International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT21767

# Picpass Algorithm for Solution of Key Exchange Problem in Symmetric and Asymmetric Key Cryptography

**Anchal Goyal[1], Deepinder Kaur[2]**
[1]M.Tech. Scholar, Department of CSE, SUSCET Tangori Mohali, Punjab, India
[2]Assistant Professor, Department of CSE, SUSCET Tangori, Mohali, Punjab, India

**Article Info**
Volume 7, Issue 6
Page Number : 305-308

**Publication Issue :**
November-December-2021

**Article History**
Accepted : 05 Dec 2021
Published : 18 Dec 2021

## ABSTRACT

In this dissertation a PicPass algorithm is proposed for the solution of Key Exchange problem using Symmetric and Asymmetric key cryptography. Diffie and Hellman proposed an algorithm for key exchange. But this algorithm suffers from Man-in middle attack. So to overcome this problem Seo proposed another algorithm that uses text password for the agreement between two parties. But again the password suffers from offline dictionary attack. In this, a PicPass Protocol i.e. picture is used as a password to make an agreement between two parties. The protocol contains two function i.e. picture function as well as distortion function is used to make picture in a compact size and then it is sent to receiver. Firstly the sender encrypts the Plain Text using Secret Picture and creates the Cipher Text using Symmetric key cryptography.Then the Secret Picture will be encrypted by covered picture resulting into Encrypted Picture.Now the Cipher Text and Encrypted Picture will be placed into digital envolpe and then the envelope will be send to the receiver. The receiver will receive the digital envelope, open it and then decrypt the Encrypted Picture using his Key Picture. This will result the receiver to get the Secret Picture. Now the receiver will open the Cipher Text using the Secret Picture and get the Plain Text. In between if any person wants to predict the Encrypted Picture then he cannot guess as the picture will only be decrypted using the Secret Key which will be only with the receiver. So in this dissertation, a picture is used as a password to authenticate key exchange is that gives practical solution against offline dictionary attacks only by using both private and public key cryptography.

Keywords : Key Exchange, Protocol, Cryptography, Authentication, Secret Picture(Sender's Private Key), Covered Picture(Receiver's Public Key) , Key Picture(Receiver's Private Key), Plain Text.

## I. INTRODUCTION

Basics of Cryptography and The Problem Of Key Agreement.

### 1.1 Basics of Cryptography

Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext(ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

The algorithm, the set of mathematical rules, dictates how enciphering and deciphering take place. Many algorithms are publicly known and are not the secret part ofthe encryption process.

The way that encryption algorithms work can be kept secretfrom the public, but many of them are publicly known and well understood. If theinternal mechanisms of the algorithm are not a secret, then something must be. Thesecret piece of using a well-known encryption algorithm is the key. The key can be anyvalue that is made up of a large sequence of random bits. Is it just any random numberof bits crammed together? Not really. An algorithm contains a keyspace, which is arange of values that can be used to construct a key. The key is made up of random valueswithin the keyspace range.

### 1.2 Key Exchange Problem

So the above methods are not completely acceptable. This problem is known as Key exchange Problem. Since the sender and the receiver will use the same key to lock and unlock, this is called as symmetric key cryptography.
So we observe that the key distribution problem is inherently linked with the symmetric key operation.
Different solutions of the problem

**Based upon symmetric key algorithm**
Diffie-Hellman Key Exchange/Agreement
Devised by Whitefield Diffie and Martin Hellman in 1976.Two parties can agree on a symmetric key using this technique i.e. the same key can be used for encryption as well as decryption.Key can be used only for key agreement ,but not for encryption & decryption of messages.Once the parties are agree on key then the key can be used for encryption as well as decryption.
Seo and Sweeney Key Agreement Protocol
Seo and Sweeney proposed a simple authenticated key agreement protocol that Alice and Bob (two users) share a common password $P$ before the protocol begins and uses the same public values of gand nas the original Diffie-Hellman. In the Diffie-Hellman key agreement protocol, the system uses public values nand gwhere nis a large prime number and gis a generator with order n-1 in GF(n) .

## II. Literature Survey

**Private Key Cryptography [34][35]**the encryption and decryption are done with the help of same key.This is also known as symmetric key cryptography.In a cryptosystem that uses symmetric cryptography, both

parties will be using the samekey for encryption and decryption. This provides dual functionality.

**Diffie et al[33] [34][35]** introduces a key agreement protocol inwhich two parties can establish a secret session key over insecure channel. Key can be used only for key agreement ,but not for encryption & decryption of messages.Once the parties are agree on key then the key can be used for encryption as well as decryption. It makes use of the difficulty of computing discrete logarithms over a finite field. Diffie-Hellman key exchange does not authenticate the participants. But it suffers from man-in-middle attack.

**Laih et al[16]** In 2005, Laih, Ding and Huang(Laih and Ding 2005) proposed a password-based key establishment protocol(referred to as the LDH protocol) such that a user and a server can authenticate each other and generate a strong session key by their shared weak password within a symmetric cipher in an insecure channel. However in (Tang and Mitchell 2005), Tang and Mitchell points out that in the LDH protocol,the protection of the password is based on the security of the function φ, i.e., the assumption thata machine (without a human being involved) cannot effectively recognise *r* from φ (*r*, *s*) .

**Olivier Blazy et al[1]**Password-Authenticated Key Exchange (PAKE) has received deep attention in the last few years, witha recent improvement by Katz and Vaikuntanathan, and their one-round protocols: the two players just have to send simultaneous flows to each other, that depend on their own passwords only, to agree on a shared high entropy secret key.

### Diffie-Hellman, Seo and Tseng Protocol

Devised by Whitefield Diffie and Martin Hellman in 1976.Two parties can agree on a symmetric key using this technique i.e. the same key can be used for encryption as well as decryption.Key can be used only for key agreement ,but not for encryption & decryption of messages. Once the parties are agree on key then the key can be used for encryption as well as decryption.

### 3.1.1 Steps of the Algorithm

Let us assume that Alice & Bob want to agree upon a key to be used for encrypting /decrypting messages that would be exchanged between them. So the steps are as :-

Firstly Alice and Bob agree on the two large prime numbers, n & g. These two numbers need not be secret. They can use some insecure channel to agree on them.

Alice choose another large random number x, and calculate A such that

$A=g^x \bmod n$

Alice sends the number A to Bob.

Bob independently choose another large random integer y and calculates B such that:

$B=g^y \bmod n$

Bob sends the number B to Alice.

A now computes the secret key K1 as follows:

$KI=B^x \bmod n$

B now computes the secret key K2 as follows:

$K2=A^y \bmod n$

At last K1=K 2 (Both will agree on same key)

## III. REFERENCES

[1]. David Pointcheval, Olivier Blazy, New Smooth Projective Hash Functions and One-Round Authenticated Key Exchange(18_22 august 2013, Santa Barbara, California, USA), Springer-Verlag, LNCS 8042, pages 449_475.

[2]. David Pointcheval, Olivier Blazy, Effcient UC-Secure Authenticated Key-Exchange for Algebraic Languages(26 February - 1 March 2013, Nara, Japan)), 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013.

[3]. David Pointcheval, Password-based Authenticated Key Exchange. (21-23 may 2012,

Darmstadt, Germany)Springer-Verlag, LNCS 7293, pages 390-397.

[4]. David Pointcheval, Michel Abdalla, Contributory Password-Authenticated Group Key Exchange with Join Capability, (February 14-18, 2011, San Francisco, CA, USA), A. Kiayias Ed. Springer-Verlag, LNCS 6558, pages 142-160.

[5]. David Pointcheval, Xavier Boyen, Strong Cryptography from Weak Secrets, (3 – 6 may 2010, Stellenbosch, South Africa), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 297–315.

[6]. David Pointcheval, Michel Abdalla, Flexible Group Key Exchange with On-DemandComputation of Subgroup Keys, (3-6 May 2010, Stellenbosch, South Africa)), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 351-368.

**Cite this article as :**

Anchal Goyal, Deepinder Kaur, "Picpass Algorithm for Solution of Key Exchange Problem in Symmetric and Asymmetric Key Cryptography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 305-308, November-December 2021.
Journal URL : https://ijsrcseit.com/CSEIT217664