Network based Security model using Symmetric Key Cryptography (AES 256– Rijndael Algorithm) with Public Key Exchange Protocol (Diffie-Hellman Key Exchange Protocol)

Nitin K. Jharbade[†] and Rajesh Shrivastava[††]

[†]ME(IV Sem) Computer Science, SRIT Jabalpur , Rajeev Gandhi Technical University Bhopal MP, India
[††]HOD, Computer Science, SRIT Jabalpur, Rajeev Gandhi Technical University Bhopal MP, India

Summary
The main aim of this paper is to strengthen secured communication over the Network by enhancing the strength of the AES algorithm with Diffie-Hellman key exchange Protocol. The Rijndael is a block cipher with variable block and key size is believed to provide much more security. The Rijndael with 128 bit block size is adopted as the Advanced Encryption Standard (AES) in 2001 and has become widely used in the bulk data encryption.The security strength of the AES algorithm can be enhanced by increasing the key length to 256 bit and thereby increasing the number of rounds in order to provide a stronger encryption method for secure communication. For the secured communication over network, AES can be more strengthen by Diffie-Hellman Key Exchange Protocol which allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

Key words:
AES, Rijndael,Diffie-Hellman,Primitive root,MIM.

1. Introduction

As the Privacy and Network Security issues are growing at rapid pace, due to the wide internet and local area network penetration, the algorithm involved must be reliable,fast and secured. In order to implement a comprehensive security plan for a given network and, thus, guarantee the security of a connection, the following services must be provided which are the major concerns of security.

(i) *Confidentiality:* Information cannot be observed by an unauthorized party. This is accomplished via public key and private-key encryption.
(ii) *Data Integrity:* Transmitted data within a given communication cannot be altered in transit due to error or an unauthorized party. This is accomplished via the use of hash functions and Message Authentication Codes (MACs).
(iii) *Authentication:* Parties within a given communication session must provide certifiable proof of their identity. This is accomplished via the use of digital signatures.
(iv) *Non-repudiation:* Neither the sender nor the receiver of a message may deny transmission. This is accomplished via digital signatures and third party notary services.

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information and is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits [7]. AES was introduced to replace the Triple DES (3DES) algorithm used for a good amount of time universally. Though, if security were the only consideration, then 3DES would be an appropriate choice for a standardized encryption algorithm for decades to come. The main drawback was its slow software implementation.For reasons of both efficiency and security, a larger block size is desirable. Due to its high level security, speed, ease of implementation and flexibility, Rijndael was chosen for AES standard in the year 2001 [8].

Authenticated Diffie-Hellman key exchange allows two parties communicating over a public network, and each holding public/private keys, to agree on a shared secret value.

In this paper a network based security model is praposed which bundles AES-256 Rijndael algorithm for strong encryption and Deffi-Hellman key exchange protocol for generation of shared secret key which is used in AES-256 as a secret round key.

2. Rijndael Algorithm

The Rijndael AES algorithm uses a symmetric key block cipher both in encryption and decryption. A prime feature of Rijndael is its ability to operate on varying sizes of keys and data blocks. It provides extra flexibility in that both the block size and the key size may be 128, 192, or 256 bits. As Rijndael specifies three key sizes, there are approximately 3.4 x 1038 possible 128-bit keys, 6.2 x

Manuscript received August 5, 2012
Manuscript revised August 20, 2012

1057 possible 192-bit keys and 1.1 x 1077 possible 256-bit keys. At the start of encryption, input is copied to the State array. The encryption algorithm encrypts one block of data at a time to produce the encrypted data block with the use of a secret key. The decryption is simply the reverse process of the encryption, and each operation is the inverse of the corresponding one in encryption. The data block length is fixed to 128 bits, while the key length can be 128, 192, or 256 bits[7]. Each data block is rearranged in a matrix form. AES algorithm is an iterative algorithm and each iteration is called a round. The number of bytes in a row of key length is given by.

$$N = L / (8 \; x \; Br)$$

where, N is the number of bytes, L is the block length in bits, and $\boldsymbol{Br}$ is the number of rows in a state array matrix. Each round is iterated 10 times for a 128-bit length key, 12 times for a 192-bit key and 14 times for 256 bit key with 4, 6 and 8 bytes in a row of key lengths respectively. Each round uses four transformations and inverses but final round excludes *MixColumn* transformations. To encipher a block of data in Rijndael an Add Round Key step is performed (XORing a subkey with the block) by itself, then the regular transformation rounds, and then a final round with the Mix Column step omitted. The cipher itself is defined by the following steps:

- an initial Round Key addition;
- Nr-1 Rounds;
- a final round.

Following Figure shows the flow of AES Encryption algorithm.

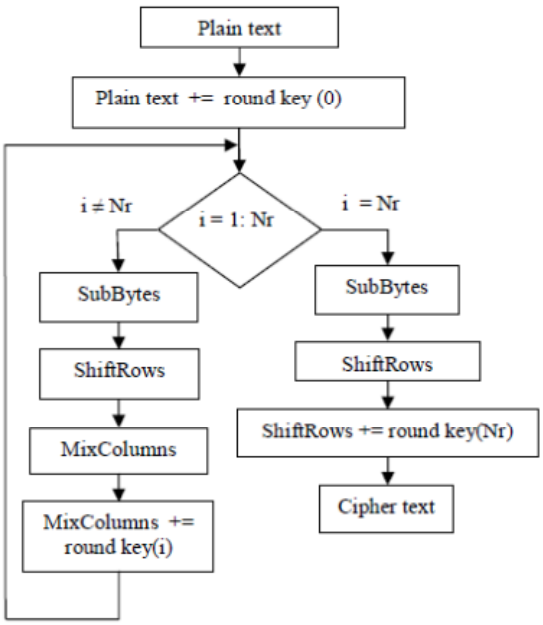

Fig. 1 AES Encryption Algorithm.

The four transformations used in each round are:

(i) *SubBytes* : Every element of State array is first inverted and processed through an affine transformation. SubBytes transformation is performed on each byte of the State array. In most of the practical applications SubBytes is calculated in advance and stored in a look-up table called S-box of $2^8 = 256$ elements.

(ii) *ShiftRows* : The rows in State array are rotated. The byte in first row is not shifted whereas second, third and fourth row is shifted left by one byte cyclically.

(iii) *MixColumns*: MixColumns is a linear transformation and is done on the State array by column by column. Each transformed byte is a linear combination of the state matrix.

(iv) *AddRoundKey*: Every 128-bit round key is divided in to 16 bytes as of data block. *AddRoundKey* is a linear transformation. A round key is added to the State array by bitwise Exclusive-OR (*XOR*) operation.Key is used as initial set of bytes in each row and the rest of the bytes are generated from the key iteratively.

As main advantages of Rijndael we can mentioned:

(i) simplicity of design (the cipher does not base its security on obscure and not well understood interactions between arithmetic operations);

(ii) variable block length (the block lentgs of 192 and 256 bits allows the construction of a collision-resistant iterated hash function using Rijndael as the compression function);

(iii) the possibility of extensions (although the number of rounds is fixed in the specifications, it can be increased as a parameter in case of security problems.

(iv) a secured encryption/decryption system(the expanded key is always derived from the cipher key).

3. Deffi-Hellman Key Exchange

The Diffie-Hellman algorithm, introduced by Whitfield Diffie and Martin Hellman in 1976, was the first system to utilize “public-key” or “asymmetric” cryptographic keys. The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms. Briefly we can define the discrete logarithms in the following ways. First, we define a primitive root of a prime number p as one whose power generates all the integers from 1 to p-1. That is, if a is a Primitive root of the prime number p, then the numbers

$$a \bmod p \; , \; a^2 \bmod p, \ldots\ldots\ldots\ldots\ldots a^{p-1} \bmod p$$

are distinct and consists of the integers from 1 through p-1 in some permutation.

For any integer b and a primitive root a of prime number p, we can find a unique exponent i such that

$$b = a^i \bmod p \text{ where } 0 \leq i \leq (p-1)$$

The exponent i is refereed to as the discrete logarithm, or index, of b for the base a mod p. This value is denoted as ind_{ap} (b) [9].

With this background we can define the Diffie-Hellman Key exchange. For this Scheme there are two publicly known numbers: a prime number P and an integer G that is the primitive root of P. Suppose the users A and B wish to exchange a key. User A selects a random Integer X_A<P and computes $Y_A = G^{XA} (mod(P))$.

Similarly, user B independently selects a random integer X_B and computes $Y_B = G^{XB} (mod(P))$. Each Side keeps the X value private and makes the Y value public to the other side. User A computes the key as Key = $Y_B^{XA} (mod(P))$ and user B computes the key as Key = $Y_A^{XB} (mod(P))$. the two Calculations produce identical results:

Key(A) = $Y_B^{XA} (mod(P))$

= $(G^{XB} (mod(P)))^{XA} (mod(P))$

= $G^{XB\,XA} (mod(P))$ ...

by the rules of modular arithmetic

= $(G^{XA} (mod(P)))^{XB} (mod(P))$

= $Y_A^{XB} (mod(P))$

= Key(B)

The result is that the two sides have exchanged a secret key. Furthermore, because X_A and X_B are private, an opponent has the following ingredients to work with: P, G, Y_A, and Y_B. Thus the opponent is forced to take a discrete logarithm to determine the keys.

Follwing table shows key exchange process between two sides A and B.

Table 1: Process D-H Key Exchange

A	B
A and B exchange a Prime (P) and Generator (G) in clear text such that P>G and G is primitive root of P	A and B exchange a Prime (P) and Generator (G) in clear text such that P>G and G is primitive root of P
A generates a random number X_A	B generates a random number X_B
$Y_A = G^{XA} (mod(P))$	$Y_B = G^{XB} (mod(P))$
A receives Y_B in clear text	B receives Y_A in clear text
Key=$Y_B^{XA} (mod(P))$	Key= $Y_A^{XB} (mod(P))$

Diffie-Hellman protocol has ability to have a Certificate Authority that the public key is indeed coming from the source only. The purpose of this certification is to prevent Man In the Middle (MIM) attacks. The attack consists of someone intercepting both public keys and forwarding bogus public keys of their own. The “man in the middle” potentially intercepts encrypted traffic, decrypts it, copies or modifies it, re-encrypts it with the bogus key, and forwards it on to its destination. If successful, the parties on each end would have no idea that there is an unauthorized intermediary. Properly implemented Certificate Authority systems have the potential to disable the attack[4].

4. New Network Based Security Model

The National Security Agency (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for U.S. Government non-classified data. In June 2003, the U.S. Government announced that AES may be used to protect classified information:

“The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use”[1]. AES with 256 bits keys has the highest security margin among three standard AES variants[3].

In AES Rijndael algorithm, the number of rounds involved in the encryption and decryption depends on the length of the key and the number of block columns[2].The security strength of the AES algorithm can be enhanced by increasing the key length to 256 bit and thereby increasing the number of rounds in order to provide a stronger encryption method for secure communication over network. Adding more rounds to Rijndael may be increase the security margin to protect from new attacks [6]. The longer the key length, the more secure is the key. Using larger key length, makes more possible keys to search, which makes the algorithm to be more secure. AES has larger key length and has been efficiently implemented both in hardware and software [5].

The Security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate the exponentials modulo a prime,it is very difficult to calculate discrete logarithms. for large primes the later task is considered infeasible [9].

Following figure shows new network based security model which uses deffi-hellman key exchange protocol for sharing secret key between two sides and the same secret

key generated is further used in AES-256 for key generation.

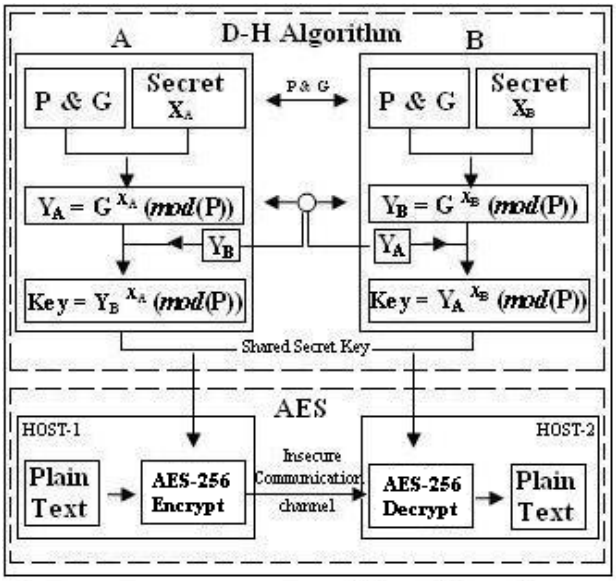

Fig. 2 New network based security model.

The process begins when each side of the communication generates a private key.Each side then generates a public key which is a derivative of the private key . The two systems then exchange their public keys. Each side of the communication now has their own private key and the other systems public key.

Once two communicating parties shares the same secrete key generated by Deffi-Hellman Key Exchange Protocol, the same secret key can be used in the AES encryption/decryption process as the round key initially.

In most real applications of the Diffie-Hellman protocol (IPSec in particular), the shared secret encrypts a symmetric key for one of the symmetric algorithms, transmits it securely, and the distant end decrypts it with the shared secret. Because the symmetric key is a relatively short value as compared to bulk data, the shared secret can encrypt and decrypt it very quickly. Speed is not so much of an issue with short values[4].

5. Conclusion

AES is a cryptographic algorithm that can be used to protect electronic data. Its security has attracted cryptographist's attentions. AES with 256 bits keys has the highest security margin among three standard AES variants. Adding more rounds to Rijndael may be increase the security margin to protect from new attacks [6]. The methods of new attacks welled show the weaknesses of AES algorithm. When the number of rounds is increased, it improves the complexity of the algorithm making it strong against the cryptographic attacks. The length of the key is increased in order to increase the number of rounds involved as number of rounds depend on the length of the key used. Thus the increase in length of the key gives the AES algorithm strong resistance against the new attacks and has an acceptable speed of data encryption and decryption.

Diffie – Hellman Key Exchange protocol provides flexibility in usage over network, though which a secured session can be maintained in the network. The prototype of this protocol can be enhanced so as to make it as a standard protocol and can be adopted in entity authentication. AES is found to be the strongest standard to provide security in network. In our prototype AES performs at the back end and gives an efficient service in encrypting and decrypting of plain text.

As this prototype is implemented using Diffie – Hellman Key Exchange Protocol and AES, Some of the features that can be analyzed are as follows:

(i) As the prototype is using AES – Rijndael Algorithm, no doubt it is strong in cryptographic compared to any other cryptographic algorithms.

(ii) Diffie – Hellman Key Exchange Protocol, which is considered to be an efficient protocol for exchanging the keys between client and server, the prototype, provides an efficient key exchange mechanism.

(iii) The prototype is simple and easier to design but the same is opposite on the other hand if the case of breaking is considered.

(iv) The cryptographic process takes very negligible time; it is of order 10^{-12}.

Rijndael limited by its inverse cipher. Though the encryption is suited for many network based applications and is quite fast, the inverse cipher takes more code and cycles is not as well suited for different implementations, such as a smart card.Presently it is an event driven prototype, and can be made as a protocol of standard type by meeting the standards of the protocol. Presently it can be communicate with terminal which has been mentioned in the socket, it can be made as standard so as to communicate any terminal in the network. The prototype can be updated as a protocol by implementing three way handshaking Mechanism, so that it can communicate with any terminal in the network. In all way it can be made as a standard protocol by meeting standards of protocol and can be used efficiently in a network for communication.

References

[1] CNSS Policy No. 15, Fact Sheet No. 1 National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information(june 2003)

[2] Joan Daemen and Vincent Rijmen. "The Design of Rijndael: AES - The Advanced Encryption Standard". Springer, 2002.
[3] LIU Niansheng, GUO Donghui, and HUANG Jiaxiang "AES Algorithm Implemented for PDA Secure Communication with Java", 1-4244-1035-5/07/$25.00.2007 IEEE.
[4] Keith Palmgren, "Diffie-Hellman Key Exchange – A Non-Mathematician's Explanation",02/02/2005. http://www.securitydocs.com/library/2978.
[5] Burr and William E.,"Selecting the advanced encryption standard", *IEEE Security and Privacy*, vol. 1(2), p 43-52,2003.
[6] N. Ferguson, J. Kelsey, S. Lucks, et al. "Improved cryptanalysis of Rijndael," *Lecture Notes in Computer Science*,vol. 1978, pp.213-230, Berlin: Springer-Verlag, 2001.
[7] Federal Information Processing Standards Publication 197, "Announcing The Advanced Encryption Standard (AES)", *November 2001*.
[8] N.Penchalaiah et. al. / (IJCSE) International Journal on Computer Science and Engineering. Vol. 02, No. 05, 2010, pp.1641-1645, 2010.
[9] William Stallings, "Network Security Essentials", 3rd edition, *Pearson Education Inc.* 2008 , pp.80-81,2008.

Nitin K. Jharbade received the B.E. degree in Electronics and Telecommunication Engineering from Rajeev Gandhi Technical University Bhopal (MP) India in year 2001. In year 2002 he completed his diploma in advance computing (C-DAC) from Soft-Polynomials Nagpur Maharashtra India . His research interest includes communication systems, computer networks, data structure and theire applications.

Rajesh Shrivastava received the M. C.A.,M.E. degrees from Rajeev Gandhi Technical University Bhopal (MP) India, in year 2003,2008 respectively. After working as a frofessor in the Dept. of M.C.A. in Shri Ram Institute of Engg. & Technology , he is now HOD,Computer Science with the same institution. His research interest includes Ad-hoc Networks and Compiler Design.