A New Security Protocol using Combination of Symmetric, Asymmetric Cryptography Algorithm and Hash Algorithm in Parallelism

Brijeshkumar Patel[1] Indrjeet Rajput[2]
[1]M.E Student [2]Assistant Professor
[1,2]Computer Engineering Department
[1,2]Hasmukh Goswami College of Engineering, Vehlal Ahmedabad

Abstract— Cryptography is that discover and study of methods and procedures for secure communication within the existence of third parties. There is a great number of techniques used in order to achieve the integrity, availability and data protection to secure information. This paper will present a viewpoint on the current state of play in the field of cryptography algorithms. Cryptography offers a lot of techniques which nowadays are difficult to fail. It is a hybrid encryption method where AES, T-DES, RC2 and BLOWFISH are combined to provide data encryption. RSA algorithm is considered for authentication and (HMACSHA256) for integrity. In this paper, results show that the proposed cryptographic algorithm gives better security and better performance in terms of computation time and the size of cipher text.

Key words: Cryptography, AES, TDES, Blowfish, RC2, RSA, HMACSHA256

I. INTRODUCTION

In presence, Internet has turned into a convenient way for data transmission due to a rapid development; ease of use and of modern technology. Cryptography [1] is a technique to scramble confidential information to make it "unreadable." It is commonly used in Internet communications to transmit data in secure way. Some potential problems during data communication on networking like unauthorized access, disclosure, interruption, use, modification, inspection, recording or destruction. The main ideas that a security system has to respect are: confidentiality, data integrity, availability and authentication. These concepts characterize the data security achievement and must be accomplished by every secure communication that aims to be functional. Most security systems use cryptography because it offers various algorithms and techniques practically impossible to break because of their complexity [2]. Cryptography, not only secure data from unauthorized access or modification, but it can also be used for user authentication. In this paper we present two main types of cryptographic algorithms used to achieve these goals: symmetric key (or secret) cryptography, asymmetric(or public-key) cryptography. After we present each of different algorithms with their weakness and strength we will summarize the main attacks that an efficient security system has to solve in each case.
Ease of Use

A. Basic Terms Used in Cryptography:

1) Plain Text :
The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. e.g.., Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.

2) Cipher Text:
The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into unreadable message before the transmission of actual message. e.g..,"Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".

3) Encryption:
A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure network. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

4) Decryption:
A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

5) Key:
A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw".

B. Purpose of Cryptography:

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

1) Confidentiality:
Information in computer is transmitted and has to be accessed only by the authorized person and not by anyone else.

2) Integrity:
Only the authorized person is allowed to alter the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

3) Non Repudiation:
Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.
4) Access Control:
Only the authorized person are able to access the given information.

C. Classification of Cryptography Algorithms

Cryptography Algorithm can be classified into two parts:

1) Symmetric Cryptography
This type of cryptography practices only one key for both encryption and decryption, and it is also called secret key cryptography [3]. This technique works by the following principles:

1) The plaintext is encrypted with the key to produce cipher text and it is sent to the receiver.
2) The receiver uses the same key to decrypt the cipher text and finds the original plaintext.

In Symmetric key cryptography both the sender and the receiver must know the same key in order to use the technique. There are two common patterns in this method stream cipher and Block cipher.

The stream ciphers generate a sequence of bits used as a key called a key stream, and the encryption is accomplished by combining the key stream with the plaintext. This is usually done with the bitwise XOR operation. The key stream is not dependent on the plaintext and cipher text, in which case the stream cipher is synchronous, or it can depend of the data and its encryption, in which case the stream cipher is self-synchronizing. A block cipher converts a fixed-length block of plaintext into a block of cipher text which is of the same length. In decryption, same secret key is used by applying the reverse transformation of the cipher text block and original plain text is produced[4].

2) Asymmetric (Public Key) Cryptography (PKC):
This technique requires two types of keys: one to encrypt the plaintext and one to decrypt the cipher text, and it doesn't work without one or another. It is called asymmetric cryptography because it is used a pair of keys: one is the public key that can be advertised by the owner to whoever he wants, and the other one is the private key and it is known only by the owner. The most common public key algorithm is the RSA algorithm, used for key exchange, digital signatures, or encryption of small blocks of data. It uses a variable size key and a variable size encryption block. The security of the RSA algorithm is based on the factorization of very large numbers. Two prime numbers are generated by a special set of rules, and the product of these numbers is a very large number, from which it derives the key-set [5].

D. Classification of Cryptography Techniques

Cryptography technique can be classified into two technique- Substitution and transposition technique. There are two techniques of encryption: Substitution Technique and Transposition Technique.

In substitution technique, the letters of plain text are replaced by other character or any number or by symbols. e.g.., Caesar cipher, hill cipher, monoalphabetic cipher etc.

In transposition technique, some sort of permutation is performed on plaintext. e.g.., rail fence method, columnar method etc.

II. Prepare Overview Of Cryptography Algorithms for Data Security

The given below are the five basic encryption algorithms:

- Triple DES
- AES
- Blowfish
- RC2
- RSA
- HMACSHA256

A. Triple DES:

In case of DES,Encryption key size was only 56bits this key size of 56 bits was generally enough when that algorithm was designed, because of increasing computational complexity brute force attack is Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.Triple DES is the modification of DES. It performs DES thrice. It is also a block cipher having three keys each of 56 bits and all are independent.

B. AES:

AES works on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. It operates on a 4×4 column-major order matrix of bytes, identified as the state, although some versions of Rijndael have a larger block size and have additional columns in the state. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The numbers of cycles of repetition are as follows:

1) 10 cycles of repetition for 128-bit keys.
2) 12 cycles of repetition for 192-bit keys.
3) 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

A round for the AES algorithm consists of four operations: the Sub Bytes operation, the Shift Rows operation, the Mix Columns operation, and AddRoundKey operation. The Sub Bytes operation substitutes bytes independently, in a black-box fashion, using a nonlinear substitution table called the S-box The Shift Rows Operation

1) The ShiftRows operation shifts the last three rows of the state cyclically, effectively scrambling row data
2) The MixColumns operation has the purpose of scrambling the data of each column. This operation is done by performing a matrix multiplication upon each column vector

3) The AddRoundKey operation determines the current round key from the key schedule, where the register arg0 serves as the argument. As an optimization we can also combine the MixColumns and AddRoundKey operations.
4) The final round has no MixColumns operation.

C. Blowfish:

Blowfish is symmetric block cipher encryption There are two parts to this algorithm;

1) A part that handles the expansion of the key.
2) A part that handles the encryption of the data.

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It consist of 16-round Feistel cipher and uses large key-dependent fixed S-boxes. The expansion of the key: break the original key into a set of different subkeys. The encryption of the data: 64-bit input is denoted with an x, while the P-array is denoted with a Pi (where i is the iteration).Security of data with blowfish Cipher is excellent.

D. RC2:

RC2 is a 64-bit block cipher with a variable size key. Its 18 rounds are arranged as a source-heavy unbalanced Feistel network, with 16 rounds of one type (MIXING) punctuated by two rounds of another type (MASHING). A MIXING round consists of four applications of the MIX transformation.

E. RSA:

RSA is one of the first practicable cryptographic algorithm and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997.[8]

A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.[8]

Breaking RSA encryption is known as the RSA problem. It is an open question whether it is as hard as the factoring problem.

The keys for the RSA algorithm are generated the following way:

1) Choose two distinct prime numbers p and q.

1) For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Compute n = pq.
2) n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

– Compute $\varphi(n) = (p-1)(q-1) = n - (p+q-1)$, where φ is Euler's totient function.
– Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
– e is released as the public key exponent.
– e having a short bit-length and

3) Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

– This is more clearly stated as: solve for d given $d=e \equiv 1 \pmod{\varphi(n)}$
– This is often computed using the extended Euclidean algorithm. Using the pseudocode in the Modular integers section, inputs a and n correspond to e and $\varphi(n)$, respectively.
– d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

F. HMACSHA256:

HMAC-SHA-256-128 is a secret key algorithm. While no fixed key length is specified in [HMAC], for use with either ESP or AH a fixed key length of 256-bits MUST be supported. Key lengths other than 256 bits MUST NOT be supported (i.e. only 256-bit keys are to be used by HMAC-SHA-256-128). A key length of 256-bits was chosen based on the recommendations in [HMAC] (i.e. key lengths less than the authenticator length decrease security strength and keys longer than the authenticator length do not significantly increase security strength).

III. The Proposed Cryptography Protocol

A. Encryption Phase:

The Encryption phase is shown in Fig. 1. The plaintext is divided into four parts.

The first part are encrypted using (AES and RSA) encryption algorithm. RSA algorithm is used for protecting secret key which is highest secure public key algorithm. Moreover, according to the mathematical problem on which RSA can be solved by fully exponential rather than sub exponential for other public key systems, RSA needs smaller key size than other algorithms and that refers to less memory size. It allows the communication nodes to handle a larger number of requests with the smallest number of dropped packet. Since that RSA consumes more power than symmetric algorithm using AES algorithm reduces the power consumption and raises the system performance. When using AES with RSA, we are able to save power, and achieve speed up to 25% for encryption and nearly 20% for decryption.

In parallel, the second part are encrypted using (T-DES and RSA) algorithm. Than in parallel third part are encrypted using (Blowfish and RSA) In parallel, the remaining fourth part are encrypted using RC-2 and RSA algorithm.

HMACSHA is applied to the cipher texts. It is the best performance of hashing function security.

1) D1 = HMACSHA256 (c1)
2) D2 = HMACSHA256 (c2)
3) D3 = HMACSHA256 (c3)
4) D4 = HMACSHA256 (c4)

At the final stage of the encryption process, the four parts are integrated to generate cipher text . The corresponding Hash values for each one are concatenated and sent to the sink node at the same time.

1) C = C1+ C2+C3+C4
2) D = D1 + D2+D3+D4.

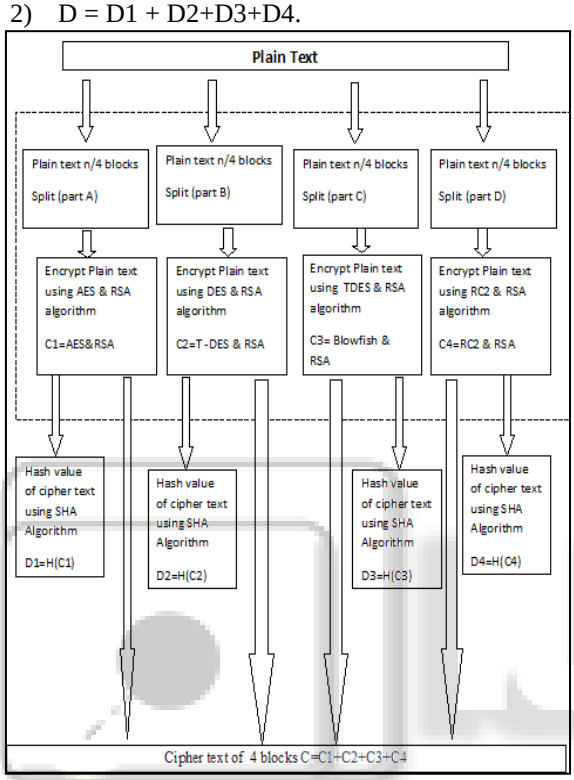

Fig. 1: Encryption Phase

B. Decryption Phase:

The decryption phase is shown in Fig. 2. The cipher text is divided into four parts .Hashing is used in order to identify whether the sink node receive the same cipher text or not. In the proposed protocol, if the Hash values in both phases are compared. If they are the same, then the protocol will proceed the decryption phase. Else, it will discard the message.

In the case of the hash values are the same at the source and
sink nodes, the first part are decrypted using AES and RSA algorithms.

The remaining three parts are decrypted using T-DES and RSA algorithm, Blowfish and RSA algorithm, RC-2 and RSA respectively. At the final stage of the decryption process, the four parts are integrated to produce plain text.

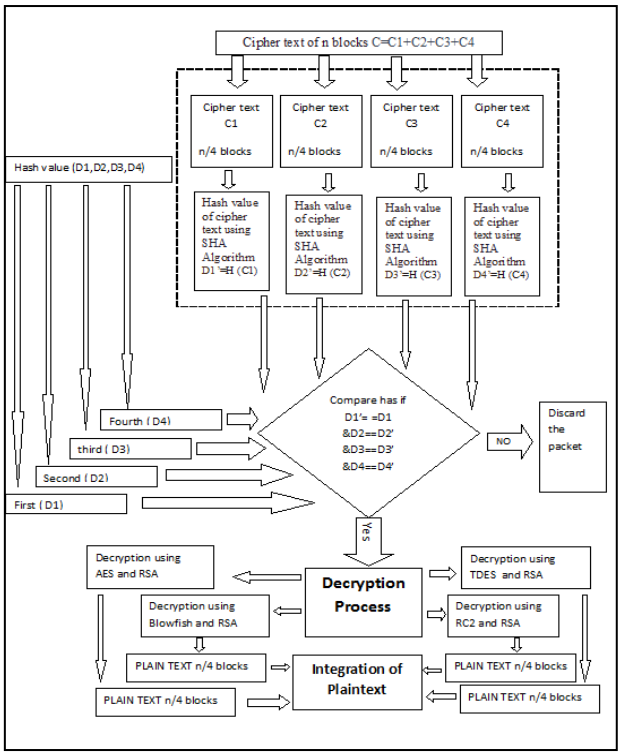

Fig. 2: Decryption Phase

IV. CONCLUSION

In this paper, solve several problems as practical implementation, short response time, efficient computation and the strength of cryptosystem. The proposed protocol tries to trap the intruder by splitting the plaintext and then applies four different techniques. The combination of different cryptography algorithms provide a maximized efficiency, correcting or compensating each other's weaknesses. The hybrid security protocol architecture is as such it can be easily upgraded and hence the protocol becomes more immune against the attacks and at the same time it becomes more time efficient. In the proposed algorithm, by analyzing the sequence of bit patterns; it is impossible for the intruder to identify which type of encryption algorithm. The attractiveness of the proposed protocol, compared to other existing security protocols, is that it appears to offer better security for a shorter encryption and decryption time.

REFERENCES

[1] Behroz A. Forouzan, "Cryptography & Network Security", McGraw Hill Publication,2008, New Delhi.
[2] Georgiana Mateescuc, Marius Vladescu "A Hybrid Approach of System Securityfor Small and Medium Enterprises: combining different Cryptography techniques", Federated Conference on Computer Science and Information Systems pp. 659–662,IEEE 2013
[3] Gary C. Kessler, An overview of Cryptography, 28 April 2013http://www.garykessler.net/library/crypto.html
[4] RSA Laboratories- Chryptographic tools; section 2.1.5.

unpublished;http://www.rsa.com/rsalabs/node.asp?id=2174

[5] Ing. Cristian MARINESCU, prof.dr.ing. Nicolae ŢĂPUŞ ; "An Overview of the Attack Methods Directed Against the RSA Algorithm"; Revista Informatica Economica, nr. 2(30)/2004

[6] Othman O. Khalifa, MD Rafiqul Islam, S. Khan and Mohammed S.Shebani, "Communication Cryptography",2004 RF and Microwave Conference, Oct 5-6, Subang, Selangor, Malaysia.

[7] G. Fang and H. Liu, "The research of database encryption based on hybrid cipher system", Journal of Harbin University of Science and Technology, 2008,13(5): 33-35.

[8] Rivest, R.; Shamir, A.; Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems".Communications of the ACM 21 (2): 120–126.

[9] Robinson, Sara (June 2003). "Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders". SIAM News 36(5).

