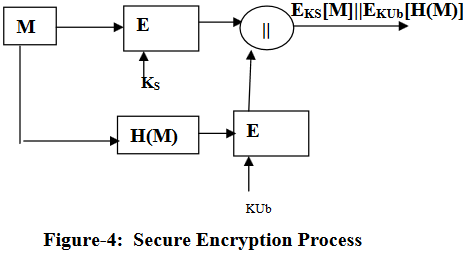
In our new protocol design, we revise the above protocol design to protect various attacks.



In our revised protocol, in step 1, A informs the Key Server (KS) of its intention to establish a secure connection with B. The A sends IDA, IDB and EKUauth[Va]. The Va is a shared common value only knows both A and KS. The KS maintains unique values for each user, it checks the user IDA and value Va is correct or not. If it is correct the KS assures that the information requisite is the correct person. If any unauthorized person as a member in KS, he/she sends the encrypted request using public key of the key server, but they don’t know about the value Va. In step 2, the KS returns to ‘A’ copy of B’s public key certificate and value Va. Using B’s public key, A informs B of its desire to communicate and sends a nonce Na(step 3). In step 4, B asks the KS for A’s public key certificate using the information IDA||IDB||EKUauth[Na ||Vb]. In this step we include Vb, so KS checks Vb and assures that the B is a correct person or not. The nonce also protected using KS public key. In step 5, the KS returns to B a copy of A’s public key certificate, plus the information {Na, IDB, IDA}. In step 6, the session key KS fixed by B and the information {Na, KS, IDB, IDA} still encrypted with B’s private key and again encrypted with A’s public key, is relayed with A together with a nonce Nb, generated by B. A retrieves the session key and uses it to encrypt Nb and return it to B. In this protocol, the KS assures the requester is a correct person or not. The session key value KS only knew by A and B.

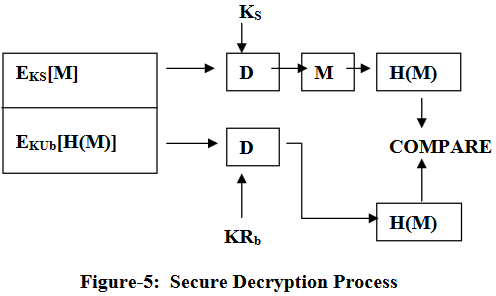
1. **Secure Transmission Phase**

The figure-4 illustrates this. In this phase, the first part sender ‘A’ selects common 128-bit session key value (KS) for encryption purpose. The AES-Rijndael symmetric encryption algorithm-using key value KS to encrypt the plain text. In the second part, the hash value was calculated by using the plain text and hash function. Again the hash value is encrypted using RSA with 1024-bit public key KUb. Both encrypted information send to the receiver B. The SHA-512 hash function used to perform hash calculation.



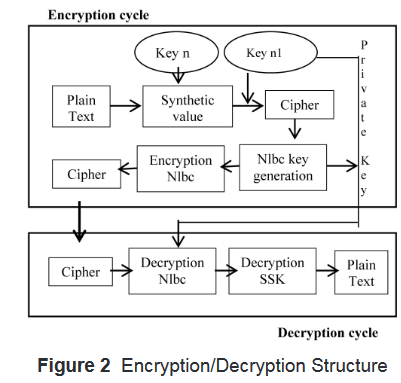
1. **Secure Decryption Phase**

In this phase, the first part sender B selects the session key KS for decryption purpose. The AES-Rijndael symmetric encryption algorithm using session key value KS to decrypt the plain text and calculate the hash value using hash algorithm SHA-512. In the second part, using receiver private key value KRb with RSA algorithm decrypts the encrypted hash value. Then, the decrypted hash value is compared with calculated hash value. If the hash value is equal, the receiver assures that integrity of the message good. The figure-5 illustrates this



**Proposed algorithm structure**

The proposed algorithm architecture of encryption and decryption method mentioned in the Figure 2 and procedure of the algorithm were as follows:



**Symmetric key algorithm (SSK)**

**SSK key generation method**

1. Select any natural number say as “n.”
2. Find the Inverse of the number using modulo 37 (key 1) say “k.”
3. Again select any negative number (for making secured key) “n1.”
4. Find the inverse of negative number using modulo 37 (key 2) “k1.”

**Encryption method**

1. Assign synthetic value for message.
2. Multiply synthetic value with random selected natural number.
3. Calculate with modulo 37.
4. Again select random negative number and multiply with it.
5. Again calculate with modulo 37 CT = (PT × n × n1) mod

**Decryption method**

1. Multiply received text with key 1 & key 2.
2. Calculate with modulo 37.
3. Remainder is Revealed Text or Plain Text PT = (CT × n–1 × n1–1) mod 1.

**Linear block cipher algorithm**

The algorithm of encryption and decryption of the technique is to use text and numbers during implementation of the message algorithm which is as follows. Here, we introduce our Nlbc algorithm asymmetric or public key algorithm. The major advantage of asymmetric cryptography is to use two different keys, one Public (open) key and one Private (secret) key. The encrypted message by sender can be decrypted by the other at receiving end and vice versa.

**Encryption technique**

Step 1: To encrypt a text message at first the given text and numbers are stored in a string variable, say m.

Step 2: Select k × k square matrix called as k.

Step 3: Select any integer value say as e.

Step 4: Make plain text or message as blocks according to the k matrix. And transpose the selected block.

Step 5: Multiply Plain text or message with selected square matrix and e value.

Step 6: Use modulation 37 with derived message. The remainder is Cipher text or decrypted message. Announce Cipher text, e, 37 as public key, and k as private key sent to the receiver in secured channel.

**Decryption technique**

Receiving the plaintext from cipher text using the key is called decryption or deciphering or decoding. Our New linear block cipher decryption sequences were as follows:

Step 1: Receiving Cipher text and Private Key k’ and e’.

Step 2: Arrange encrypted message as r blocks.

Step 3: Calculate with cipher text using Private key and d.

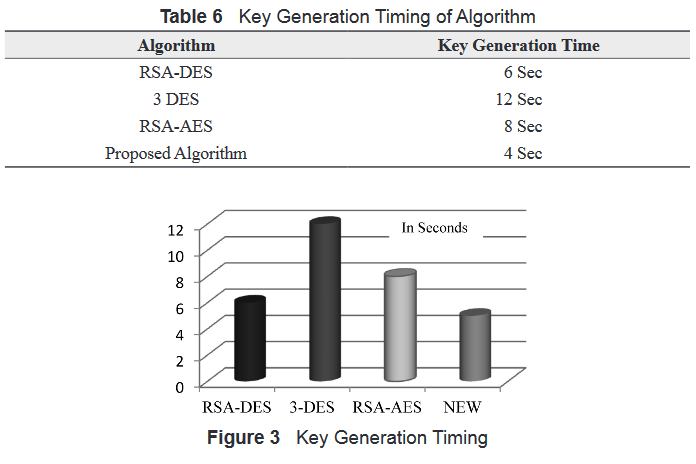
Step 4: Make modulo 37 with calculated message. The remainder value is called Plain Text.

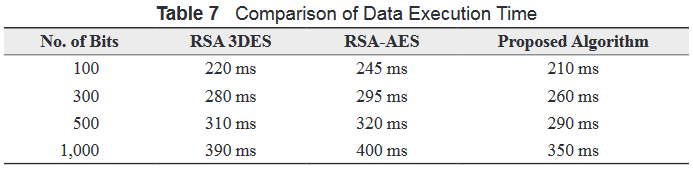
Step 5: Now we use modulation with calculated value the remainder text is called our Plain Text.

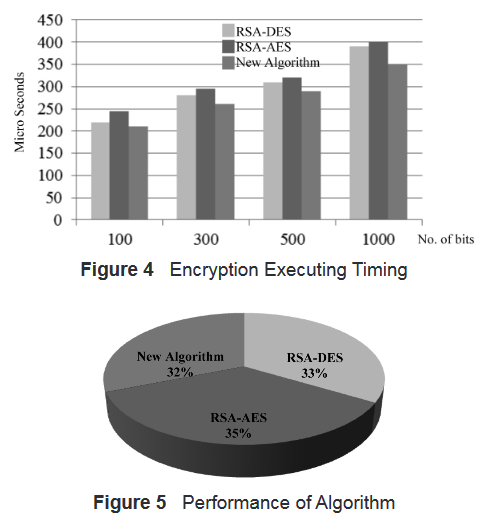
**Result & discussion**

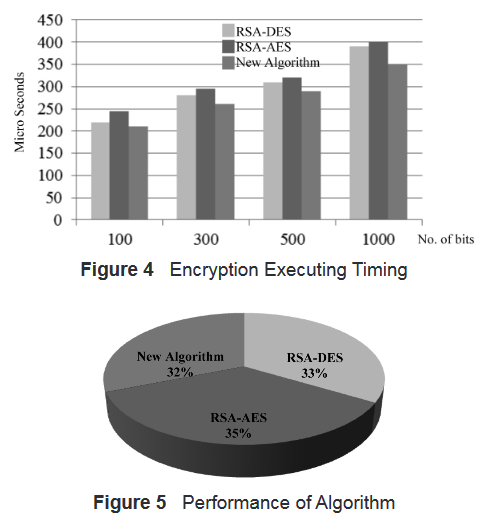
The encryption/decryption algorithm is compared on the basis of time consumption check which pair of algorithms is more efficient for hybrid encryption/decryption of messages. We have taken various different message lengths are used and results are drawn as shown in the following Table 6. Figure 3 shows 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.









**Conclusion**

The encryption and decryption of any data has a secure key, which is used for data encryption. For this purpose asymmetric key is used. This work secures the data, using linear block cipher algorithm. The block cipher algorithm is more efficiently using in symmetric encryption technic. The result of the proposed research plan shows that processing time is more efficient other algorithm. Thus AES algorithm along with the use of RSA algorithm for key management will provide an efficient technique to ensure the security of transmitted data. The security RSA AES better than RSA-DES and our proposed algorithm is efficient than RSA AES during the application of data transmission. Finally we illustrated the new directions for the future research. We can develop the derivatives of outburst attack. Thus the proposed Hybrid Encryption Algorithm using Block cipher and symmetric key provides a more secure and convenient technique for secure data trans-mission for all kind application.

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.

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".

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](http://www.schneier.com/paper-keylength.html).

**References**

* Elminaam, D.S.A., Kader, H.M.A. and Hadhoud, M.M. (2010), ‘Evaluating the performance of symmetric encryption algorithms’, International Journal of Network Security, Vol. 10, No. 3, pp. 213-219.
* Gupta1, R.K. and Parvinder, S. (2013), ‘A new way to design and implementation of hybrid crypto system for security of the information in public network’, International Journal of Emerging Technology and Advanced Engineering, Vol. 3, No. 8, pp. 108-115.
* Janssen, C. (n.d.), ‘Hybrid encryption’, available at http://www.techopedia.com/definition/1779/hybrid-encryption (accessed 22 November 2014).
* Kuppuswamy, P. and Al-Khalidi, S.Q.Y. (2012), ‘Implementation of Security through simple symmetric key algorithm based on modulo 37’, International Journal of Computers & Technology, Vol. 3, No. 2, pp. 335-338.
* Kuppuswamy, P. and Chandrasekar, C. (2011), ‘Enrichment of security through cryptographic public key algorithm based on block cipher’, Indian Journal of Computer Science and Engineering, Vol. 2, No. 3, pp. 347-355.
* Ramaraj, E., Karthikeyan, S. and Hemalatha, M. (2009), ‘A design of security protocol using hybrid encryption technique’, International Journal of the Computer, the Internet and Management, Vol. 17, No. 1, pp. 78-86.
* Shaar, M., Saeb, M., Elmessiery, M. and Badawi, U. (2003), ‘A hybrid hiding encryption algorithm (HHEA) for data communication security’, Proceedings of 2003 IEEE 46th Midwest Symposium on Circuits and Systems, Cairo, Egypt, pp. 476-478.
* Tat Wi, C. (2010), ‘Implementation of hybrid encryption method using Caesar cipher algorithm’, Unpublished master thesis, University Malaysia Pahang (UMP), Pahang, Malaysia