iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: II Month of publication: February 2022

DOI: https://doi.org/10.22214/ijraset.2022.40292

Customized AES Using Pad and Chaff Technique Diffie Hellman Key Exchange

Rushiil Nakka[1], M. Sai Krishna Teja[2], Dr. R. Lakshminarayanan[3]
[1, 2]SRM Institute of Science and Technology, Kattankulathur
[3]Assistant Professor, SRM Institute of Science and Technology, Department of Networks and Communications Kattankulathur

Abstract: In today's world, transferring or exchanging the information on a secure connection has become the most crucial part. Hence in order to have a safe/reliable connection it needs keys exchangement and also they should be transferred on a secure connection. Hence the data that is secured, when passed through the internet should be protected. Hence the data protection can be measured in two ways 1.Confidentiality - ensuring no one except the authorized users or admins can access the data. 2. Integrity - ensuring no one can alter while transferring. Hence Confidentiality, Integrity is achieved using Symmetric Encryption, Message Authentication Code(MAC). Hence in order to achieve these, identical and secret keys are required. For these reasons this algorithm is developed.

I. INTRODUCTION

Diffie-Hellman key exchange is an algorithm in which a secret key is generated between two people/parties such that the secret key is not known to other people. It is not sharing information, it is only generating a key. It is a cryptography keys method used in symmetric encryption(AES).The application will secure the data such that admin can decrypt it. Only admin who has the secret key only is permitted to access the secured data. Also, authorized user can access the data. Any unauthorized or third party cannot access the secured data. It identifies the private data and also the ability of quality data integration. The Diffie Hellman key exchange algorithm secures the data, cannot be accessed by any unauthorized user. This algorithm gives excellent results, but the input data should be given accurately.

II. LIST OF SYMBOLS AND ABBREVIATIONS

1) MAC - Message Authentication Code .
2) AES - Advanced Encryption Standard .
3) DH - Diffie Hellman .
4) RSA - Rivest, Shamir, and Adleman (Algorithm).
5) MITM - Man in the Middle Attack.
6) PK = G pow(a)(mod(P)) G- Generator Key , P- Prime Number , a - Private Key , PK- Public Key.
7) S1= Gda(mod P) d- Another Private Key , S1 - Common Secret Key

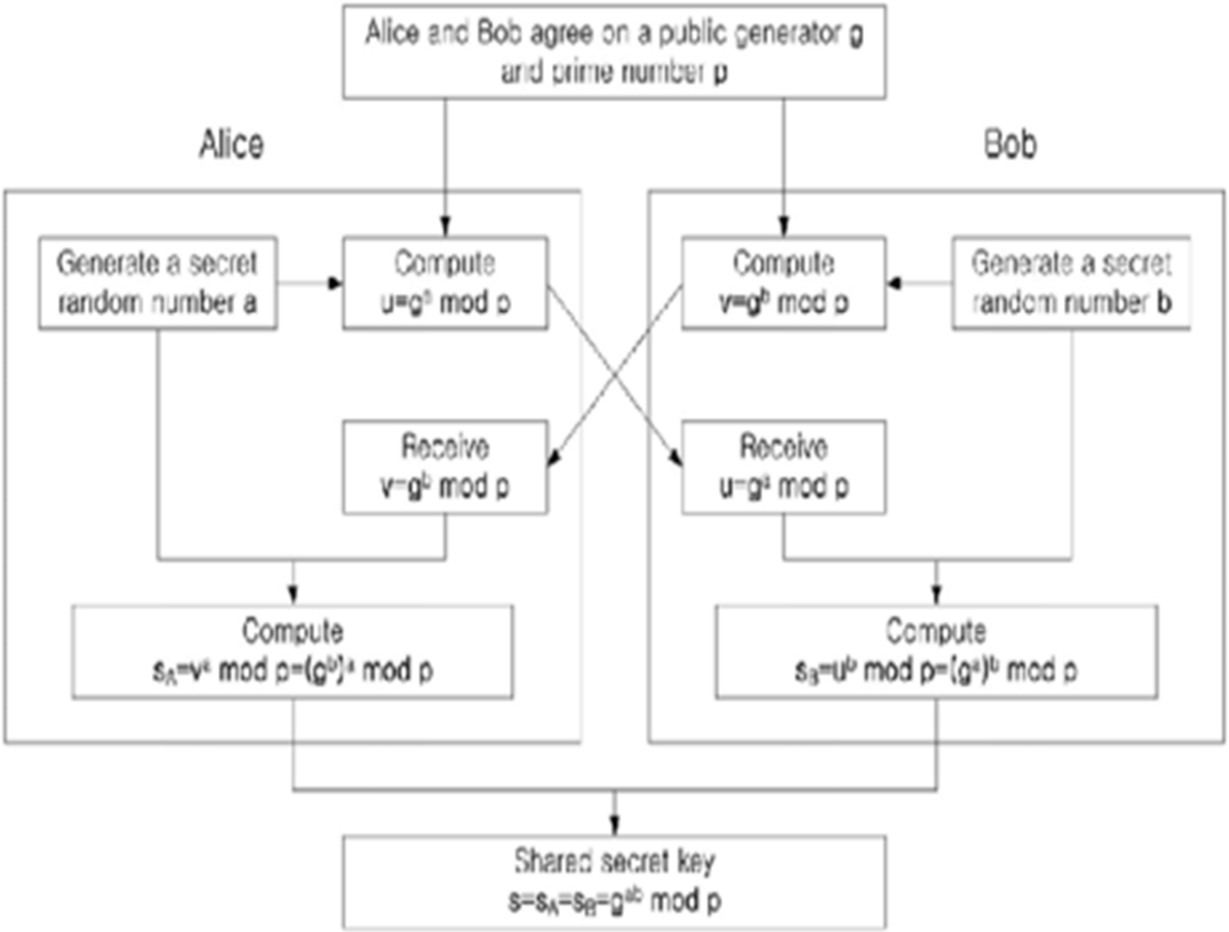
III. WORKING

Diffie Hellman key exchange is used to create secret keys. This algorithm can be understood clearly by taking an example-Imagine me and my friend standing in a crowded room. The task is to agree upon an identical number and that number shouldn't be known to other people in the room. In order to solve this challenge Diffie Hellman key exchange is used. This algorithm would help me and my opponent to exchange some random numbers, from which another identical number can be calculated. Even though the exchanged numbers are known to all the people in the room, they cannot determine the final number that is known to me and my friend. After implementing the diffie key exchange algorithm , secret keys are created. The additional benefit is creating keys by combining values. Security protocols (SSL/TLS etc) create keys for traffic security in each direction, a total of four keys (MAC + Encryption in one direction, MAC + Encryption in the other direction). These keys are derived from Diffie-Hellman.

Hence this secret key is combined with few other values, Encryption and MAC keys are generated.

1) Prime number - P
2) Generator of P - G

To Generate a Secret Key:
(G^Private key) MOD P.
The basic idea works like this:
$(g^a \bmod p)^b \bmod p = g^{ab} \bmod p$
$(g^b \bmod p)^a \bmod p = g^{ba} \bmod p$


Alice and Bob agree on a public generator g and prime number p
Alice
Bob
Generate a secret random number a
Compute $u=g^a \bmod p$
Compute $v=g^b \bmod p$
Generate a secret random number b
Receive $v=g^b \bmod p$
Receive $u=g^a \bmod p$
Compute $s_A=v^a \bmod p=(g^b)^a \bmod p$
Compute $s_B=u^b \bmod p=(g^a)^b \bmod p$
Shared secret key $s=s_A=s_B=g^{ab} \bmod p$

IV. CONSTRAINTS

Diffie-Hellman key exchange allows two people/organizations to share a common information.But there might be a possibility of communicating with the devil instead of the desired person/group.Hence to overcome this challenge at least one party is to be authenticated.

This is also called Man-in-Middle Attack. Let's see an example:We see that an anonymous person acts as a middle man in the conversation. •Now he sends messages to individuals , as if they are coming from other individuals.

•Now he generates his own private keys , so that he can manipulate them. •Now he receives the messages from each other , with the private keys he shared. •Now he obtains the Public keys of each other .i.e. Ka, Kb.

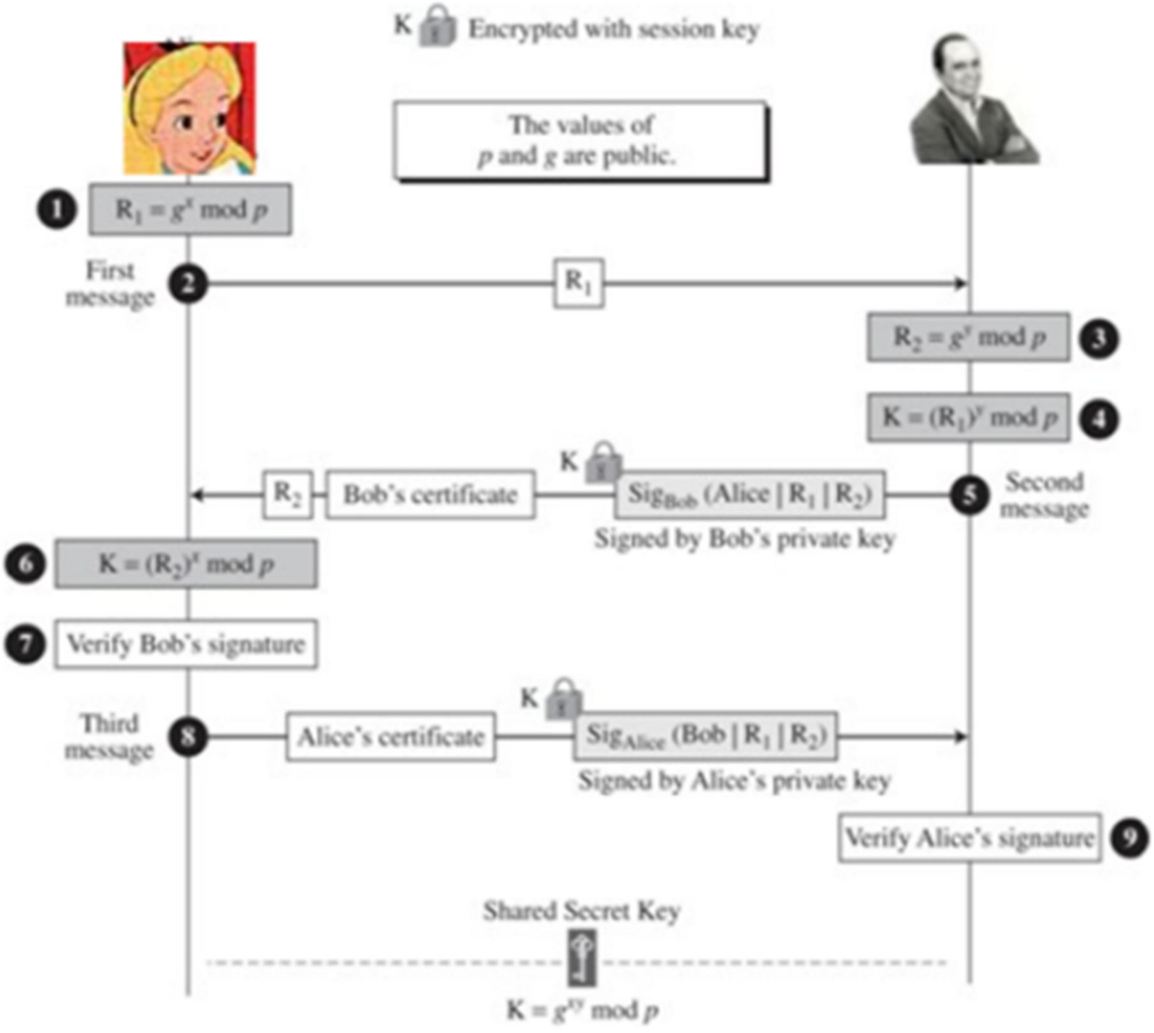
•Now he exchanges the information of Public keys by opposite to each other .i.e. Alice Public key to Bob Public key and vice versa.

•Finally , he obtains a Common secret key after exchanging information of many keys.

V. SOLUTION TO THE CONSTRAINTS

A web server is secured using public key infrastructure, safe/reliable connection is established between user and website. As the website is secured, now the client can trust the website but not vice-versa. Hence it is secure for the client to provide personal details on the web page. Authentication can be done through certifications signed by trusted authorities, containing public keys for participants, etc.

VI. RESULTS & DISCUSSIONS



VII. CONCLUSION

In this paper, Diffie hellman key exchange algorithm, its challenges and also the solution to its constraints are presented. A survey on secure and efficient key exchange Algorithms.

REFERENCES

[1] Samyuktha, S., C. Vijaya and D. Durai, 2015. “Implementation of key Aggregate Cryptosystem with Steganography for Secure Data sharing cloud Computing” ISSN: 2277-9655, March, 2015.

[2] Suganyadevi, G. and S. Punitha Devi, 2015. “Effective Data Sharing in Cloud Using Aggregate Key and Digital Signature”.

[3] Rashmi Khawale, Roshani Ade, 2015. “Development of improved Aggregated Key Cryptosystem for scalable data sharing” Rashmi Khawale International Journal of Computer Science and Information Technologies.

[4] Baojiang Cui, Zheli Liu and Lingyu Wang, 2014. “Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage” IEEE Transactions on Computers

[5] E. Okamoto and K. Tanaka, Key distribution system based on identification information, Selected Areas in Communications, IEEE Journal on , vol. 7, no. 4, pp. 481-485 , 1989.

[6] A. Fiat and A. Shamir, How to prove yourself: practical solutions to identification and signature problems, in Advances in cryptology—CRYPTO 86, Springer-Verlag London, 1987, pp. 186-194.

[7] W. Diffie, P. C. V. Oorschot and M. J. Wiener, Authentication and authenticated key exchanges, Designs, Codes and Cryptography , vol. 2, no. 2, pp. 107 - 125 , June 1992 .

[8] M. Just and S. Vaudenay, Authenticated Multi-Party Key Agreement, in ASIACRYPT 96 Proceedings of the International Conference on the Theory and Applications of Cryp-Tology and Information Security: Advances in Cryptology, 1996.

[9] R. Canetti and H. Krawczyk, Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels, in International Conference on the Theory and Application of Cryptographic Techniques Innsbruck, Austria, May 6–10, 2001 Proceedings, 2001.

[10] B. LaMacchia, K. Lauter and A. Mityagin, Stronger security of authenticated key exchange, in First International Conference, ProvSec 2007, Wollongong, Australia, Novem-ber 1-2, 2007. Proceedings, 2007.

[11] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva and M. Yung, Systematic Design of Two-Party Authentication Protocols, in Advances in Cryptology — CRYPTO 91, 1992.

[12] S. Blake-Wilson and A. Menezes, Authenticated Diffie-Hellman Key Agreement Protocols, in SAC '98 Proceedings of the Selected Areas in Cryptography, Tavares, 1998.A STUDY ON... 189

[13] C. Boyd, W. Mao and K. G. Paterson, Key Agreement Using Statically Keyed Authenticators, in Applied Cryptography and Network Security, Jakobsson, 2004.

[14] O.-R. P. f. T.-P. A. K. Exchange, One-Round Protocols for Two-Party Authenticated Key Exchange, in Applied Cryptography and Network Security, Jakobsson, 2004.

[15] L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone, An efficient protocol for authenticated Key Agreement, Designs, Codes and Cryptography, vol. 28, no. 2, pp. 119 - 134,2003.

[16] R. Lu, Z. Cao, R. Su and J. Shao, Pairing-Based Two-Party Authenticated Key Agreement Protocol, 2005.

[17] H. Krawczyk, HMQV: a high-performance secure diffie-hellman protocol, in Advances in Cryptology – CRYPTO 2005: 25th Annual International Cryptology Conference, SantaBarbara, California, 2005.

[18] S. Blake-Wilson, D. Johnson and A. Menezes, Key agreement protocols and their security analysis, in Proceedings of the 6th IMA International Conference on Cryptography and Coding, Darnell, 1997.

[19] R.J.D.M. Ankney, The Unified Model, in Contribution to X9F1, 1995