AN IN-DEPTH ANALYSIS OF PICPASS ALGORITHM IN PROVIDING AN EFFECTIVE SOLUTION FOR ‘KEY EXCHANGE PROBLEM’

Muskaan Juneja

Ramjas College, University of Delhi

ABSTRACT

This paper proposes a PicPass calculation to take care of the Key Exchange issue utilizing Symmetric and Asymmetric key cryptography. Diffie and Hellman proposed a calculation for key exchange. However, this calculation experiences a Man-in centre assault. So to defeat this issue, Seo proposed one more calculation that involves text passwords for the understanding between two gatherings. Be that as it may, the secret phrase experiences a disconnected word reference assault once more. For example, a Picasso Protocol is utilized as a secret phrase to concur with two gatherings. The convention contains two capacities, for example, picture capacity and mutilation work, which is utilized to take pictures in a minimized size and afterwards, it is shipped off the beneficiary. Initially, the source encodes the Plain Text utilizing Secret Picture and makes the Cipher Text utilizing Symmetric key cryptography. Then, at that point, the Secret Picture will be encoded by a canvassed picture bringing about an Encrypted Picture. Presently will put the Cipher Text and Encrypted Picture into a computerized envelope and afterwards send the envelope to the beneficiary. The receiver will get the advanced notification, open it, and decrypt the Encrypted Picture utilizing his Key Picture. This will bring about the collector getting the Secret Picture. The recipient will open the Cipher Text utilizing the Secret Picture and get the Plain Text. To anticipate the Encrypted Picture, he can't figure that the image might be decoded utilizing the Secret Key, just with the receiver. So in this paper, an image is used as a secret word to confirm the key exchange, which gives a pragmatic arrangement against disconnected word reference attacks simply by utilizing private and public-key cryptography.

INTRODUCTION

Cryptography is the study of data security. The word is gotten from the Greek kryptos, which means stowed away. Cryptography is firmly connected with the disciplines of cryptology and cryptanalysis. Cryptography incorporates procedures like microdots, combining words with pictures, and alternate ways of concealing data away or travel. Notwithstanding, in the present PC driven world, cryptography is most frequently connected with scrambling plaintext (standard message, at times, alluded to as cleartext) into ciphertext (an interaction called encryption), then, at that point, back once more (known as decoding). People who practice this field are known as cryptographers. As of late, cryptography has transformed into a landmark of some of the world's best mathematicians and PC researchers. The capacity to safely store and move delicate data has demonstrated a basic element in accomplishment in war and business.

LITERATURE SURVEY

Private Key Cryptography [34][35]the encryption and decryption are done with the help of a similar key. This is also called symmetric-key cryptography. The two players will involve a similar key for encryption and decoding in a cryptosystem that utilizes symmetric cryptography. This gives double usefulness. Symmetric keys are additionally called secret keys since this sort of encryption depends on every client to stay quiet about the key and appropriately ensure. Assuming this key got into an attackers hand, that interloper would decode any blocked message scrambled with this key.

Website design enhancement and Sweeney (Seo and Sweeny 1999) proposed a basic validated key understanding convention dependent on a pre-shared secret phrase technique and adjusted the Diffie-Hellman plan to give client confirmation. They guaranteed that the setup session key between two clients is additionally confirmed. In any case, (Tseng 2005) said that they couldn't accomplish confirmation of the meeting key in their convention. Checking the session key can't be accomplished in the Seo-Sweeney convention (Seo and Sweeny 1999). Assuming that the enemy answers to the received message after getting the legit client's message, the legitimate client can't decide the shortcoming of the session key.

Diffie et al. [33] [34][35] present a key understanding convention in which two groups can build up a unique session key over an unreliable channel. Can utilize key just for fundamental understanding, yet not really for encryption and decryption of messages. When the meeting settles on the key, they then, at that point, can involve the key for encryption and decryption. It utilizes the trouble of processing discrete logarithms over a limited field. Diffie-Hellman key trade doesn't validate the members. Yet, it experiences a man-in-centre attack. Man-in-the-centre attacks are regularly managed by planning conventions that ensure against a rundown of known attacks; such a methodology, notwithstanding, leaves the convention vulnerable against new attacks as they are created.

Tseng [14]By utilizing a pre-shared secret phrase method, Seo and Sweeney (Seo and Sweeny 1999) proposed a basic key arrangement convention that planned to go about as a Diffie-Hellman conspire (Diffie and Hellman 1976) with client validation. In the Seo-Sweeney convention, two groups who have shared a typical secret key can set up a meeting key by exchanging two messages. The originators likewise guaranteed that they could accomplish key approval by trading two additional messages. Afterwards, (Tseng 2005) managed to a shortcoming in the key approval steps of the Seo-Sweeney convention. The enemy can trick the legit party into accepting an off-base meeting key by answering the message sent from the appropriate party. Tseng altered the key approval steps of the Seo-Sweeney convention and asserted that it could accomplish key approval in the changed convention.

Diffie-Hellman, Seo and Tseng Protocol Devised by Whitefield Diffie and Martin Hellman in 1976. Two gatherings can settle on a symmetric key utilizing this strategy. When the gatherings settle on the key, they can involve it for encryption and decoding. For example, it can involve a similar key for encryption and unscrambling. Can utilize key just for key arrangement, however not so much for encryption and decoding of messages.

Steps of the Algorithm

Allow us to expect that Alice and Bob need to concur upon a key to be utilized for scrambling/decoding messages that would trade between them. So the means are as:- Firstly, Alice and Bob settle on the two enormous indivisible numbers, n and g. These two numbers need not be confidential. They can utilize some shaky channels to settle on them.

- Alice pick another enormous irregular number x and compute A with the end goal that
- A=gx mod n
- Alice sends the number A to Bob.
- Sway freely picks another enormous irregular number y and works out B with the end goal that:

B=gy mod n

- Sway sends the number B to Alice.
- A presently figures the mysterious key K1 as follows:

KI=Bx mod n

- B presently figures the mysterious key K2 as follows:

K2=Ay mod n

Finally, K1=K 2 (Both will settle on a similar key)

THE PROPOSED PROTOCOL

LDH proposed a secret key based key foundation convention to such an extent that two clients can validate and produce a solid meeting key by their common secret word inside a symmetric code in an unreliable medium. In their review, they proposed an exceptional kind of capacity which is a combination of image work and a twisting capacity, is blended to validate the client and shield the secret word from the disconnected word reference tackles that are significant issues for a large portion of the soft secret key based conventions. They suggested that the proposed convention is secure against some predefined assaults. Notwithstanding, Tang shows that the convention experiences a disconnected word reference assault requiring a machine-based pursuit of size 223, which requires just around 2.3 hours. So planning such a sort of convention that gives a viable security arrangement against disconnected assaults is as yet a test. This review presents picture secret word-based key foundation conventions that give pragmatic security arrangements against disconnected word reference assaults by just utilizing private key cryptography.

Passwords are the most generally utilized verification strategy, albeit their utilization has some significant security issues with the end goal that they can be effectively speculated via mechanized projects running disconnected word reference assaults. The situation where two clients verify one another and produce a solid meeting key through private key cryptography from the low strength secret word known by the two players is exceptionally useful and advantageous. In any case, planning a safe arrangement convention for this issue is an open issue because of the adequacy of separate word reference assaults. Leigh et al. proposed a secret key based verified key foundation convention to determine this issue. In reality, the significant distinction of the convention from a few notable conventions is that it doesn't utilize public-key cryptography to join a huge space with secret word space to shape a huge sufficient room to shield from the disconnected word reference assault. The critical thought behind this convention is utilizing an exceptional capacity comprised of image work and a twisting capacity. This capacity is characterized as $\varphi(r, s)=g(p(r, s))$, where g is a contortion work, p is an image work which takes an irregular series of characters/digits r and an arbitrary number s as info contentions. The CAPTCHA, which a few organizations utilize to keep away from many free record applications from machines alone, illustrates this sort of capacity.

CONCLUSION AND FUTURE SCOPE

This research introduces another secret image word-based key foundation calculation that utilizes private and public-key cryptography. The proposed conventions give a down to earth answer for the issue of separate word reference assaults from which Seo and Sweeny's convention endures. By customization of the convention, it turns out to be exceptionally helpful and pragmatic.

The examination of time with similar text size and a similar size of the image. From the chart, it is presumed that the Pic-Pass convention takes additional time at the beginning of the encryption. Yet, in the wake of meeting a specific point with Text encryption, it requires some investment and text encryption takes additional time with similar measures of information.

After a specific computation, we can say that the PicPass calculation is 55% better when contrasted with Text encryption. Additionally, straightforward text encryption/unscrambling experiences the issues of secrecy, verification, and honesty. For example, the direct assault is the Man-in-Middle assault. On the other hand, a convention, for example, the PicPass, is shielded from the attacks.

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.