NOVEL HYBRID KEY EXCHANGE ALGORITHM

R. Pradeep Kumar Reddy[1], B. Ravindra Naik[2], T. Lokesh[3]

[1]*Assistant Professor Dept. of CSE, YSR Engineering College of YVU, (India)*

[2,3]*Student Dept. of CSE, YSR Engineering College of YVU, (India)*

ABSTRACT

Security is an important issue in communication in past there exist so many methods to provide security for the information. Diffie-Hellman is one of the effective algorithm to exchange the key between sender and receiver. But there exists a problem in Diffie-Hellman called as man-in middle attack. To ensure the security, present paper introduces a hybrid approach with the combination Caesar cipher with HMAC and Rail-fence to exchange the key between sender and receiver.

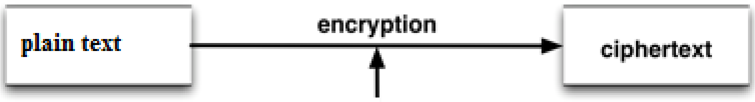
Keywords: Attack, Caesar Cipher, Communication, HMAC, Security.

I. INTRODUCTION

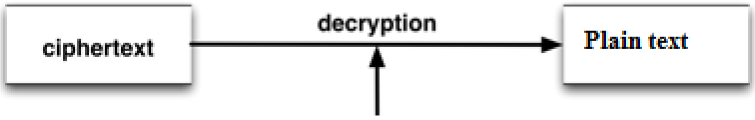
Cryptography:

Cryptography is a process that transforms normal text into unreadable form, further normal text is referred as plain text and unreadable is referred as cipher text. In the process of transferring data through the wireless or wired communication[2] channel there exists a security problem. To protect the information from the hackers cryptography introduces two mechanisms encryption and decryption.

Encryption: It is the process that is used to make a cipher, where the plaintext is transformed into unknown form



Decryption: It is a process that retrieves the actual data from the encrypted data.



To perform the encryption and decryption there exist two types of techniques known as Symmetric and Asymmetric cryptography. In Symmetric cryptography, there exists only one Key and it is shared by both sender and receiver to implement encryption and decryption process.

In asymmetric cryptography, there exist two keys public and private. Among the two keys public is visible to all whereas private is hidden from third party.

II. NETWORK SECURITY

Network Security[1,2] provides different important applications such as firewalls etc, for System business organizations, government Sectors. The main difficulty is take place in communication that they allows virus applications or program which are harmful for data. There are few mechanisms including cryptography and firewalls utilized by the various organizations for shielding data from the unauthorized access.

Network place a great role in exchange of information between one to other now a days wireless communication is used as a medium in communicating the information. Cryptography is a one of the concept which introduces security. The basic requirements for cryptography is

1. Integrity
2. Confidentiality
3. Non-repudiation.
4. Authentication

Confidentiality – The Confidentiality is a fixed of policies or a promise that limits get admission to or locations regulations on certain sorts of statistics.

Authentication – The authentication assets is used to affirm the statistics and become aware of information from the liaising parties.

Integrity – The integrity is classified into two types called as data integrity and system integrity. The data integrity that which consists of two types of threats they are passive and active threats and the system integrity is a state of a gadget wherein it's miles acting to support the features without being degraded or impaired by way of changes or disruptions in its inner or external environments.

Non-repudiation-The Non-repudiation guarantee that someone can’t deny something. Generally, non-repudiation refers potentiality to make sure that a celebration to a settlement or a verbal exchange can't deny the authenticity in their signature on a file or the sending of a message that they originated.

III. SYSTEM ANALYSIS

3.1 Existing System

The Diffie-Hellman[3] is the key exchange[1,4,5] algorithm introduced in 1976 by Diffie and Hellman, the advance version has been proposed in 2002, popularly known as Diffie-Hellman Merkle key exchange algorithm.

Steps for the Existing system:

A. The p and g are the two parties that is present in the algorithm as a parameter that agree with the aid of the parties.

B. The communication parties are generating a secret keys, that are not sharable by the third party, the a, b, and c are the private keys.

C. Dr.S.Kiran computes g^a and transfer to R.Pradeep.

D. R.Pradeep computes $(g^a)^b = g^{ab}$ and transfer to Dr.B.Reddiah.

E. Dr.B.Reddiah computes $(g^{ab})^c = g^{abc}$ and then use as a security key.

F. R.Pradeep computes g^b and the transfer to Dr.B.Reddiah.

G. Dr.B.Reddiah computes $(g^b)^c = g^{bc}$ and then transfer it to Dr.S.Kiran.

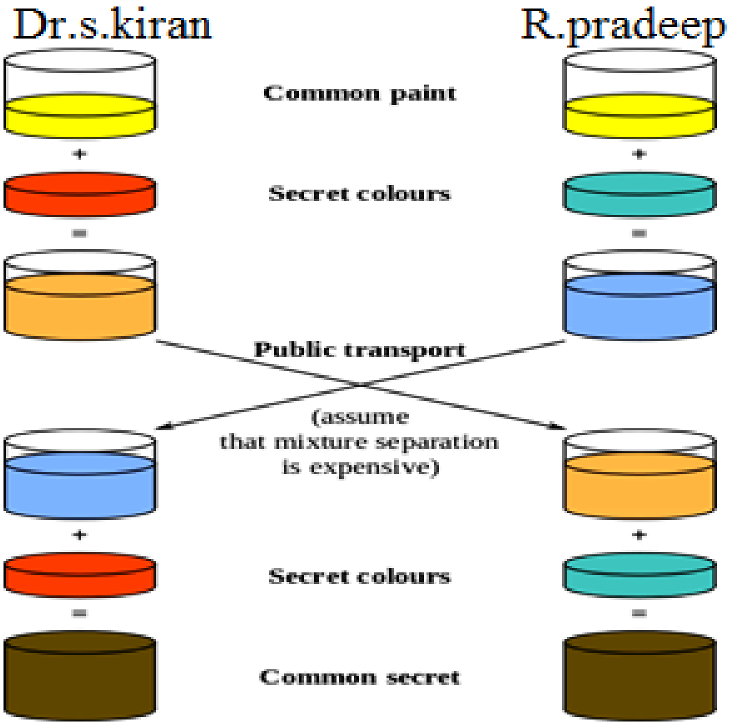
H. Dr.S.Kiran computes $(g^{bc})^a = g^{bca} = g^{abc}$ and the use as a security key.

I. Dr.B.Reddiah computes g^c and transfer to Dr.S.Kiran.

J. Dr.S.Kiran calculate $(g^c)^a = g^{ca}$ and transfer to R.Pradeep

computes $(g^{ca})^b = g^{cab} = g^{abc}$ and then uses resulted content as his secret.

Diffie and Hellman invented a technique for secret data sharing. The data is transfer with aid of wired or wireless devices with secure and hidden communication. The implementation of existing Diffie-Hellman uses set of rules and regulation in that influences on, integer groups, multiplicative modules, are defined in the given below.



Here p is prime number and g is primitive root mod p. The instance for protocols[6], the Boldface Red is secret number and the Blue color is used as non-secret number.

Dr.s.kiran				**R.Pradeep**		
Secret	Public	Computes	Sends	Computes	Public	Secret
J	p, g		p,g →			F
J	p, g, J	g^a mod p= J	J →		p, g	F
J	p, g, J		← F	g^b mod p = F	p, g, J, F	F
a, k	p, g, J, F	F^a mod p = k		J^b mod p = k	p, g, J, F	b, k

1. Dr.s.kiran and R.pradeep decide to use a prime p as 31 and base g as 6.
2. Dr.s.kiran wish to select secret value a as 5, then transfers to R.pradeep J = g^a mod p
   - J = 6^5 mod 31
   - J = 7,776 mod 31
   - J = 26
3. R.pradeep wish to select the secret value as b 14, then transfers to Dr.s.kiran F = g^b mod p
   - F = 6^{14} mod 31
   - F = 78,36,41,64,096 mod 31
   - F = 5
4. R.pradeep Calculate s = F^a mod p
   - k= 5^5 mod 31
   - k=3,125 mod 31
   - k = 25
5. Dr.s.kiran Calculate s = J^b mod p
   - k= 26^{14} mod 31
   - k= 6,45,09,97,47,03,29,71,50,976mod 31
   - k= 25
6. Dr.s.kiran and R.pradeep shares a common secret key s =25. This is because 14*5 is the same as 5*14. The third party who knows above integers able to calculate key as follows
   - k= 25^{5*14} mod 31
   - k= 25^{14*5} mod 31
   - k= 25^{70} mod 31
   - k=7.174648137343063403129495466444e+97 mod 31
   - k= 25

Dr.s.kiran and R.pradeep shares secret key as same because the $(g^a)^b$and as well as the $(g^b)^a$ number are equal mod p. The a, b and g^{ab}= g^{ba} mod p. The g, p and g^b mod p, g^a mod p are the values that doesn't need security. The Dr.S.Kiran and R.pradeep computes the secret key and then they both extract the information using their own keys.

Set of rules for exchanging the information are described below.

1. Dr.S.Kiran and R.Pradeep are both agree on a restricted cyclic group g is generated from G.
2. Then Dr.S.Kiran select a random number a and transfer g^{a} to R.Pradeep.
3. Then R.Pradeep select a random number b and transfer g^{b} it to Dr.S.Kiran.
4. Dr.S.Kiran Computes the $(g^{b})^{a}$.
5. R.Pradeep Calculates $(g^{a})^{b}$.
6. Dr.S.Kiran and R.Pradeep are both now in protection of group elements g^{ab} , which is used as sharable secret value. The groups $(g^{b})^{a}$ and $(g^{a})^{b}$ are identical results values for the purpose those groups are power associative.
7. To generate Plain text m from the cipher text then we need to send mg^{ab} , Dr.S.Kiran (or R.Pradeep) must compute $(g^{ab})^{-1}$ values first, as follows:
8. R.Pradeep knows |G|, b, and g^{a}. A result from group theory creates that from the structure of G, $x^{|G|} = 1$ ∀ x in G.
9. R.Pradeep then computes: $(g^{a})^{|G|-b} = g^{a(|G|-b)} = g^{a|G|-ab} = g^{a|G|}g^{-ab} = (g^{|G|})^{a}g^{-ab}=1^{a}g^{-ab}=g^{-ab}=(g^{ab})^{-1}$
10. When Dr.S.Kiran transfer value to R.Pradeep to generate plain text characters with the aid of mg^{ab} , R.Pradeep smears $(g^{ab})^{-1}$ and receive the original data with the aid of $mg^{ab}(g^{ab})^{-1} = m(1) = m$

Pitfalls:

a. The "Man-in-the-middle-attack-problem" is one of the main backdrop of Diffie-Hellman algorithm.

b. Denial of Service

Denial of service if one of the hacking technique that used to do by the unauthorized persons, going to send a bunch of requests to degrade the system the performance.

c. Spoofing Attacks

Spoofing is used for guessing the key by unofficial public to access the private information.

3.2 Proposed System

The main objective of the proposed system is to avoid the “Man in the middle attack problem”. This paper introduces “HYBRID METHOD” Caesar cipher along with MAC and Railfence to handle the backdrops of existing system.

CAESAR CIPHER ALONG WITH MAC FUNCTION:

Caesar cipher is one of the basic encryption and decryption technique and it is placed in the category of substation cipher mechanism. This technique is used to replace the actual plain text with other character but it is breakable. To increase the strength of Caesar cipher, MAC function is introduced, it adds additional strength to Caesar cipher. After applying a Caser cipher with MAC, further Rail fence is add to increase the strength of the cipher. The problem man-in-middle attack is solved with proposed method with better security.

MAC function

The acronym for MAC is Message Authentication Codes (MAC). The HMAC is the one that is standard among other MAC functions. In this HMAC function is used to carry out the public and private keys to manage the data transfers between the authorized persons. It is an hash-based MAC function that plots not only the message but also the secret key. HMAC function aids in providing the better generation or verification of the messages only by the authorized persons. The description terms that are used by HMAC function is

- K: this used as a secret value
- M: this is used as indicating the message
- H: this H is used to indicate the hash functions such as RIPEMD-160, MD5, SHA-1,etc.,
- b: this b is used as length of K+
- n: this n is used to indicate the length of the output from H. $n < b$
- K+ : If the b bits is longer than the secret key value, K+ = padding 0s || H(K).
  Otherwise, K+ = K || padding 0s.
- Ipadd: 01011010 reiterating b/8 times.
- Opadd: 00110110 reiterating b/8 times.
- HMACK(M) = H [(K+ $\oplus$ Opadd) || H[(K+ $\oplus$ Ipadd) || M]]
- In detail, (K+ $\oplus$ Ipadd) & (K+ $\oplus$ Opadd) can be pre-calculated to enhance efficiency since K+, Ipadd & Opadd are known in advance.

The proposed method is described below:

1. Both p and g elements are the secret values that generates the p and g values from the image.
2. Dr.S.Kiran selects a huge random element x from another image or same image such that $0 \leq x \geq p-1$ and computes N1=gx mod p.
3. R.Pradeep also selects a hung random value y from another image or same image □ $0 \leq y \geq p-1$ and computes N2=gy mod p.
4. Dr.S.Kiran transfers N1 to R.Pradeep. Likewise, R.Pradeep transfer N2 to Dr.S.Kiran.
5. Dr.S.Kiran computes K=(N2) x mod p.
6. R.Pradeep also compuetes K=(N1) y mod p.

EXAMPLE FOR CEASAR CIPHER

Normal text characters: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Encrypted text characters: Y N R O T K M C P B D V X Z A L E W U S F Q J H GI

Ex: - KIRAN // ORIGINAL characters

The generated cipher text "DPWYZ".

The deciphered text is "KIRAN" by means of the above encrypted text characters.

EXAMPLE FOR RAIL FENCE

Normal text characters: PRADEEP.

Encryption process: P A E P
R D E

Encrypted text: PAEPRDE //CIPHERED MESSAGE

Logic for text decryption:

	P A E P	
Round 1:	R D E	PAEPRDE
	P E R E	
Round 2:	A P D	PEREAPD
	P R A D	
Round 3:	E E P	PRADEEP

Decrypted text is: PRADEEP

IV CONCLUSION

In present era utilization of internet gradually increasing at the same time so many security threads are also increasing in other hand while transmitting the data through wired or wireless medium. To improve the security as well as conditionality in network the present paper proposes hybrid key exchange algorithm to avoid man in middle attack.

REFERENCES

1. Erdem Alkim, Ege University; Léo Ducas, Centrum voor Wiskunde en Informatica, "Post-quantum Key exchange-a new hope", ISBN 978-1-931971-32-4, (August 10–12, 2016).
2. Łukasz Wronkowski, Damian Kuniszewski ETAL "Send It Safe – A Novel Application for Secure Key Exchange Using Telecommunications Open Middleware APIs", Federated Conference on Computer Science and Information Systems, DOI: 10.15439/2014F319 ACSIS, Vol. 3, pp. 171–174 (2014).
3. Sunita, Neeraj Goyat, Annu Malik, "Review of Diffie–Hellman key Exchange" ISSN: 2277 128X Volume 3, Issue 7, (July 2013).
4. Sakthi Nathiarasan A, Yuvaraj K, "Secure Key Exchange Algorithm - Mathematical Approach" Volume 3, Issue 6, ISSN: 2277 128X, (June 2013).

5. ETH Zurich, Switzerland, "Key Exchange in IPsec revisited: Formal Analysis of IKEv1 and IKEv2" (2010).

6. Mohammad Ahmad Alia and Azman Bin Samsudin, "New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets", IJCSNS International Journal of Computer Science and Network Security VOL.7 No.2 (2007 February).