



**An Improved Technique to Prevent Man-in-the-Middle
Attack in DH Protocol Using Feige-Fiat Shamir
Algorithm**

A Dissertation submitted

By

RITU SINGH

To

Department of Computer & Science Engineering

In partial fulfillment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science

Under the guidance

of

Ms. SANGEETA SHARMA

(May, 2015)



LOVELY
PROFESSIONAL
UNIVERSITY

Creating Education. Transforming India.

School of: LETS

DISSERTATION TOPIC APPROVAL PERFORMANCE

Name of the Student: Ritu Singh

Registration No.: 11310791

Batch: 2013-15

Roll No.: RX2306862

Session: 2014-15

Parent Section: K2306

Details of Supervisor:

Designation: Asst

Name: Sangeeta

Qualification: M.Tech

UID: 15681

Research Experience: 3

SPECIALIZATION AREA: Network Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Attacks on DH protocols. (Security of
2. Man in the middle attacks
3. solution of some attacks in N/A.

Signature of Supervisor: 

PAC Remarks:

Yes, I will make sure the student publishes a paper on this in some well-known journal.

APPROVAL OF PAC CHAIRPERSON:

Signature: 

Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for a approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

Network security is a wide area for research. Online communication mostly takes place used. All communication is done over network. Online communication, data transfer is very common today. When a data is transferred over a communication channel then attacker can attack over the data to get the information transferred over communication channel. To transfer data securely over network authentication protocols are used. By using these authentication protocols only authorized person can access the data. Authorized are those who have the legal access to the information. Unauthorized users can't get the information transferred. Nowadays it becomes the need to secure the confidential information. The proposed technique is to provide a secure authentication protocol. In this technique, feige-fiat-Shamir algorithm is applied to prevent the data from different types of attacks. In feige-fiat-Shamir algorithm, sender chooses random integer r and n . Then it calculates witness with the help of r and n , send this witness to the receiver. Receiver chooses a vector of challenges and sent it to the sender. Sender calculates y with the help of these challenges and sent it to receiver. Receiver calculates its value and compares the value to the sender's value. Both the values are same then only key is shared in DH protocol between user and receiver.

ACKNOWLEDGEMENT

I owe a debt of deepest gratitude to my thesis supervisor, **Ms. Sangeeta Sharma**, Department of Computer Science And Engineering, for her guidance, support, motivation and encouragement throughout the period this work was carried out. Her readiness for consultation at all times, her educative comments, her concern and assistance even with practical things have been invaluable.

I am grateful to **Mr. Dalwinder Singh**, Head of the Department, Computer Science and Engineering for providing me the necessary opportunities for the completion of my work. I also thank the other faculty and staff members of my department for their invaluable help and guidance.

DECLARATION

I hereby declare that the dissertation proposal entitled, **an improved technique to prevent man-in-the-middle attack in D-H protocol** submitted for the M-Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Ritu Singh
Registration No: 11310791

CERTIFICATE

This is to certify that **RITU SINGH** has completed M-Tech (computer science and technology) dissertation proposal titled **an improved technique to prevent Man-in-the-middle attack in Diffie-Hellman protocol using Feige-fiat Shamir algorithm** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfilment of the conditions for the award of M-Tech Computer Science & Engineering.

Date:

Signature of Advisor:

Name: Sangeeta Sharma

UID: 15681

TABLE OF CONTENT

CHAPTER1-INTRODUCTION	1
1.1AUTHENTICATIONPROTOCOLS	4
1.2DIFFIE-HELMAN KEY EXCHANGE PROTOCOL	7
1.3ATTACKS ON DIFFIE-HELLMAN PROTOCOL	8
CHAPTER 2-REVIEW OF LITERATURE	12
CHAPTER 3- PRESENT WORK	16
3.1- PROBLEM FORMULATION	16
3.2- OBJECTIVES OF THE STUDY	16
3.3- RESEARCH METHODOLOGY	17
CHAPTER 4- RESULTS AND DISCUSSIONS	20
CHAPTER 5-CONCLUSION AND FUTURE SCOPE	46
5.1- FUTURE SCOPE	46
CHAPTER 6- LIST OF REFERENCES	47
CHAPTER 7- APPENDIX	50

LIST OF FIGURES

FIGURE 1. DENIAL OF SERVICE ATTACK.....	2
FIGURE 2 MAN IN THE MIDDLE ATTACK.....	2
FIGURE 3 ACTIVE ATTACKS.....	3
FIGURE 4 PASSIVE ATTACKS.....	3
FIGURE 5 RELEASE OF MESSAGE CONTENT.....	4
FIGURE 6 SHARED SECRET KEY.....	5
FIGURE 7 PUBLIC KEY SYSTEM.....	5
FIGURE 8 KEY DISTRIBUTION CENTRE.....	6
FIGURE 9 KERBEROS.....	7
FIGURE 10 DH PROTOCOL.....	8
FIGURE 11 MITM ATTACK.....	9
FIGURE 12 FFS ALGORITHM.....	11
FIGURE 13 MATLAB.....	20
FIGURE 14 MATLAB INTRODUCTION.....	21
FIGURE 15 MATLAB WORKSPACE.....	21
FIGURE 16 COMMAND WINDOW.....	22
FIGURE 17 GRAPH IN MATLAB.....	23
FIGURE 18 OUTPUT.....	24
FIGURE 19 OUTPUT 1.....	25
FIGURE 20 OUTPUT 2.....	25
FIGURE 21 OUTPUT 3.....	26
FIGURE 22 OUTPUT 4.....	26
FIGURE 23 OUTPUT 5.....	27
FIGURE 24 OUTPUT 6.....	27
FIGURE 25 GRAPH 1.....	28
FIGURE 26 GRAPH 2.....	28
FIGURE 27 ZERO KNOWLEDGE PROOF.....	30
FIGURE 28 BASE PAPER GRAPH.....	31
FIGURE 29 SNAPSHOT 1.....	32
FIGURE 30 SNAPSHOT 2.....	32
FIGURE 31 SNAPSHOT 3.....	33
FIGURE 32 SNAPSHOT 4.....	33
FIGURE 33 SNAPSHOT 5.....	34
FIGURE 34 SNAPSHOT 6.....	34
FIGURE 35 SNAPSHOT 7.....	35
FIGURE 36 SNAPSHOT 8.....	35
FIGURE 37 SNAPSHOT 9.....	36
FIGURE 38 SNAPSHOT 10.....	36
FIGURE 39 SNAPSHOT 11.....	37
FIGURE 40 SNAPSHOT 12.....	37
FIGURE 41 SNAPSHOT 13.....	38
FIGURE 42 SNAPSHOT 14.....	38
FIGURE 43 SNAPSHOT 15.....	39
FIGURE 44 SNAPSHOT 16.....	39
FIGURE 45 SNAPSHOT 17.....	40
FIGURE 46 SNAPSHOT 18.....	40
FIGURE 47 SNAPSHOT 19.....	41

FIGURE 48 SNAPSHOT 20.....	41
FIGURE 49 SNAPSHOT 21.....	42
FIGURE 50 SNAPSHOT 22.....	42
FIGURE 51 SNAPSHOT 23.....	43
FIGURE 52 SNAPSHOT 24.....	43
FIGURE 53 SNAPSHOT 25.....	44
FIGURE 54 SNAPSHOT 26.....	45

Chapter 1

INTRODUCTION

Network security is an area in which administrator provide access of information to the only authorized users. Today most of the work is done online. Most of the information is shared over communication channel. Personal, confidential data is also shared over network. Network can be of two types, private and public network. Network is used in organizations, companies and institutes. There is high risk of information theft or misuse of that information shared over information. To provide security over network, network security is used. When data or some information is shared over network then there can be some attacks over data and information. There are two types of attacks.

Active Attacks:- Active attacks are those types of attacks in which modification or alteration of takes place. In this attacker destroy or harm the data by modification or alteration data. There are some attacks, come under active attacks. Denial of service attacks, man in the middle attacks, replay attack, spoofing etc.

Denial of service attack, it is an attempt to suspend services of host or system temporarily. This attack is used in business and website attacks. In DOS attacker makes a large number of request to the host. Host becomes unable to handle large number of request. Due to these requests services become unavailable to the users or system crashes. Requests sent by the attacker, seems as authorized users. Those systems are known as zombie systems through which attacker sends request to the host. Attacker sends a command to the zombie systems. On the basis of the command zombie systems sends a large number of packets of the useless information to the website to make website available.

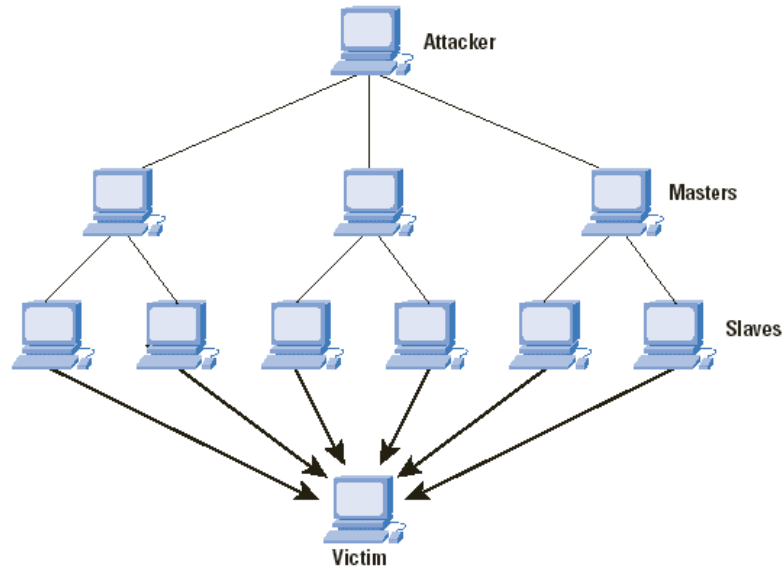


Figure 1. Denial of service attack

Man in the middle attack, attacker attacks between sender and receiver to get the information shared between sender and receiver. In this sender thinks that he is communicating to the receiver but actually he is communicating to the attacker. Receiver also thinks that he is getting the data to the sender but in real attacker is sending the data to the receiver. In MITM attacker impersonates the identity of sender and receiver..

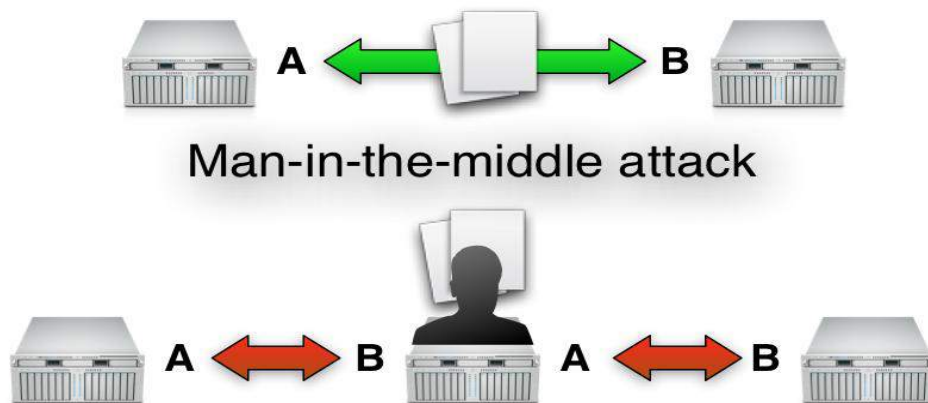


Figure 2 Man in the middle attack

Replay attacks, in this attack attacker first intercepts a message, later retransmits it again and again to the receiver. Spoofing, it is a type of attack in which attacker attempts to get unauthorized access to the authorized user's system or information and pretend as an authorized user.

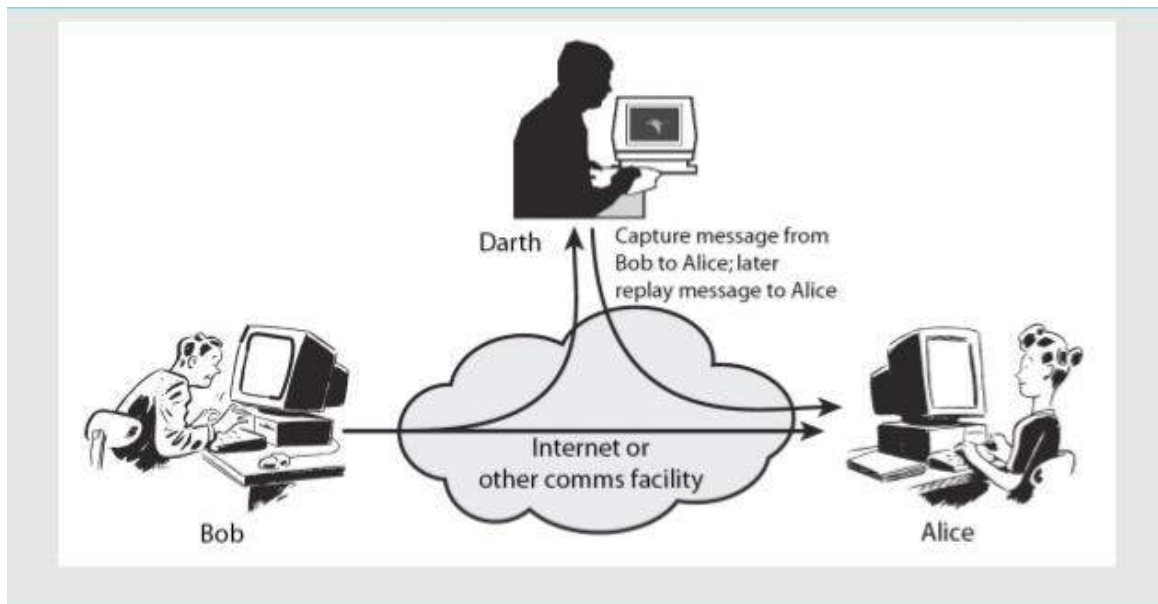


Figure 3 Active attacks

Passive Attacks:- Passive attacks are those types of attacks in which no modification or alteration takes place. In this attack, attacker only learns or makes use of the information but do not destroy or alter the data. Passive attacks are traffic analysis, release of message content, wiretapping, port scanner etc.

Passive Attacks

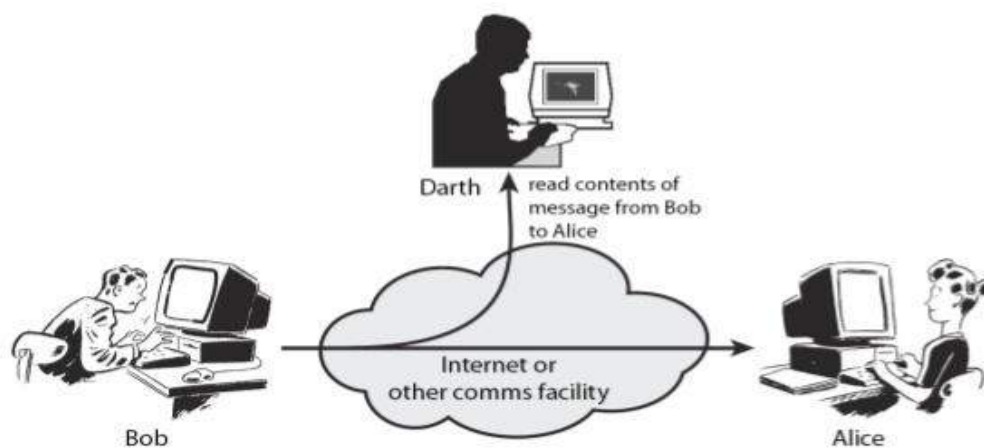
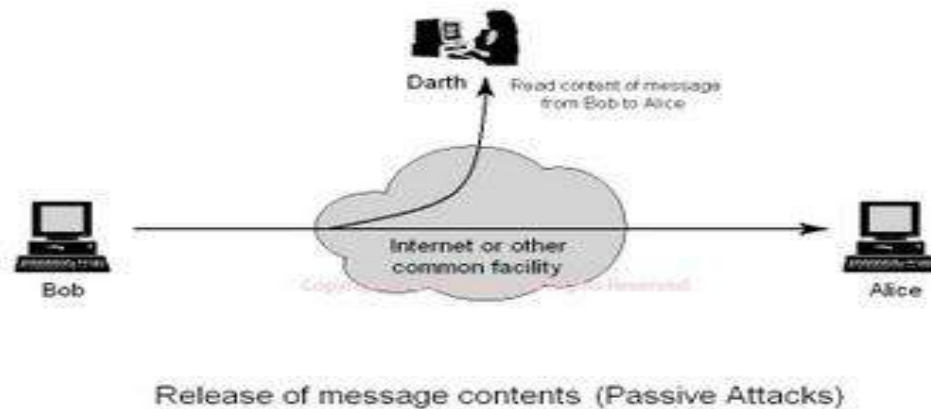


Figure 4 Passive attacks

Traffic analysis, in this attacker, analyzes the traffic over the network. Release of message content, attacker monitors the content of the message but do not alter the message. Wiretapping, attacker or intruder monitors communication over electronic devices like telephone. Port scanner, attacker sends a list of messages to host to identify the running services on that host.



Release of message contents (Passive Attacks)

Copyright © 2007 Sun Microsystems, Inc. All rights reserved.

Figure 5 Release of message content

To provide security to the network authentication is used. Authentication is used to prevent unauthorized access. To provide authentication to a user, choose or assigned an ID and password or some other authenticating information that allows the access to data within their authority. Authentication is the process of confirming the identity of the user. By authentication technique a process verifies that its communication partner is authorized and not a fake user. Authentication can be of three types. Types of authentication are following.

First type of authentication is accepting proof of identity given by a person who has first-hand evidence that the identity is genuine. Second type of authentication is comparing the attributes of the object itself to what is known about objects of that origin. Third type of authentication relies on documentation or other external things.

1.1 Authentication Protocols:- These types of protocols used for authentication in network security.

(A) Direct authentication:- these are of two types.

- Based on a shared secret key:- in this type of authentication protocol a secret key is shared between all the parties involved in the secure communication. This secret key can be a password, a number or an array of random chosen bytes. This secret key can be shared before the communication that time it is called pre-shared key. Or it can be shared at the start time of communication session. In this type of protocol a key is shared between sender and receiver, is used for encryption of data at sender side to create cipher-text and decryption of data at receiver side to get plaintext. It is known as symmetric key cryptography.

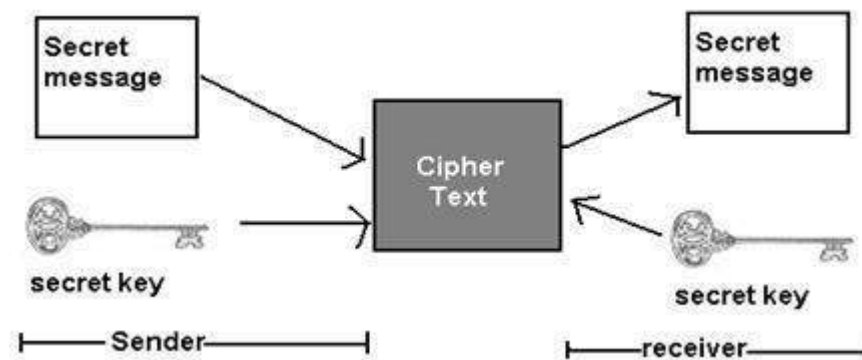


Figure 6 shared secret key

- Based on a public key system:- In this type of systems two separate keys are required. One key is known as public key and another is known as private key. Both keys are different. Public key is used to encrypt the data at sender side while private key is used to decrypt the data at receiver side. This is used in digital signatures, where public key is used to create a digital signature or encrypt the data while private key is used to verify the signature or decrypt the data at receiver side. This method also known as asymmetric key cryptography.

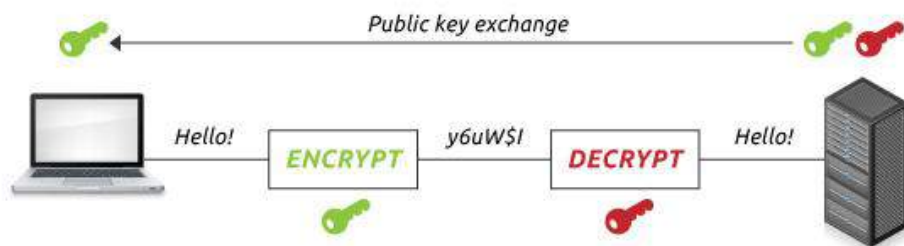


Figure 7 Public key system

(B) Mediated authentication:-

- Based on key distribution Centre:- In cryptography, a key distribution centre is used to reduce the risks occur in exchanging keys. KDCs used in that system in which some users want to get permission to use services at some times. In this system an administrator is used to provide the services to the users. This administrator is also known as third party. If a user wants to use some service then it should send a request to the KDC. If that user meets all the authenticated conditions, the KDC can issue a ticket to the user. KDCs operate symmetric key cryptography. KDC shares a key with each of all the users. KDC produces a ticket and sends it to client. Client receives the ticket and sends it to the server. Server can verify the ticket and grant access to the user who submits the ticket.

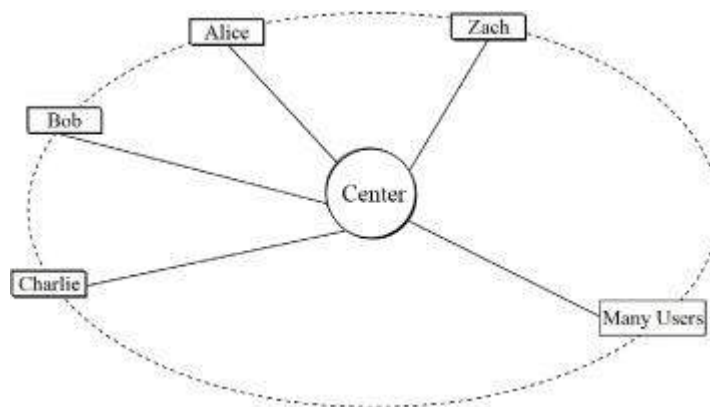


Figure 8 Key distribution Centre

- Kerberos:- it is also a third party authentication protocol. It works on basis of ticket to allow users to communicate over a non-secure communicating network. Tickets also help to prove the identity of the users to one another in a secure way. It provides mutual authentication, the user and the server both verify each other's identity. It protects messages against eavesdropping and replay attacks. Kerberos builds on third party and symmetric key cryptography concept. It may use public key cryptography sometimes when required. In Kerberos AS and TGS is used for ticket granting. When a user want to get the service first authenticates itself to the AS, then user sends a TGT to the TGS. TGS verify that TGT is valid,

grant access with issuing ticket and session keys. This ticket and keys are sent to the client.

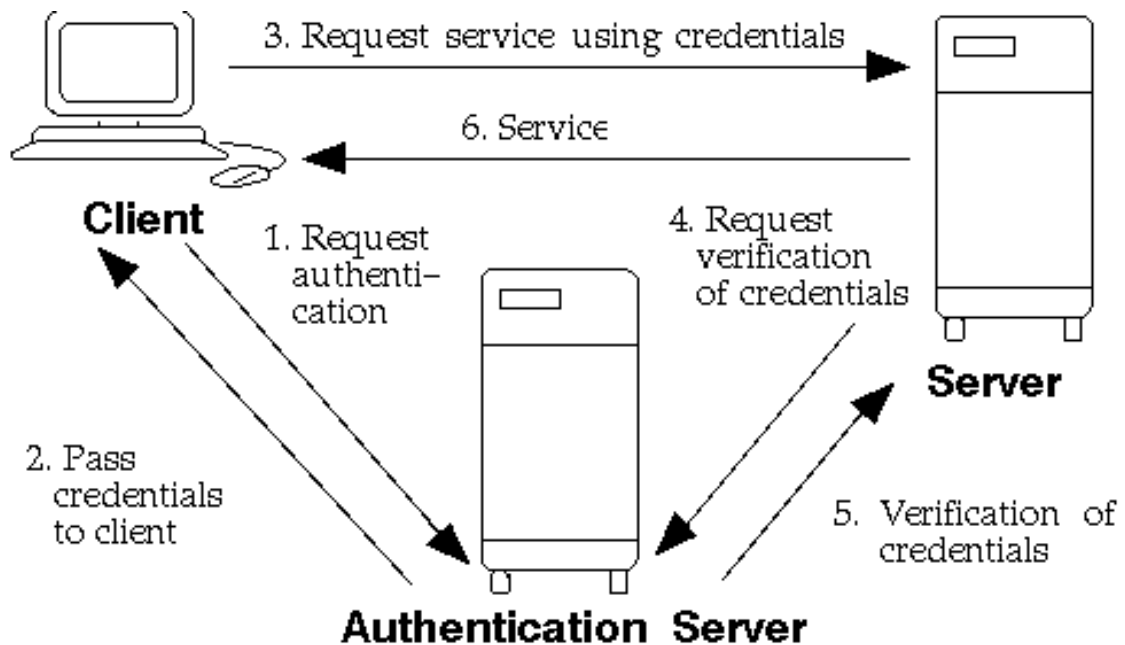


Figure 9 Kerberos

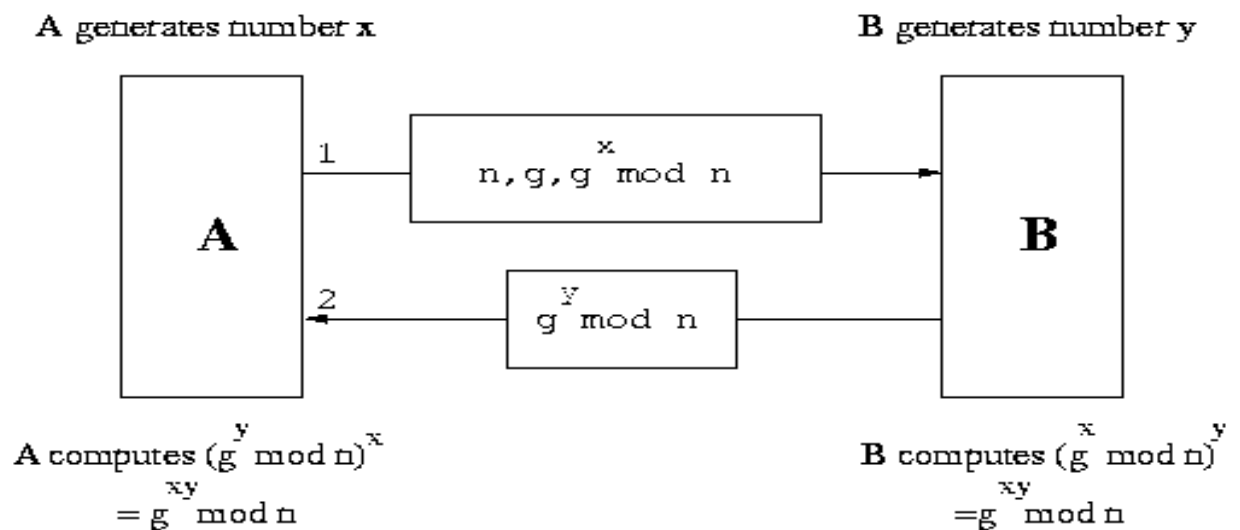
1.2 DIFFIE-HELLMAN KEY EXCHANGE PROTOCOL:- It is shared key cryptography algorithm. It is a specific method of exchanging keys over a communication channel. This scheme was first published by Whitfield Diffie and Martin Hellman in 1976. This method allows two parties to share secret key over an insecure communication channel. This key is used to encrypt communications. Diffie- Hellman key agreement is an anonymous key-agreement protocol. It is used for providing perfect forward secrecy. Diffie-Hellman method was followed afterwards by RSA, an implementation of public key cryptography using asymmetric algorithms.

Diffie-Hellman establishes a secret between the parties to establish a secure communication between parties over an insecure channel. If Alice wants to send data to Bob then there are some steps which Alice and Bob should follow. Alice and Bob first agree on a large prime number n and an element g ($2 \leq g \leq n-2$) that generates a cyclic subgroup of large order. Rest steps of the protocol are following.

- Alice chooses a number, x , at random from the set $\{1, 2, \dots, n-2\}$. And Bob chooses y randomly from the same set.
- Alice sends g^x to Bob and Bob sends g^y to Alice.

- The shared secret key is $K = g^{(x*y)}$. A, knowing x and g^y , can easily calculate $g^y \wedge x = g^{(x*y)}$. Bob can determine the secret key in a similar manner by computing $g^y \wedge x$.

x and y are referred to as the private keys, g^x and g^y are referred to as public keys and $g^{(x*y)}$ is called as shared secret key. This protocol is secure against eavesdropping if n and g are selected properly. But this approach is vulnerable to man-in-the-middle attack. In this approach key is shared between sender (Alice) and receiver (Bob) that is why it is called shared secret key approach.



The Diffie-Hellman Key Exchange

Figure 10 DH protocol.

1.3 Attacks on Diffie-Hellman Key exchange protocol:-Attacks against the D-H protocol are following.

- Denial of service attacks:- DOS attack is that in which attacker sends a large number of request to make service unavailable. In D-H protocol attacker will try to stop sender and receiver from communicating successfully. For doing this, attacker can delete the messages that sender and receiver send to each other, or can disturb the sender and receiver with unnecessary computation or communication.

- Outsider attacks:- In this attacker tries to disrupt the protocol by adding, removing, replaying messages. So that attacker can get some interesting knowledge.
- Insider attacks:- If one of the participants holds a static secret key that is used in many key agreement protocol runs. This attack can be mounted with the malicious software.
- Man-in-the-middle attack:- An attacker Eve attacks on the communication taken place between Alice and Bob. When Alice sends a message to Bob then Eve wants to get that message. So Eve generates two keys and sends one key to the Alice and another to the Bob. Alice thinks that Bob is sending the key and Alice sends the message to the Eve. Eve sends a wrong message to the Bob while Bob thinks that Alice sends that message. All the information Alice wants to send the Bob is captured by Eve. Eve altered the information and send wrong information to the Bob. All the information which is confidential between Alice and Bob is captured by Eve. This type of attack is known as man-in-the-middle attack. These are some steps in man-in-the-middle attack.

Alice sends her key A to Bob, and Bob sends his key B to the Alice. In between Eve captured key of Alice and Bob. Eve generates key E and sends it to Alice and Bob. Alice thinks E is sent by Bob while Bob thinks it is sent by Alice. Eve calculates the secret key $S(AE)$ with the help of A and Alice calculates secret key $S(AE)$ with the help of E. Alice and Eve communicates using secret key $S(AE)$. In same manner Bob and Eve computes secret key $S(BE)$ and communicates using this secret key.

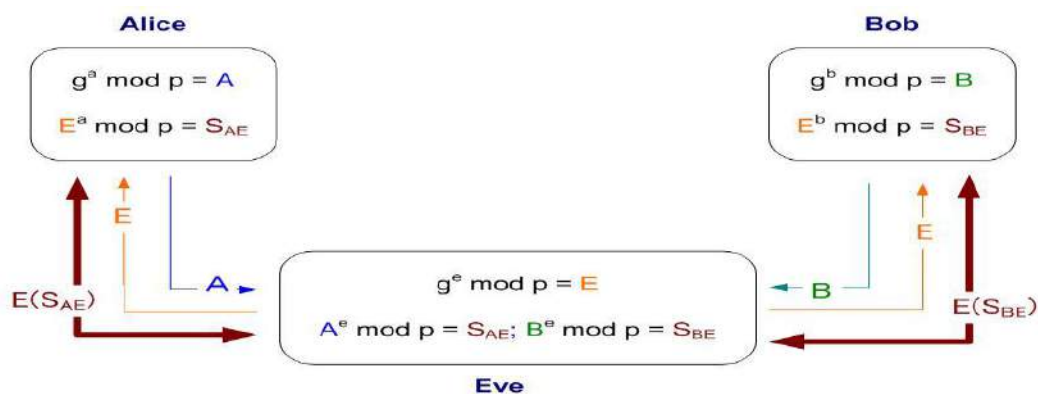


Figure 11 MITM Attack

In my research work, main problem is man-in-the-middle attack. I want to remove this problem by using some authentication method. Today Man-in-the-middle attack is very common in communication over an insecure channel. All the work is done online in today's world. There is a high risk of information theft. To remove problem, I want to work on man-in-the-middle attack in Diffie-Hellman protocol.

Diffie- Hellman protocol is key sharing protocol. It is used to share the key between the parties used in the communication. Man in the middle is third party attack, which is attacked on the DH protocol. It is done by the third person, who wants to get the information sent between the parties involved in the communication. In this attacker gets all the information shared between the sender and receiver. Sender thinks that he is communicating to the receiver but in real he is communicating to the attacker. Attacker gets all the information from the sender on behalf of receiver. In the same manner, receiver also thinks that he is getting the data from the sender. In actual receiver gets the data sent by the attacker.

Applications of DH protocol:-

- DH protocol used in SSH
- DH protocol used in SSL
- DH protocol used in IPsec

FFS algorithm is used as third party key authentication protocol. It is used to verify the claimant that either he is right person or not. It can be detect with the Fiat algorithm that another person is trying to access the information on behalf of authorized person.

In this algorithm we have these steps:-

There are two parties, claimant and verifier.

1. Claimant chooses a random number r . it also chooses a number $e \in \{0, 1\}$. Now claimant calculates the value of $x = (-1)^e \cdot r^2 \pmod n$. claimant sent x to the verifier.
2. Verifier chooses a random number $b \in \{0, 1\}$ and sent it to claimant.
3. Now claimant calculates the value $y = (r^s)^b \pmod n$. and sent it to verifier.
4. After getting y from the claimant, verifier $z = y * y^{(v^b)} \pmod n$. Now $z = x \pmod n$ and $z \neq 0$.

If in step 4 is not verified than there no action takes place in this algorithm. In this algorithm $z=x \text{ mod } n$ is mandatory to verify the claimant.

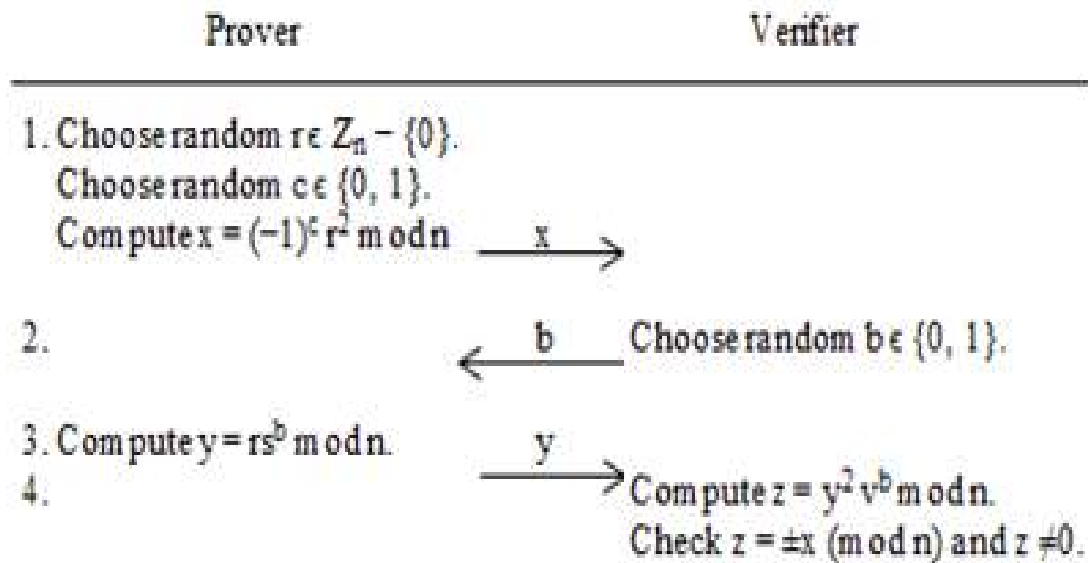


Figure 12 FFS algorithm.

Fiat algorithm is vulnerable to the attacker because in this we have only two possible values of e either 0 or 1. It is very easy for attacker to guess the value of challenge and response. If first time attacker guesses the right value then information can be achieved easily by the attacker and this is a threat to the security of the information.

In this algorithm, the probability of attack is 0.5 because it works upon the Ali Baba's cage theory. In which we have two paths from entering the cage. One is on left and other one is on right side. Among both of these, only one path is correct. If first time attacker enter on the right path then he will reach to the right place. If first time attacker chooses the wrong path then there is a chance of attack failure. So there is 0.5 probability of successful attack.

To enhance the security in this algorithm, we choose an array of public key and private key in the algorithm. Original algorithm was executing in only one step. In our proposed algorithm we have k number of values in the array. So there are k numbers of iterations, in which steps will execute. If even a single time values will not matched then the entire process will not take place. Process will terminate at that step where values not matched.

REVIEW OF LITERATURE

P. Bhattacharya, M. Debbabi and H. Otok(2005) said that Diffie-Hellman is used in cryptographic protocols such as SSL, SH, IP security. In this paper, it is said that DH works under the domain of Z_n^* , where $n=p$, p and α are two parameters of DH, where p is a large prime number and α is generator selected from the cyclic group Z_n^* . In this paper, two modifications of DH are proposed. The first modification is to change the domain to integer with $n=2p^t$ where Z_n^* is still cyclic and second modification is to change the domain with the Gaussian arithmetic Z_n^* [i]. After implementation of this algorithm it is found that the key size of symmetric key is very large. It is also found that to attack on the protocol using large key takes more time in comparison to the actual one. Using this method the security can be improved of those protocols, in which DH protocol is used. To ensure the security of this proposed method Pohlig-Hellman algorithm is used. This algorithm depends on discrete logarithm problem. Attacking this proposed method shows that the time needed to compute the private key for the method is greater than the actual one. The proposed methods are more secure than the classical one because it takes long time to be cracked. So this method is not purely secure but secure than the classical one.

Albina. N, U.J. Raju, K.G. Revathi, K. Raghava Rao said that HTTP is a protocol known as hypertext transfer protocol. It is used to transfer the data over World Wide Web. It is also used for communication purpose like file transfer, data transfer, chatting etc. HTTP is used to provide privacy or security. HTTP is used in banking, e-commerce to deal with the sensitive data. By using HTTPs financial, personal, and confidential information can prevent from unauthorized access. But transfer of data can be attacked by man-in-the-middle attack. In this paper Steganography technique is used to detect unauthorized access over HTTP communication. It allows detection of attack over the communication. In this paper first authentication protocol is used to verify the authentication details of the users. After successfully login data is kept in the form of encrypted data using Data Encryption standard algorithm. DES is used to encrypt the file or data. File or data can be of any length. After encryption data is sent over the media. At the receiver side DES

algorithm is used to decrypt the data. A password is supplied to decrypt the file or data. But in the DES password should be of maximum 8 characters. It is the maximum limit of the password. After decryption, original message can be viewed by the receiver.

Maryam Saeed, Ali Mackvandi, Mansour Naddafiun, Hamid Reza Karimnejad said that Password authenticated key exchange protocols permits two parties to generate a common Session key. PAKE authenticate two parties based on a pre-shared password. In this paper, it is shown that DH-BPAKE protocol is vulnerable to password impersonation attack. First in this paper DH- BPAKE protocol is defined, how is it work. But it is found that this protocol is vulnerable to impersonation attack in password guessing. To resolve this problem a proposed scheme is defined in this paper. In this paper two rounds are used for mutual authentication and key exchange between the sender and the receiver. In this scheme plain password is not sent to the receiver. Password is sent using hash function over ID of sender, ID of receiver, plain password and a random chosen number. This scheme is used to avoid forward secrecy. It also resilience to unknown key share attack, off-line dictionary attack, replay attack, password compromised impersonation attack. It provides known session key attack. This proposed scheme provides several security properties still it has a lower number of rounds and a good remarkable computational efficiency.

Aaron C. Geary (2009) said that DH protocol allows two parties two exchange keys over an unsecured channel. But the exchange becomes vulnerable to man-in-the-middle attack if key exchange takes place in mathematical environment. In this paper, countermeasures are analyzed against the attack and attack is extended to the multi-party setting. To prevent the attack over the DH protocol is to force the authentication over the key exchange. Or the other one is to create a prime order subgroup before the key exchange between the parties. In this paper, to provide authentication between the sender and the receiver RSA signature scheme is used. To employ RSA signature scheme public and private pairs must be generated first. In RSA signature scheme two steps are done. First one is signature generation and other one is verification. And in this paper n-party setting is also used to provide security. In this n users are there and everyone has to choose a prime number and a generator to generate a key. Two stages are there up-flow and down-flow. In up-flow, each member has to make their contribution to shared key. In second

stage, value is broadcasted to the entire group and each member factors out their contribution and forwards the result. In this a large number of secret values are present. If attacker wants to attack then a large number of values are possible.

Kazuomi Oishi, Tsutomu Matsumoto(2011). In this paper an efficient verifiable implicit asking protocol is proposed for DH protocol. The structure of protocol makes is resistant to both active and passive attacks. If a passive attack is applied on this proposed scheme then the efficiency and security of the protocol does not decrease. In this paper, an implicit asking protocol for DH scheme is proposed using RSA cryptosystem as a building block. This scheme utilizes the features of DH scheme. In this scheme two VIA is used. In proposed scheme user A executes DH scheme with user B.

C. Krishna Kumar, G. Jai Arul Jose, C. Sajeev and C. Suyambulingom(2012) said that in authentication protocols key exchange takes place in certain mathematical ways, the exchange of keys becomes vulnerable to man-in-the-middle attack. They explore the man-in-the-middle attack and analyze the countermeasures against the man-in-the-middle attack. To prevent this attack, they use the method to force authentication prior to the key exchange. In the scheme they use identifiers and double encrypts the message M first with sender's private key and then receiver's public key. Now this message is secured and it can only read by receiver. This scheme has a number of advantages. No information is shared among the users before communication, prevents unauthorized access. In this scheme a timestamp also used to show the valid timings of the keys. First a will verify that time keys are valid or not. If keys are valid then a will send the message to the Y with time T. So no incorrect dated message can be send using this scheme. Double encryption is used in this scheme so content of message is secret from sender to receiver. Main drawback of this scheme is that it is too time-consuming due to double encryption and decryption

Zhao Hu, Yuesheng Zhu, Limin Ma (2012). In this paper an improved Kerberos protocol is used to provide authentication in DH protocol. Kerberos is a third trusted party protocol. As a third party KDC is used to provide authentication between client and server. But there are a number of weaknesses in Kerberos. It is vulnerable to password guessing attack, replay attack and complex key management. Password guessing attack is main attack in Kerberos. If a user selects a weak password then it is easy for attacker to

guess the password. DH-DSA key exchange can secure the protocol against replay attacks. In this paper an improved Kerberos proposed on optimized DH-DSA. In improved Kerberos protocol, first registration is done to provide mutual authentication between the client and the server. After this the key exchange takes place. In this protocol a third party KDC is used to provide security. This improved protocol only modifies Authentication Service Exchange, but all other parts are same as in Kerberos. In this protocol nonce is used to avoid replay attacks. That message is valid only a particular time, noncethat message becomes invalid. By using improved Kerberos protocol password guessing attack and replay attack are avoided.

Dhanya R. Sarath, Megha V. Ainapurkar (2014) said that it is necessary to authenticate users before exchanging the data or information over the unsecured channel. Zero-knowledge proofs are those protocols in which no information is revealed during the protocol or to any attacker. In this paper an improved FFS identification scheme is proposed with complete zero-knowledge and almost zero soundness error. This scheme is based on FFS digital scheme. Main aim of this scheme is that even if attacker guesses the challenge, it should not be able to impersonate and not be able to find the secret. This new FFS scheme uses SHA-1 to generate hash function. In this scheme an array of challenge is used to generate the keys. Classical FFS works on Ali Baba's cave. There are only two Challenges in classical one, 0 or 1. So it is easy to attacker guess the challenge. There are 0.5 probability of attacker to guess the password. To overcome this problem an array of challenges is used to generate the keys. In new FFS scheme is based on complete zero knowledge and almost soundness error. Result of completeness is that honest verifier always accepts proof from honest user. This scheme is more secure than classical FFS. Even if attacker guess the challenge, it will very difficult to impersonate the attacker. In this scheme soundness error is very negligible.

PRESENT WORK

To transfer the data from one user to another one, we use communication channel. All personal, banking information, file, images and data are transferred over communication channels. This communication channel can be unsecured. There can be many attacks over the information shared over unsecured channel. Man-in-the-middle attacks, replay attacks, password guessing attacks are common today over communication channels. To send data in secure way over communication channel authentication protocols are used. In this only authorized users can access the data or get the information shared over communication channel. There are so many attacks, which attacker can apply over authentication protocols. Man-in-the-middle attack and replay attack are common attacks over authentication protocols in published papers. To provide security from these types of attacks in authentication protocols is one of the hottest research areas in network security.

3.1 PROBLEM FORMULATION:-

In this section, the process of problem formulation is discussed below.

We found that single algorithm is not enough to provide security in communication between two parties. We have seen that key shared using DH protocol can be compromised in between the communication. Attacker can change the value of shared key in between the sender and receiver, which is known as MITM attack.

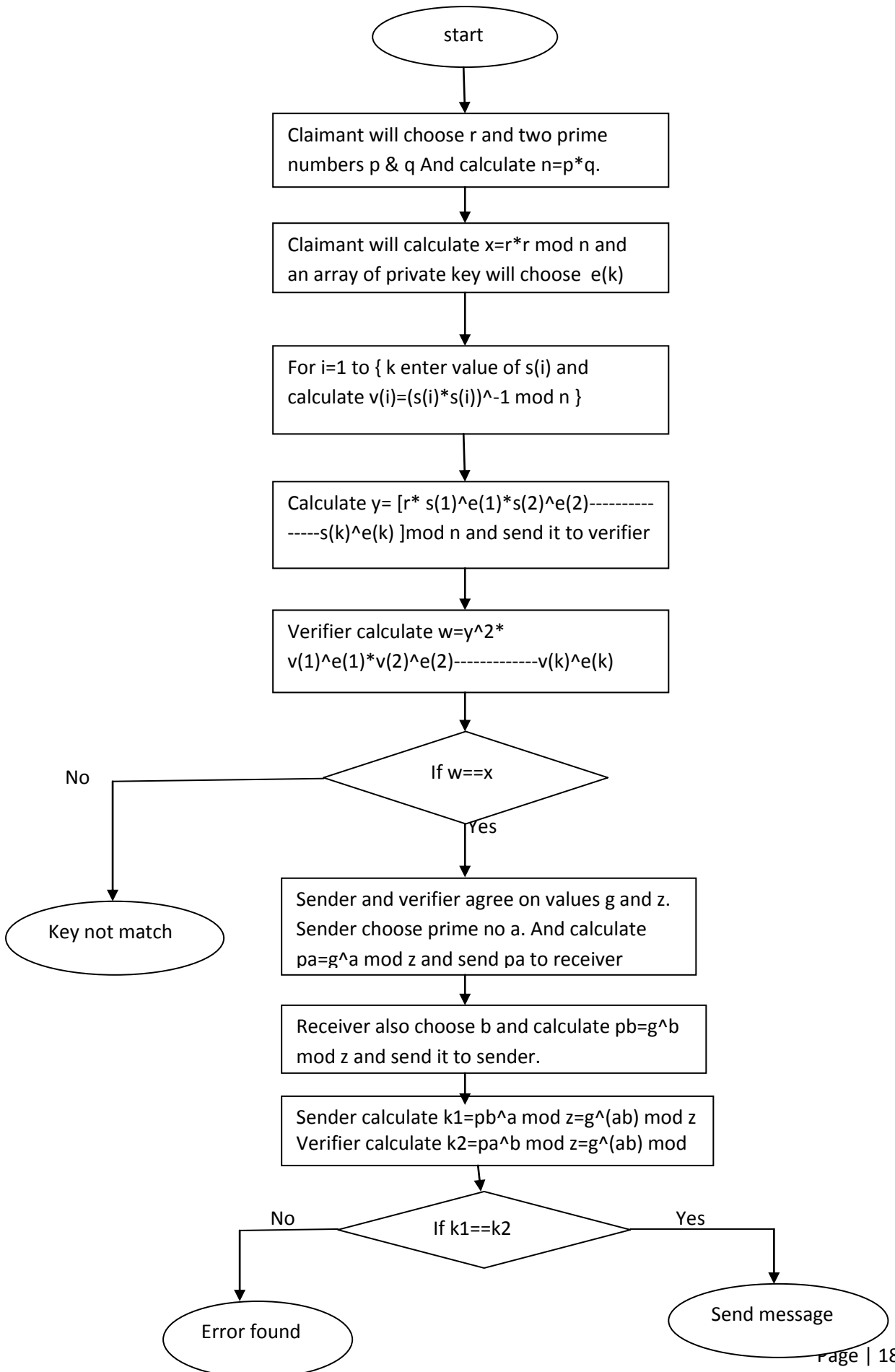
To remove this MITM attack in DH protocol, we are using FFS algorithm with the DH protocol to verify the parties involved in the communication. To provide more security in DH protocol against MITM attack we are combining this protocol with the FFS algorithm.

PROBLEM OBJECTIVE:- An improved technique to prevent man-in-the-middle attack in Diffie-Hellman protocol using Feige-fiat Shamir algorithm.

3.2 OBJECTIVES OF THE STUDY:-Following are the various objectives of this research work.

1. The study focus on analysis of DH protocol and attack over it.
2. To study the man-in-the-middle attack over DH protocol and its countermeasures.
3. To study the previously proposed plans suggested for counter measurement of man-in-the-middle attack over DH protocol.
4. To propose new scheme to prevent man-in-the-middle attack and to improve performance of DH protocol.

3.3 RESEARCH METHODOLOGY:- In our methodology we are using FFS algorithm with DH protocol to provide security to the DH protocol. In our methodology we have two parts. First one is verification and another one is key sharing for communication between sender and the verification using DH protocol. If users are verified in first part then only second phase will be implemented otherwise key sharing will not take place. To provide security or to eliminate MITM attack this methodology is used.



VERIFICATION:- this is the first phase of our methodology. In this sender and receiver are verified using FFS algorithm. This section describes the feige-fiat-shamir algorithm, which is used to provide authentication in the Diffie-Hellman protocol.

Feige-fiat-shamir algorithm:- there are six steps to implement this algorithm. There are two parties in the scheme. One is claimant and other one is verifier.

1. Claimant choose random number r and n . Claimant calculates $x = r^2 \pmod n$.
2. X is known as witness and claimant send it to verifier.
3. Verifier chooses an array of challenges $(e_1, e_2, e_3, \dots, e_k)$. Verifier sent this array to claimant.
4. Claimant use array of their private keys (s_1, s_2, \dots, s_k) and calculates $y = (r * s_1^{e_1} s_2^{e_2} s_3^{e_3} \dots s_k^{e_k}) \pmod n$.
5. Y is known as response and claimant sent it to verifier.
6. Verifier compares the value y to the $(y^2 v_1^{e_1} v_2^{e_2} v_3^{e_3} \dots v_k^{e_k}) \pmod n$. If both values are same then key will be shared otherwise no key will be shared.

KEY SHARING FOR COMMUNICATION:- After verifying the parties using this algorithm key is shared in DH protocol. This technique prevents the protocol from man-in-the-middle attacks.

DH protocol:- There are some steps which are used in DH protocol. Sender and receiver first agree on a large prime number n and an element g ($2 \leq g \leq n-2$) that generates a cyclic subgroup of large order. Rest steps of the protocol are following.

- Sender chooses a number, x , at random from the set $\{1, 2, \dots, n-2\}$. And receiver chooses y randomly from the same set.
- Sender sends g^x to receiver and receiver sends g^y to sender.
- The shared secret key is $K = g^{(x*y)}$. Sender, knowing x and g^y , can easily calculate $(g^y)^x = g^{(x*y)}$. Receiver can determine the secret key in a similar manner by computing $(g^x)^y = g^{(x*y)}$.

x and y are referred to as the private keys, g^x and g^y are referred to as public keys and $g^{(x*y)}$ is called as shared secret key.

RESULTS AND DISCUSSIONS

In this section, results of the proposed research work have been discussed. The results are shown using MATLAB tool. MATLAB tool is used for mathematical and applied science programming work. MATLAB is an easiest tool for programming. MATLAB allows matrix manipulation, implementation of algorithm, mathematical works also. MATLAB also provides interfacing with the programs written in different programming languages. The name MATLAB stands for matrix laboratory. MATLAB also provides GUI (graphical user interface). In MATLAB graphs can be plot using different variables In MATLAB inbuilt mathematical functions are available. We can pick the function from the toolbox.

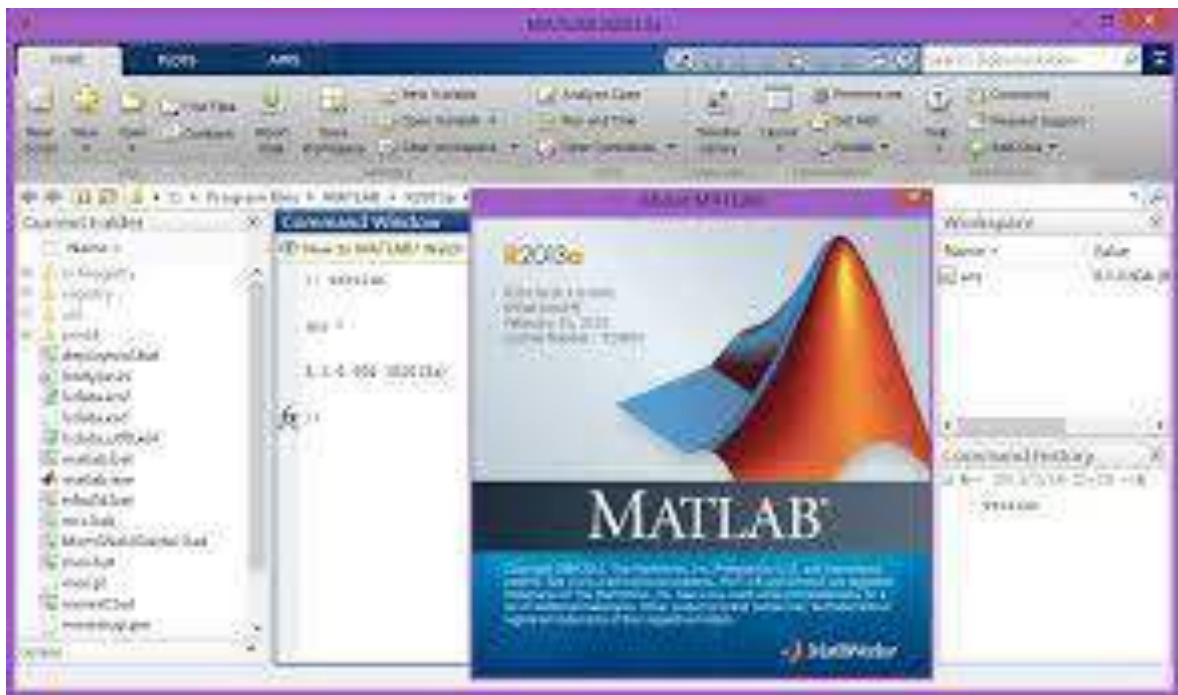


Figure 13 MATLAB

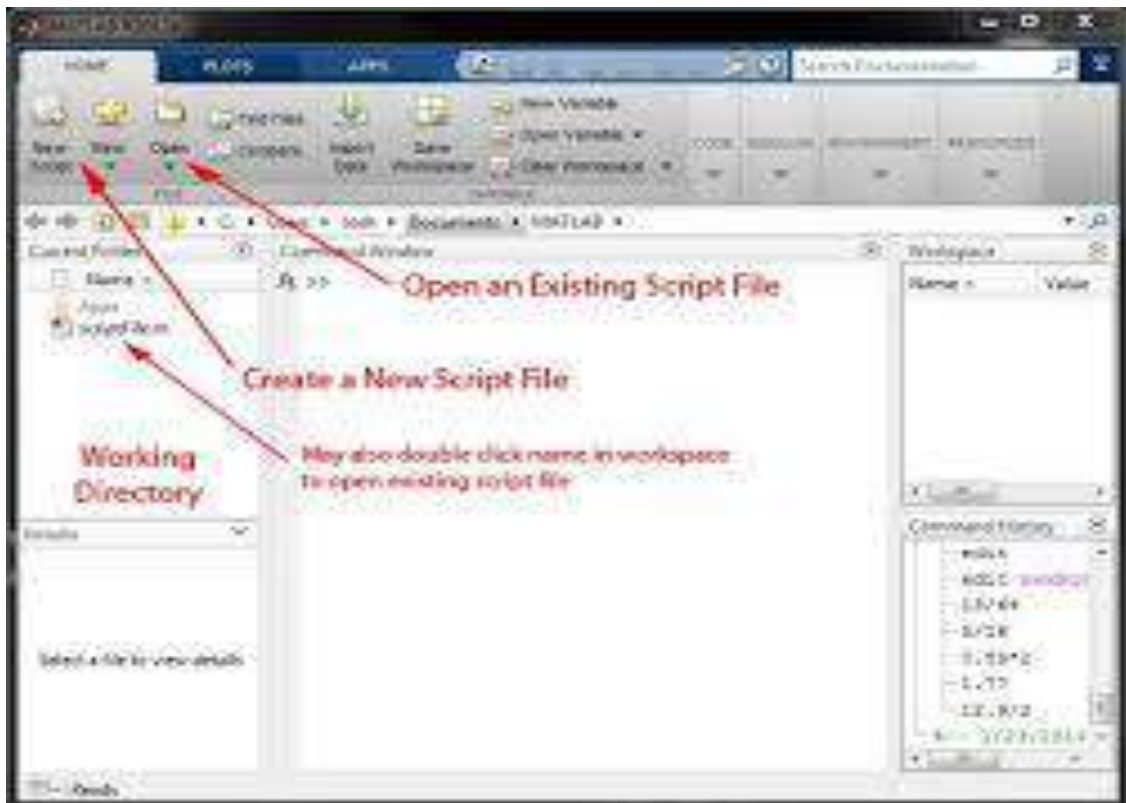



Figure 14 MATLAB introduction



Figure 15 MATLAB workspace



```
1 function sequence=collatz(n)
2 % collatz problem. Generate a sequence of integers resulting in 1.
3 % For any positive integer, n
4 %   Divide n by 2 if n is even
5 %   Multiply n by 3 and add 1 if n is odd
6 %   Repeat for the result
7 %   Continue until the result is 1
8
9 sequence = n;
10 next_value = n;
11 while next_value > 1
12     if (rem(next_value,2)==0)
13         next_value = next_value/2;
14     else
15         next_value = 3*next_value+1;
16     end
17     sequence = [sequence, next_value];
18 end
```

Figure 16 command window

MATLAB is used for these applications.

- Math and computation.
- Algorithm development.
- Simulation, prototyping and modelling.
- Graphical user interface building.
- Data analysis.
- Scientific and engineering graphics.

MATLAB system consists of five main parts, MATLAB language, MATLAB working environment, Graphics, Mathematical functions, Application protocol interface. In MATLAB we can plot the graph between the variables. In the MATLAB files are saved with .m extension. Figures are saved in the MATLAB with .fig extension. MATLAB is very easy to implement. We can implement any algorithm in it. Mathematical functions are inbuilt so we need not to evaluate any function or to define any function in it.

In MATLAB we have matrix manipulation. MATLAB is case sensitive. It understands the difference between lower case and upper case variables. In this we need not to define

variables first before using it unlike other languages. We also need not to define data type of the variables in the MATLAB.

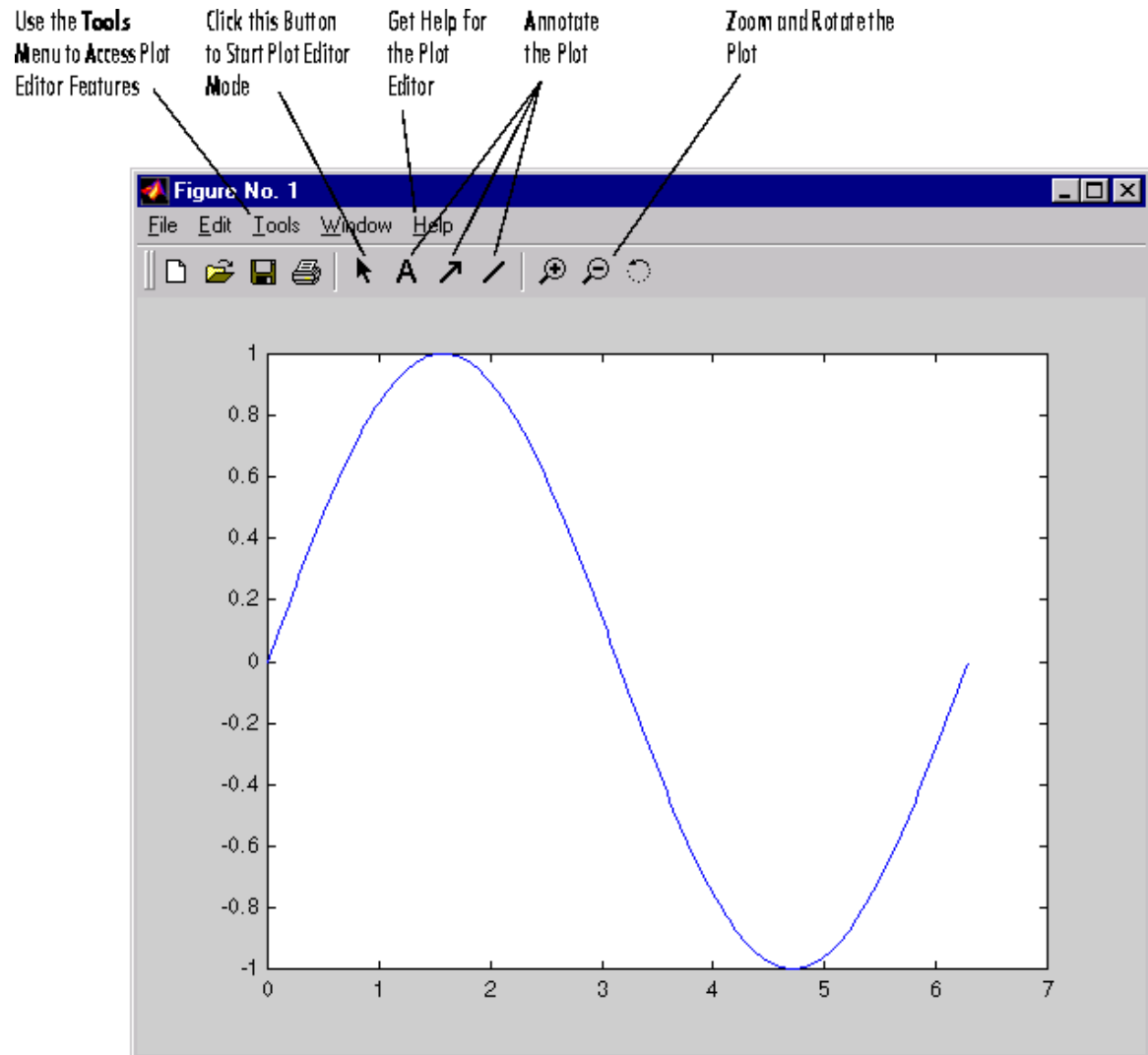


Figure 17 Graph in MATLAB

In MATLAB we use conditional and unconditional loops like other languages. We can use MATLAB for simulation of the model. In the MATLAB we have Simulink library. By using this library we can create different types of model in MATLAB and can simulate them.

In the Simulink library components of models are differentiated on the basis of use in area. There are so many areas in the simulink like communication, hydraulic, mathematics, motion etc.

MATLAB algorithm for security does:

- Extract the man in the middle attack.
- Verifies the communicating parties.
- Key sharing between the parties.
- Compares the key of the parties.

Here are some results of our proposed work using MATLAB:

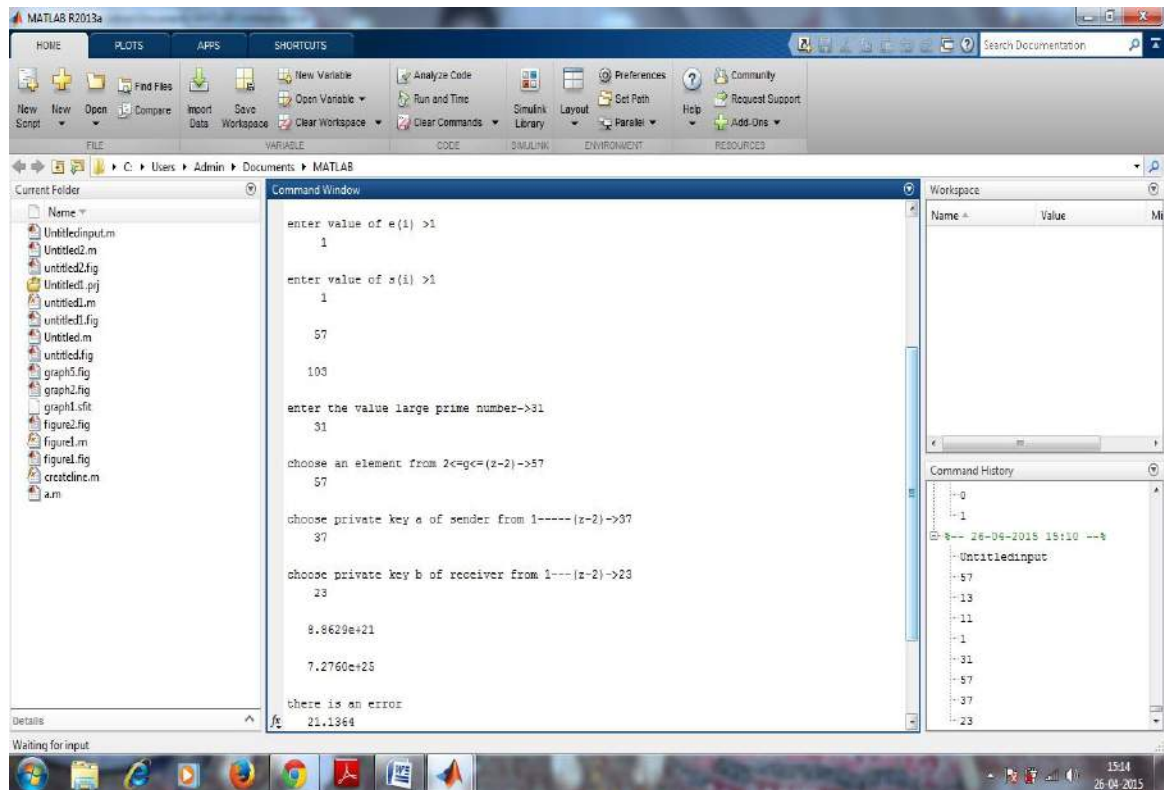


Figure 18 Output

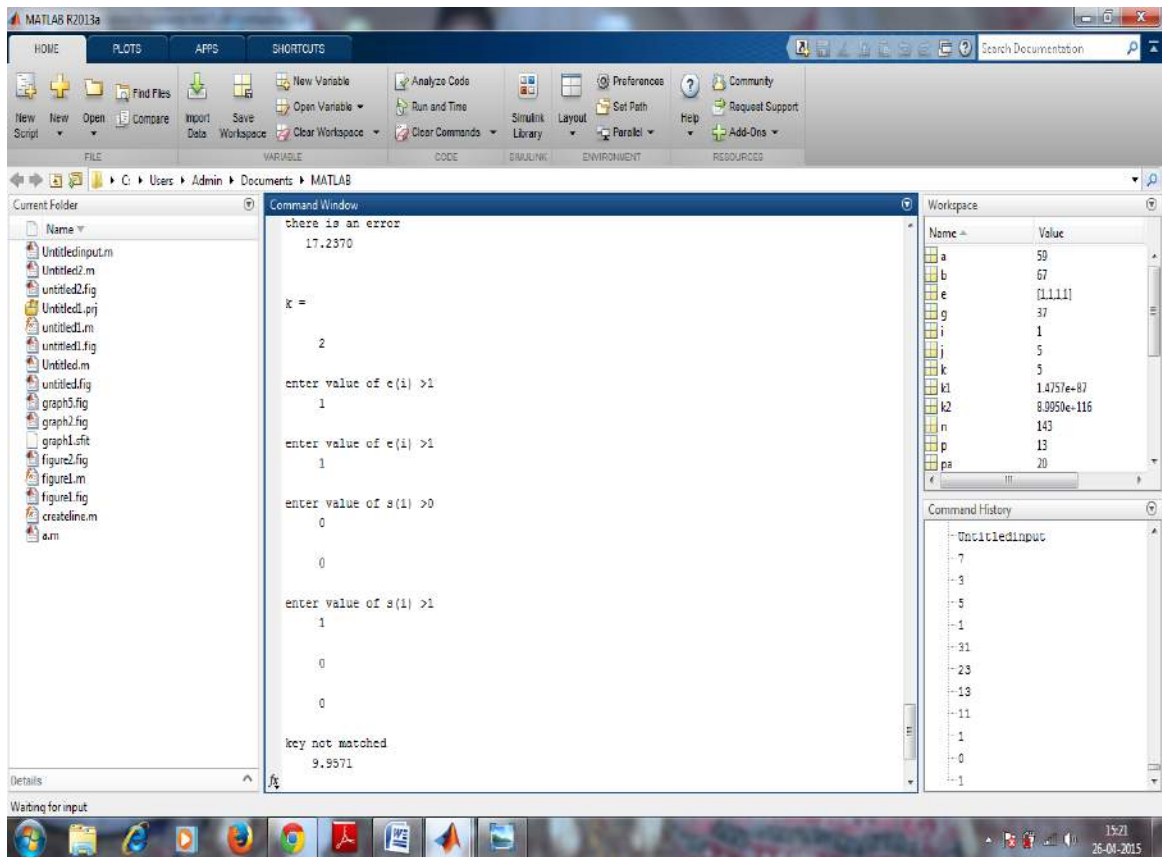


Figure 19 Output 1

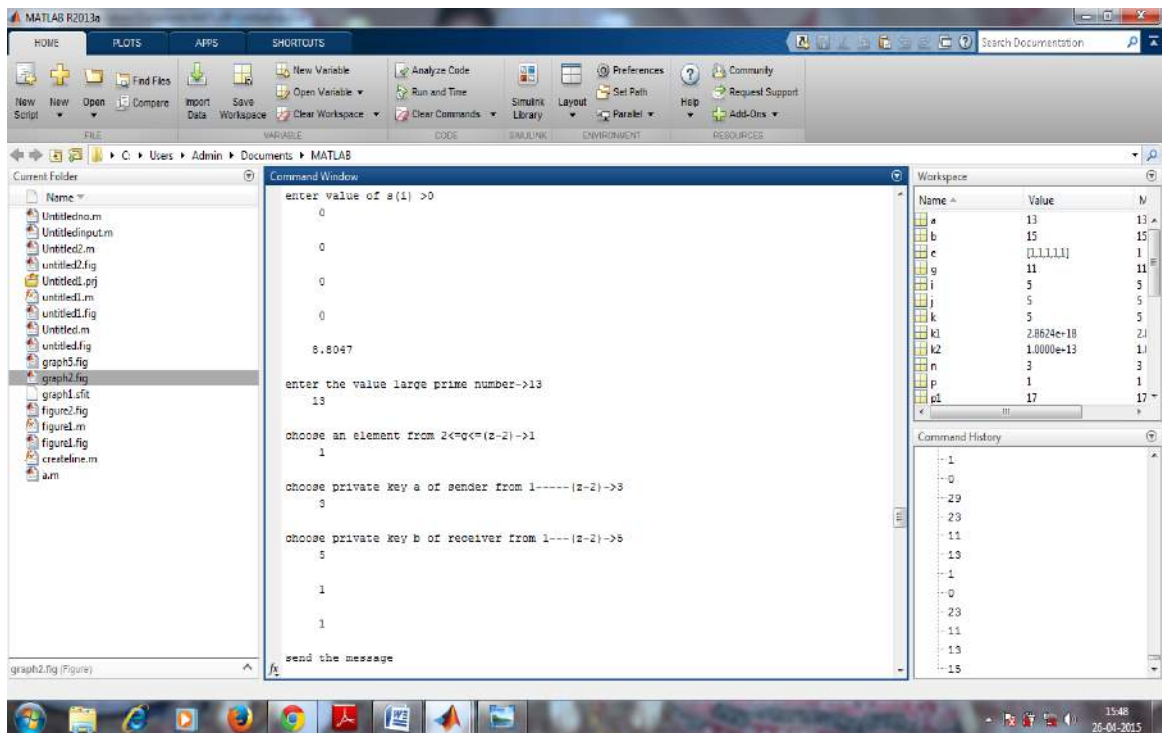


Figure 20 Output 2

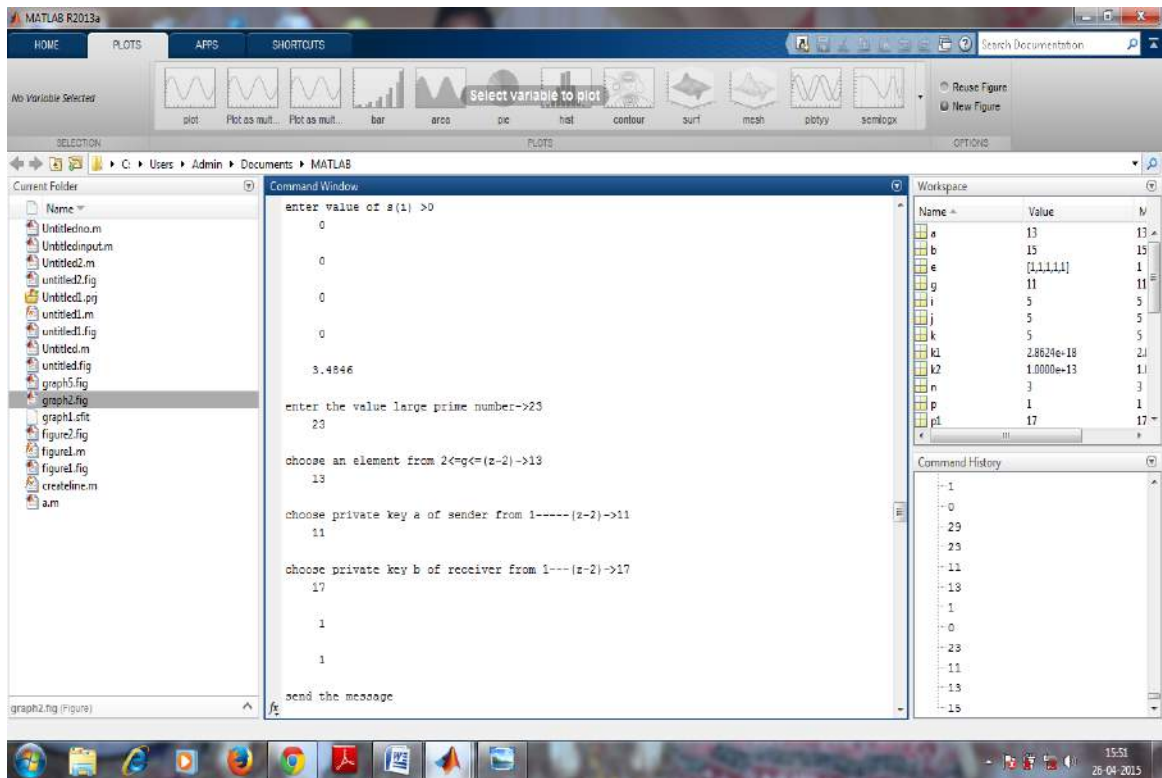


Figure 21 Output 3

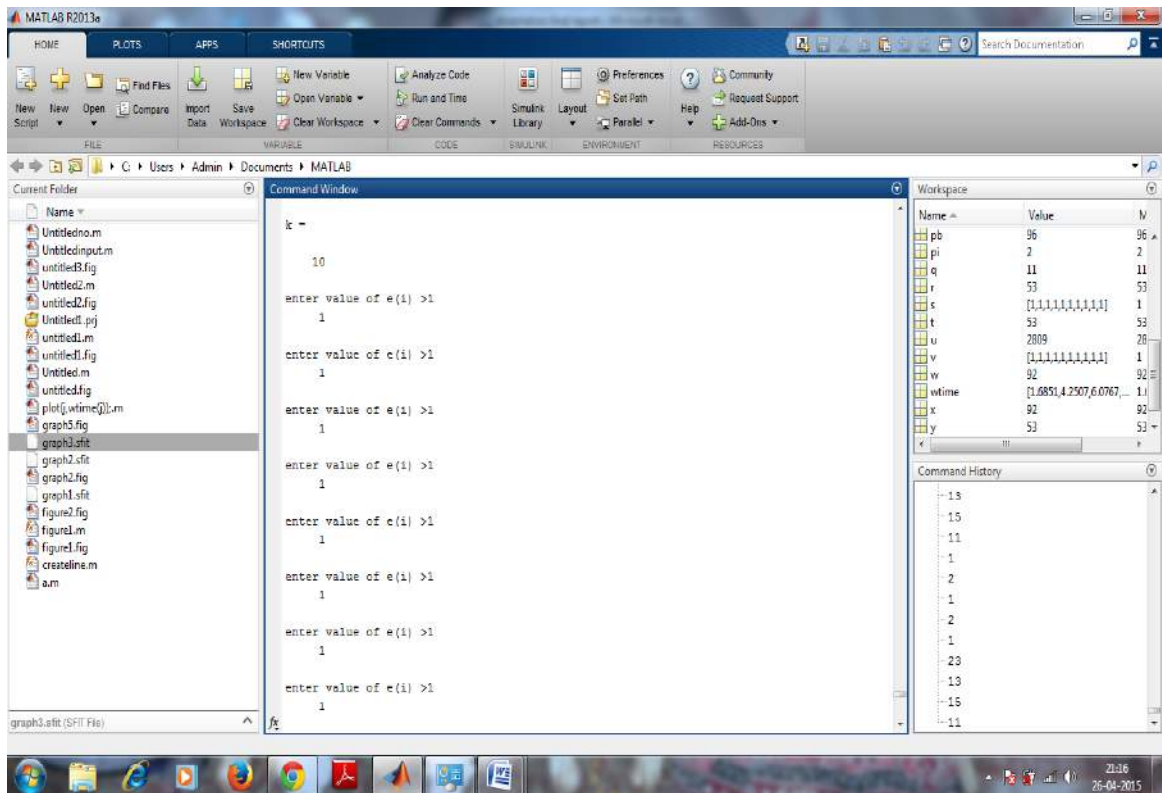


Figure 22 Output 4

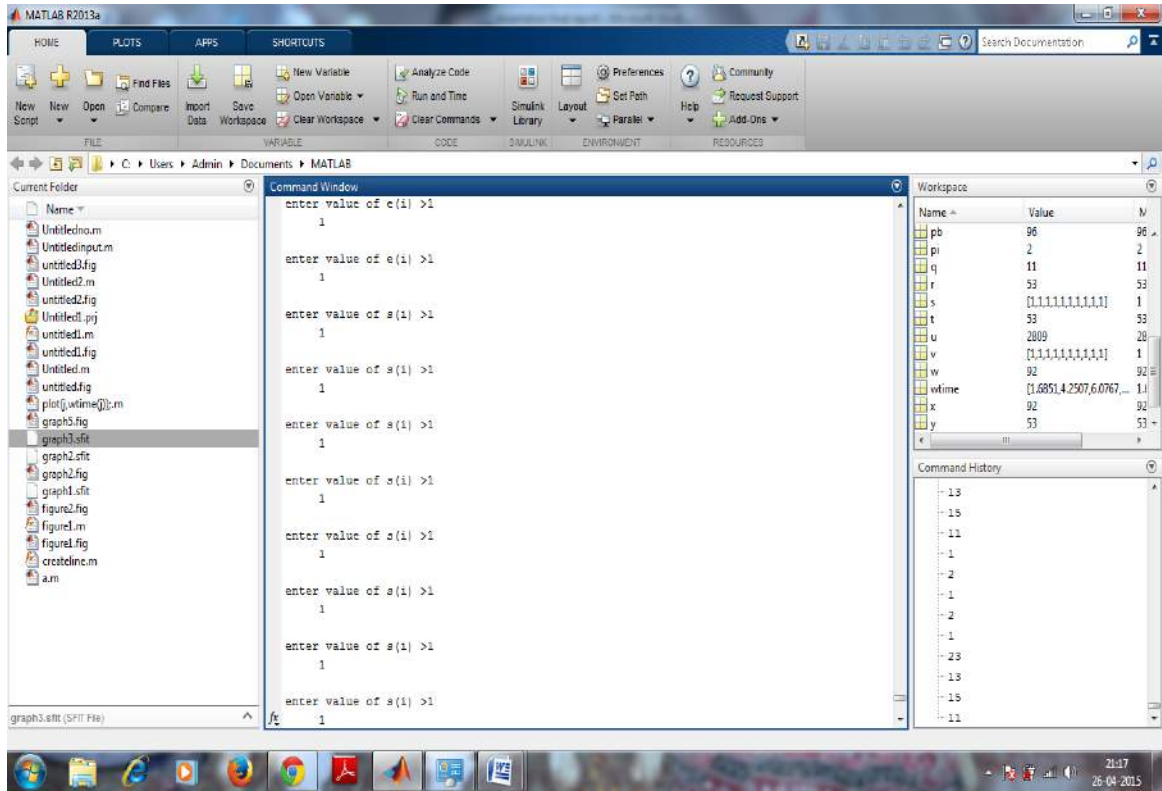


Figure 23 Output 5

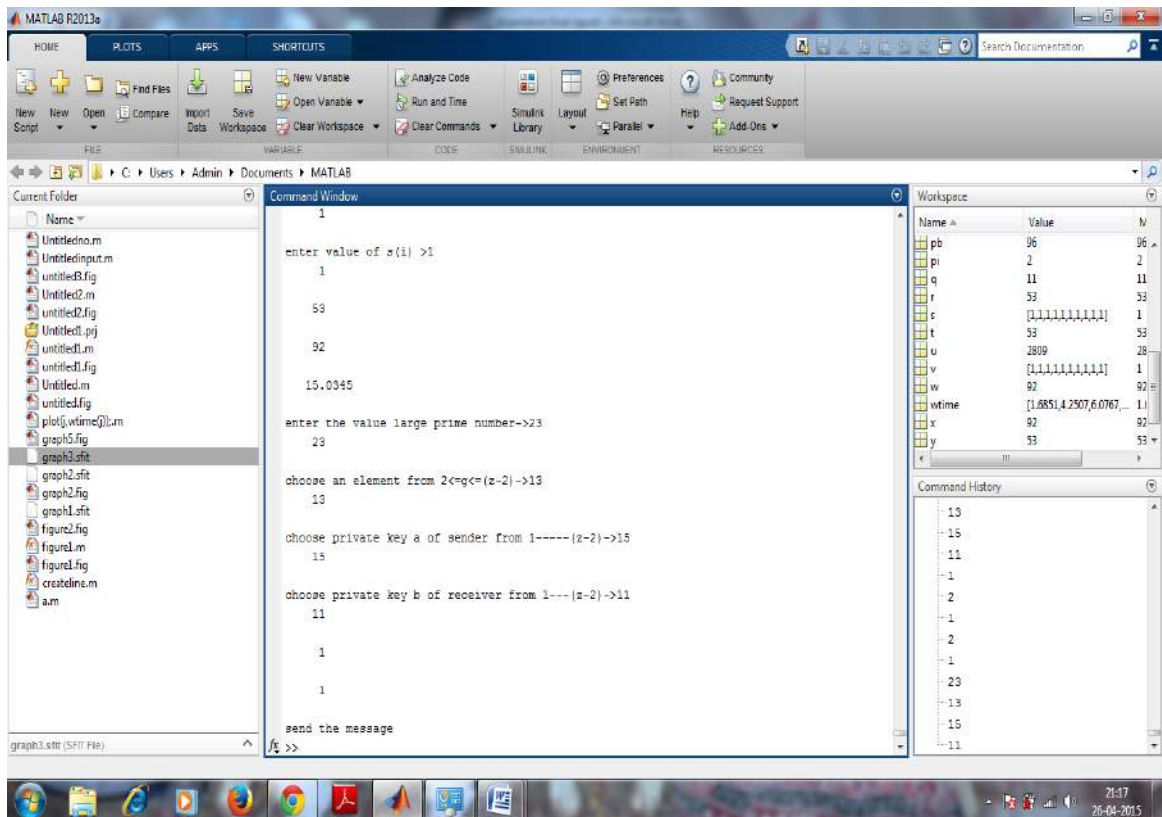


Figure 24 Output 6

Graph for time evaluation:-

Graph 1:- when k=5

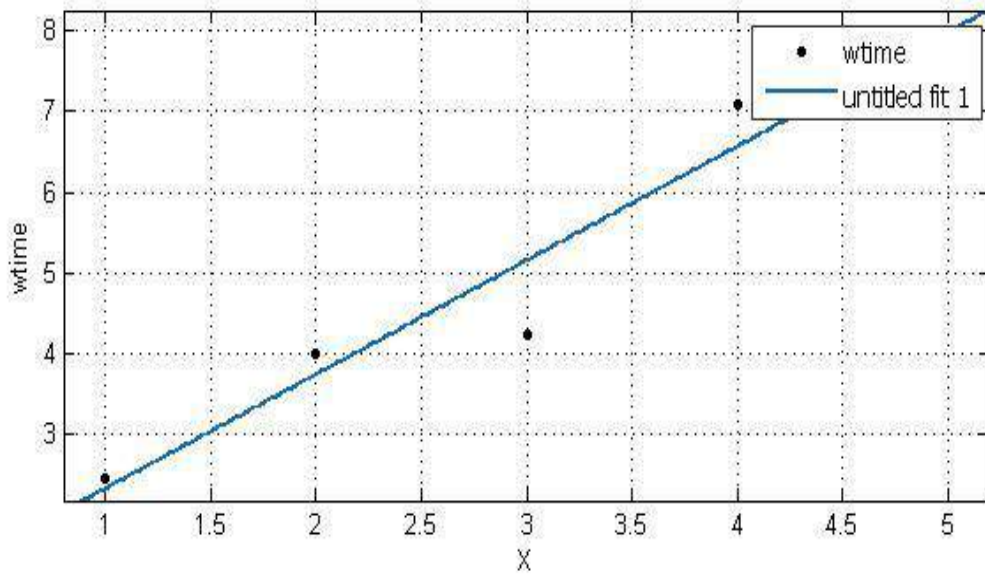


Figure 25 Graph 1

Graph 2:- when k=10

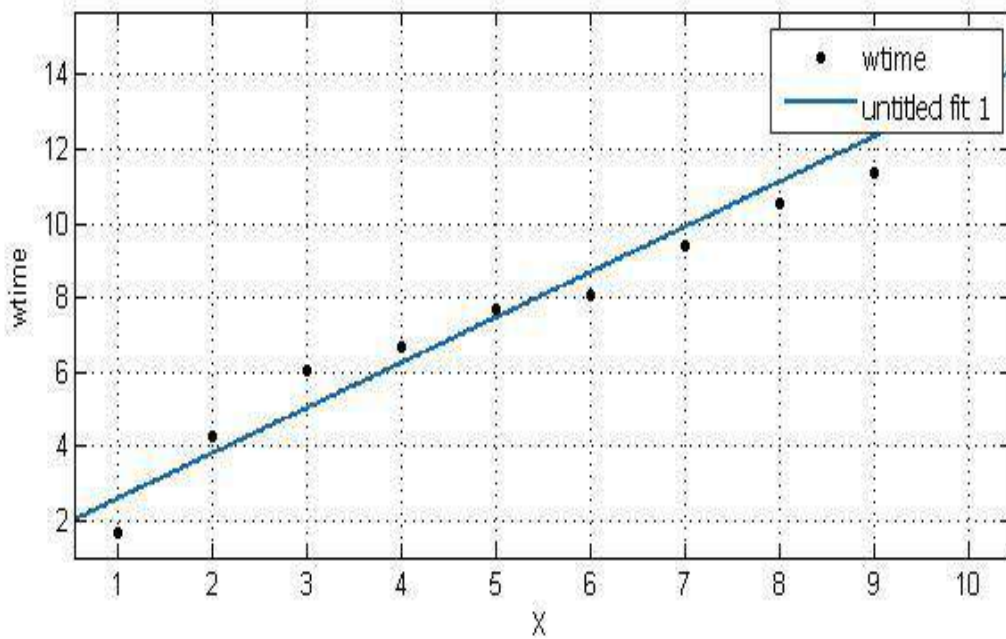


Figure 26 graph 2

In the results, we have seen that the output is different for different inputs. If verifier verifies to the claimant then only steps of DH protocol executed. If claimant is not verified then steps of DH protocol do not execute. And output is “key not matched”. So on the basis of this output, it can be verified either there is an attack or not.

If claimant verified by the verifier. Then DH protocol is used to share the key between the parties. There are two possibilities in the DH protocol also if shared key matched then message sent by the sender otherwise not. In our result we make graph between number of X and wtime (evaluation time). We have shown that there is no linear relation between the X and wtime.

As the value of X increases in the array evaluation time also increases. But it is not linear increment. So we can use it in future for our research work. In the future research work, we can research on the evaluation time of the algorithm. In the original FFS algorithm, time was constant for all values. But in our proposed work, when we are using this FFS algorithm with the DH protocol then time is increasing with the value X.

In the above diagram we can see that man in the middle attack can occur on DH protocol. To remove man in the middle attack we are using FFS algorithm with the DH protocol. With the FFS algorithm verifier verifies to the claimant. Once both the parties are verified then only key sharing with the DH protocol takes place. If claimant is not verified the no key sharing will take place.

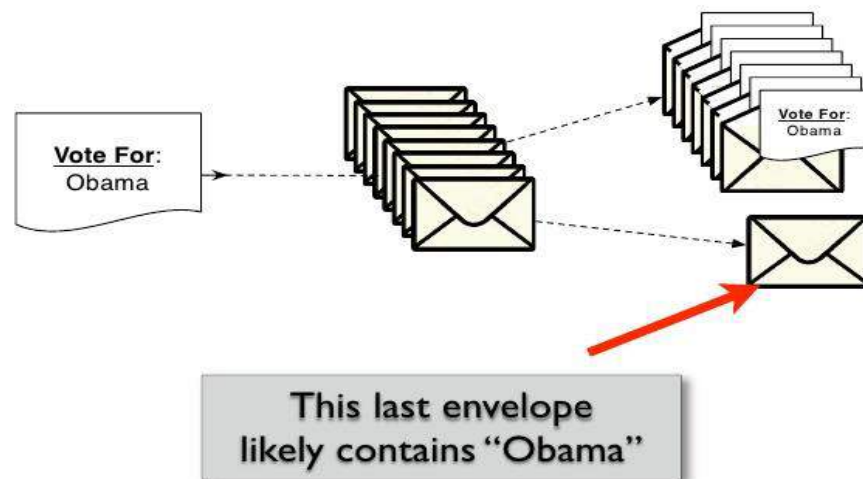
There are the some parameters which we got in our proposed work.

MITM attack:- By using this proposed technology, no MITM attack will take place in the DH protocol. In this technology verifier and claimant both are verified before key sharing. No attacker can attack between the communications. In this we have k number of values to verify the claimant and verifier. FFS algorithm is advanced version of Fiat algorithm. In our algorithm we have an array of k values while in main algorithm only two values are possible for private key (0 or 1). It is very easy for attacker to guess the value of e. Only 2 values are possible so attacker can guess value easily. There is 0.5 Probability of successful attacks. This works upon Ali Baba’s cave theory.

Zero knowledge:- zero knowledge proof also available in this algorithm. Zero knowledge proofs are those protocols in which no part of information disclosed itself during the

protocol. In our technology no part of information is revealed during the protocol so zero knowledge proof is available in this protocol.

Zero-Knowledge Proof



9

Figure 27 Zero knowledge proof

Completeness:- our protocol also provides the completeness property. Completeness is that property in which verifier always receives a proof from the claimant to prove him that he is the right one. In our FFS algorithm verifier always verify claimant before proceeding to the key sharing.

These are the results of our proposed research work. In which we use two algorithms. First one FFS algorithm for verifying the parties and other one is DH protocol for key sharing between the parties involved in the communication.

Our FFS algorithm is more secure than original algorithm. Property of original algorithm was zero knowledge and time. Zero knowledge property is maintained in our proposed algorithm also. The evaluation time increases with the number of values in array. There is no constant relationship between the values of x and evaluation time unlike original algorithm.

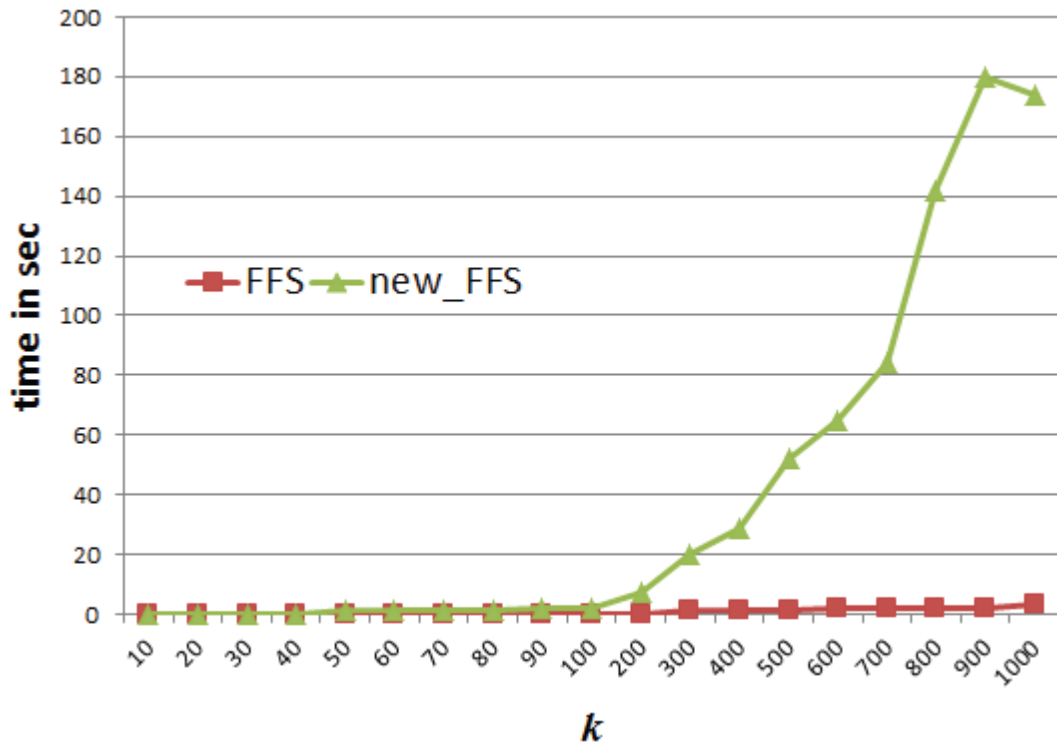


Figure 28 Base paper graph

In our base paper, time is constant for some values of X. After that value time increased with the increment in value of array size. But in our algorithm, it is safer than the original one. But it takes more time than the original one.

Animation:-

Diffie-Hellman Protocol

Choose prime number g, n and x
Calculate $X = g^x \text{ mod } n$



Figure 29 snapshot 1

Diffie-Hellman Protocol

Choose prime number g, n and x
Calculate $X = g^x \text{ mod } n$

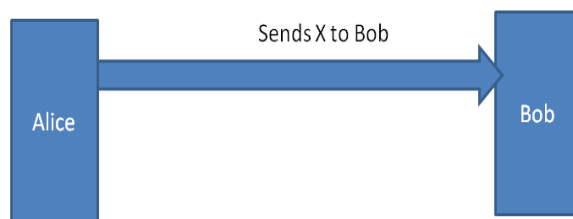


Figure 30 Snapshot 2

Diffie-Hellman Protocol

Choose prime number g, n and x
Calculate $X = g^x \text{ mod } n$

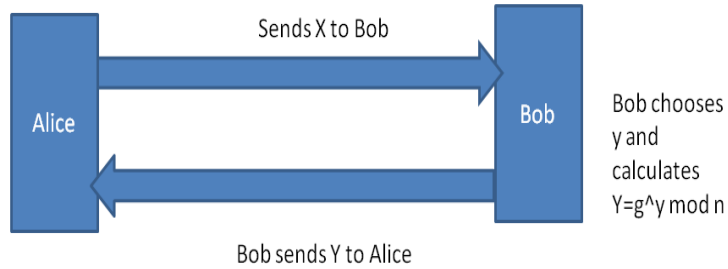
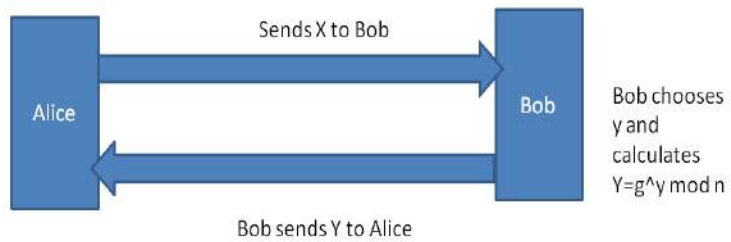


Figure 31 Snapshot 3

Diffie-Hellman Protocol

Choose prime number g, n and x
Calculate $X = g^x \text{ mod } n$

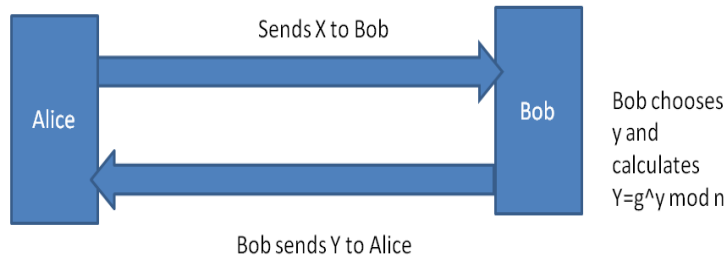


Alice calculates
 $K = Y^x \text{ mod } n$
 $= g^{xy} \text{ mod } n$

Figure 32 Snapshot 4

Diffie-Hellman Protocol

Choose prime number g, n and x
Calculate $X = g^x \text{ mod } n$



Bob chooses y and calculates $Y = g^y \text{ mod } n$

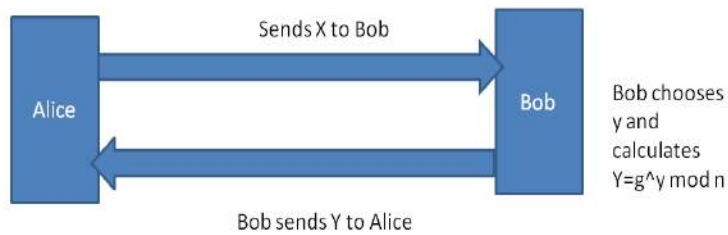
Alice calculates $K = Y^x \text{ mod } n = g^{xy} \text{ mod } n$

Bob calculates $K = X^y \text{ mod } n = g^{xy} \text{ mod } n$

Figure 33 Snapshot 5

Diffie-Hellman Protocol

Choose prime number g, n and x
Calculate $X = g^x \text{ mod } n$



Bob chooses y and calculates $Y = g^y \text{ mod } n$

Alice calculates $K = Y^x \text{ mod } n = g^{xy} \text{ mod } n$

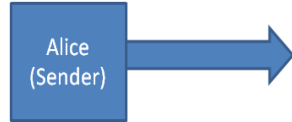
K is shared key between Alice and Bob.

Bob calculates $K = X^y \text{ mod } n = g^{xy} \text{ mod } n$

Figure 34 Snapshot 6

Man in the middle attack

Choose g, n and x
And calculates $X = g^x \text{ mod } n$



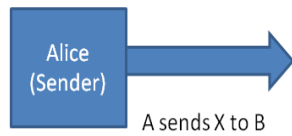
Choose y and calculates
 $Y = g^y \text{ mod } n$



Figure 35 Snapshot 7

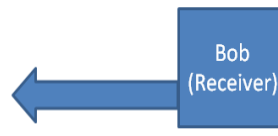
Man in the middle attack

Choose g, n and x
And calculates $X = g^x \text{ mod } n$



A sends X to B

Choose y and calculates
 $Y = g^y \text{ mod } n$



B sends Y to A

Figure 36 Snapshot 8

Man in the middle attack

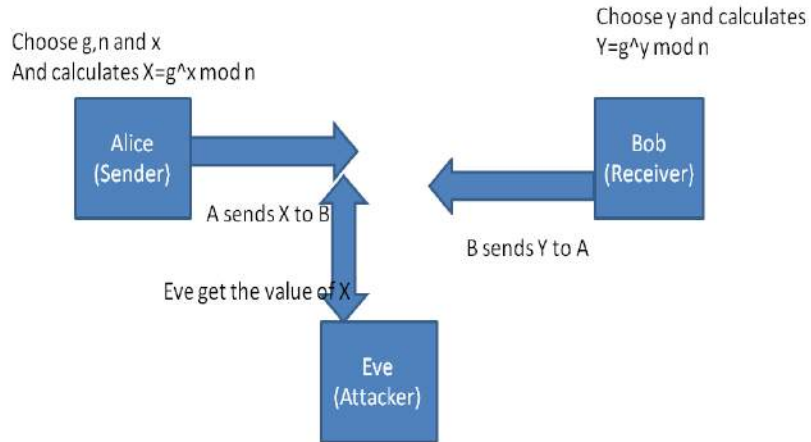


Figure 37 Snapshot 9

Man in the middle attack

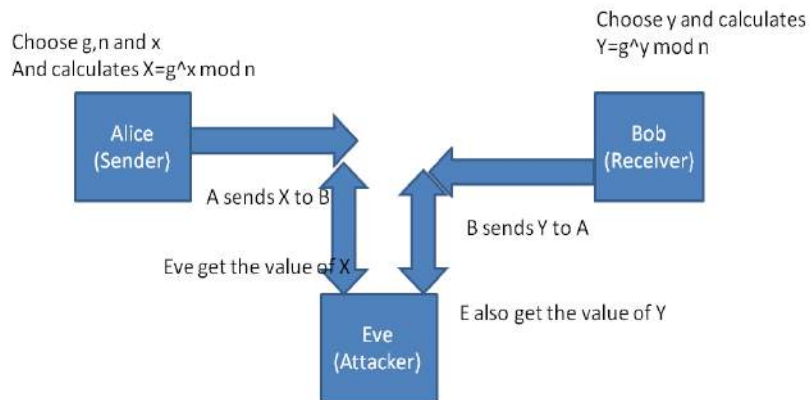


Figure 38 Snapshot 10

Man in the middle attack

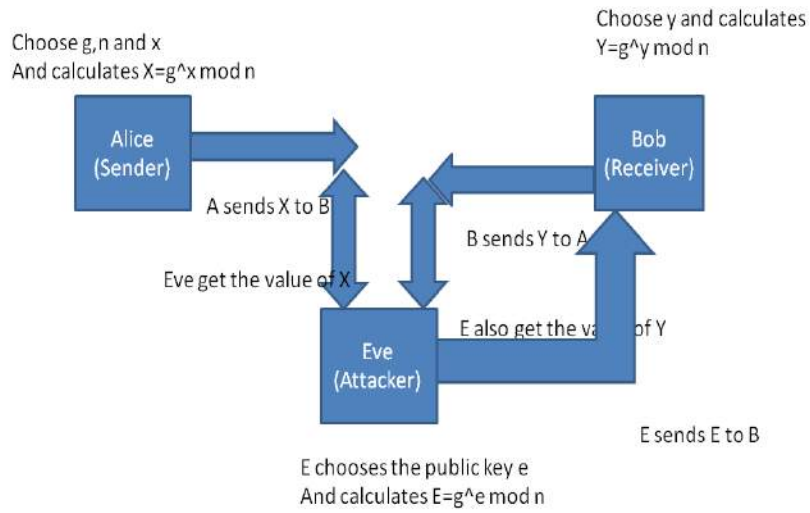


Figure 39 Snapshot 11

Man in the middle attack

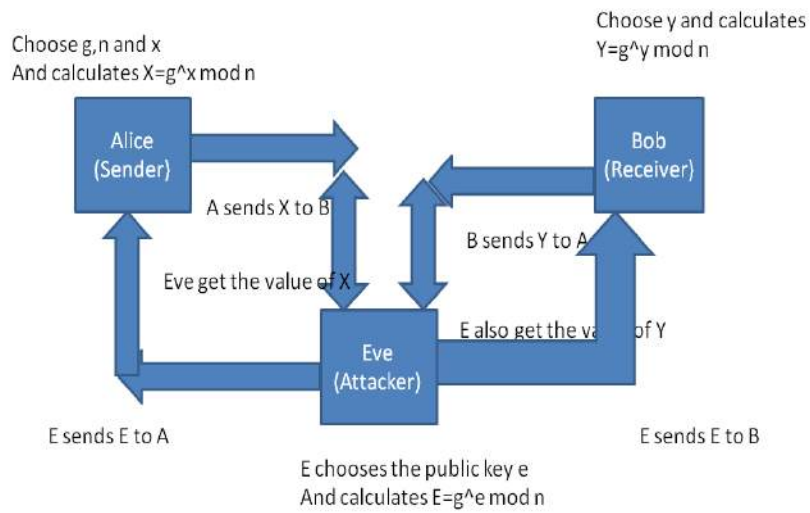


Figure 40 Snapshot 12

Man in the middle attack

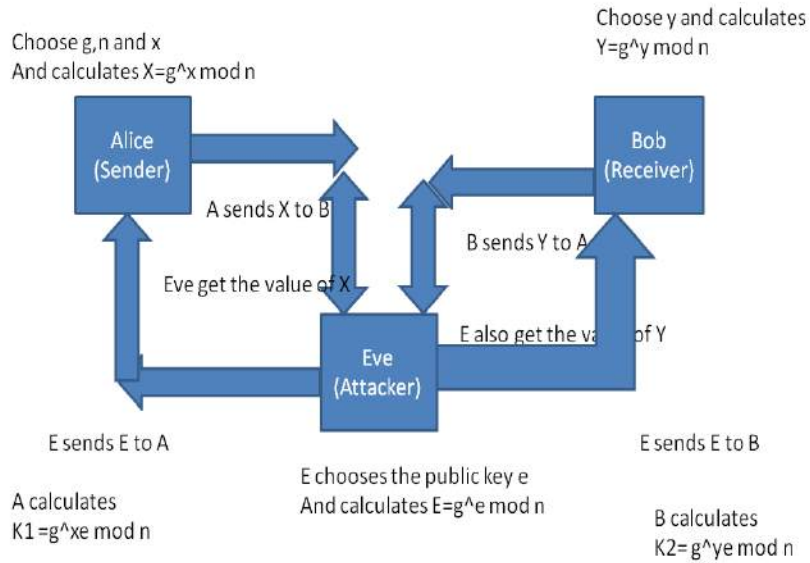


Figure 41 Snapshot 13

Man in the middle attack

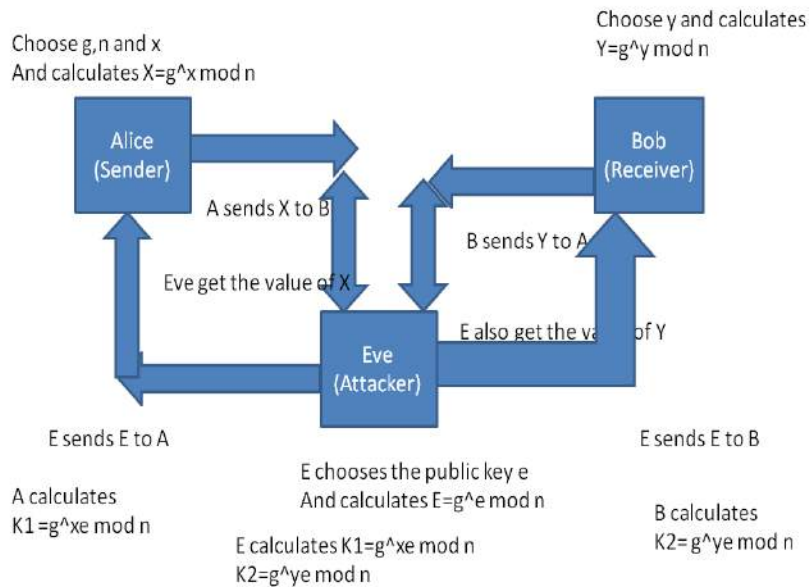


Figure 42 Snapshot 14

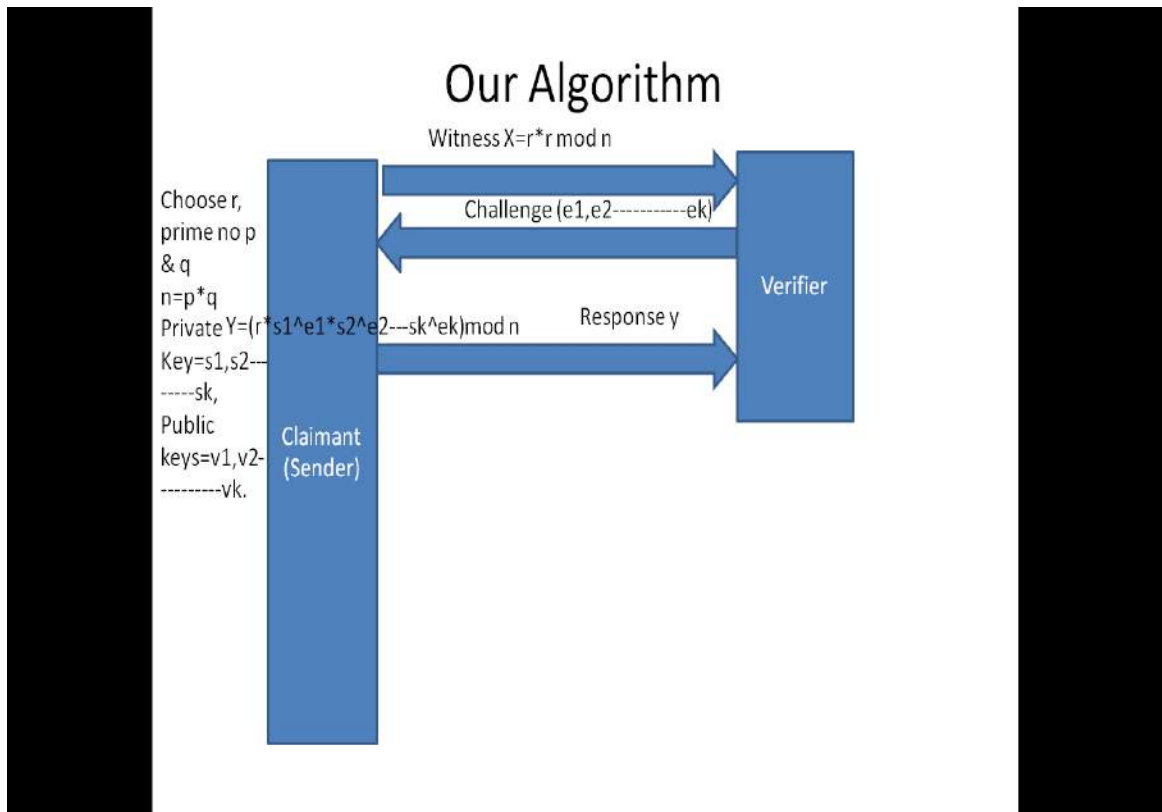


Figure 45 Snapshot 17

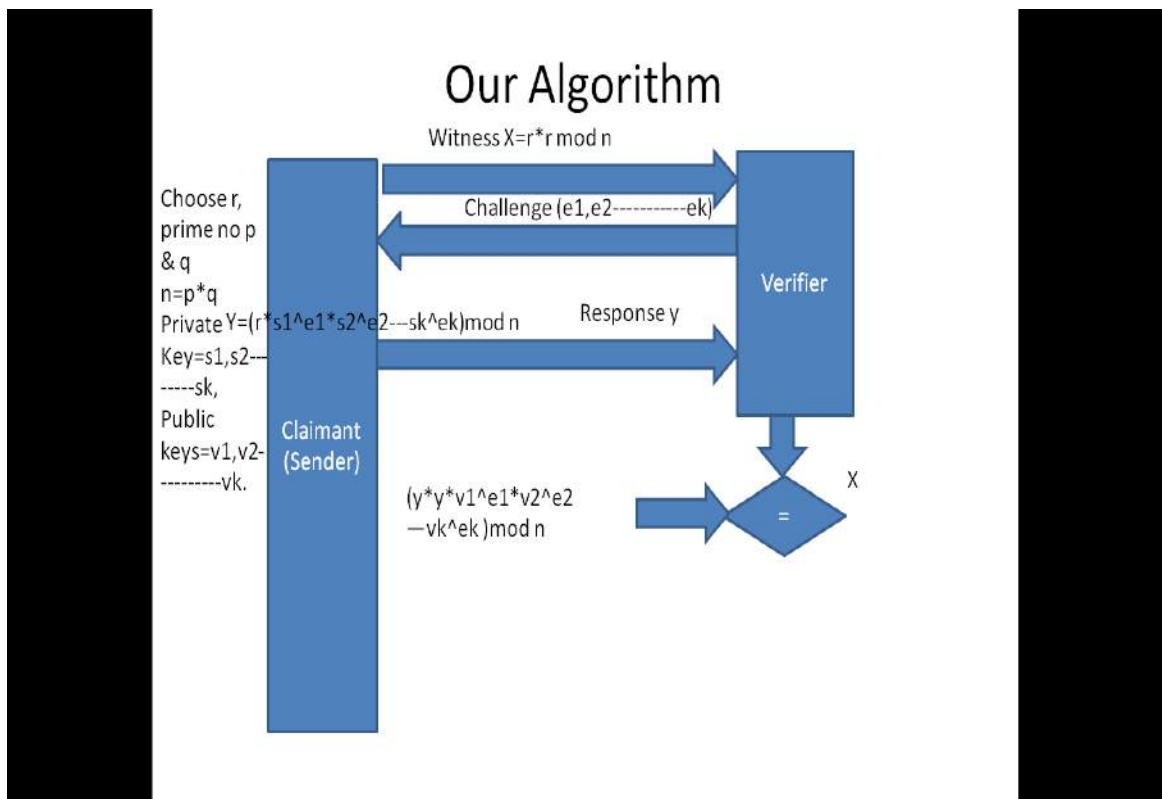


Figure 46 Snapshot 18

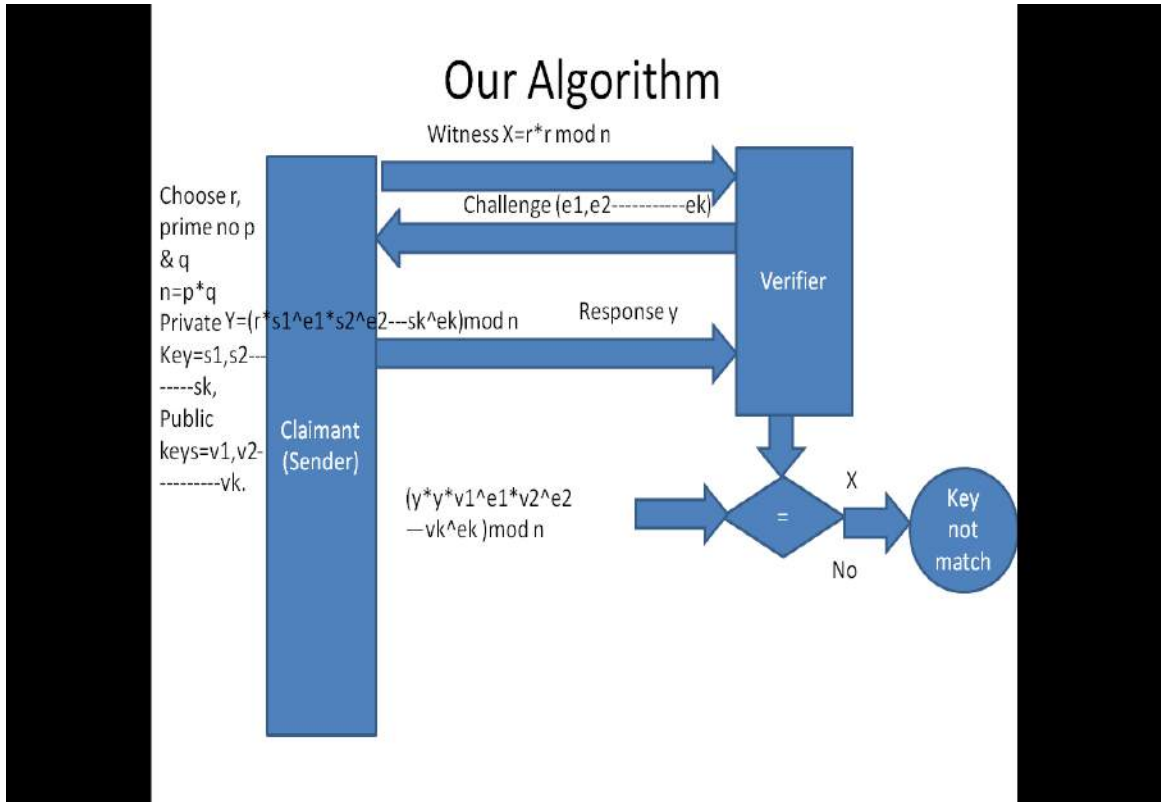


Figure 47 snapshot 19

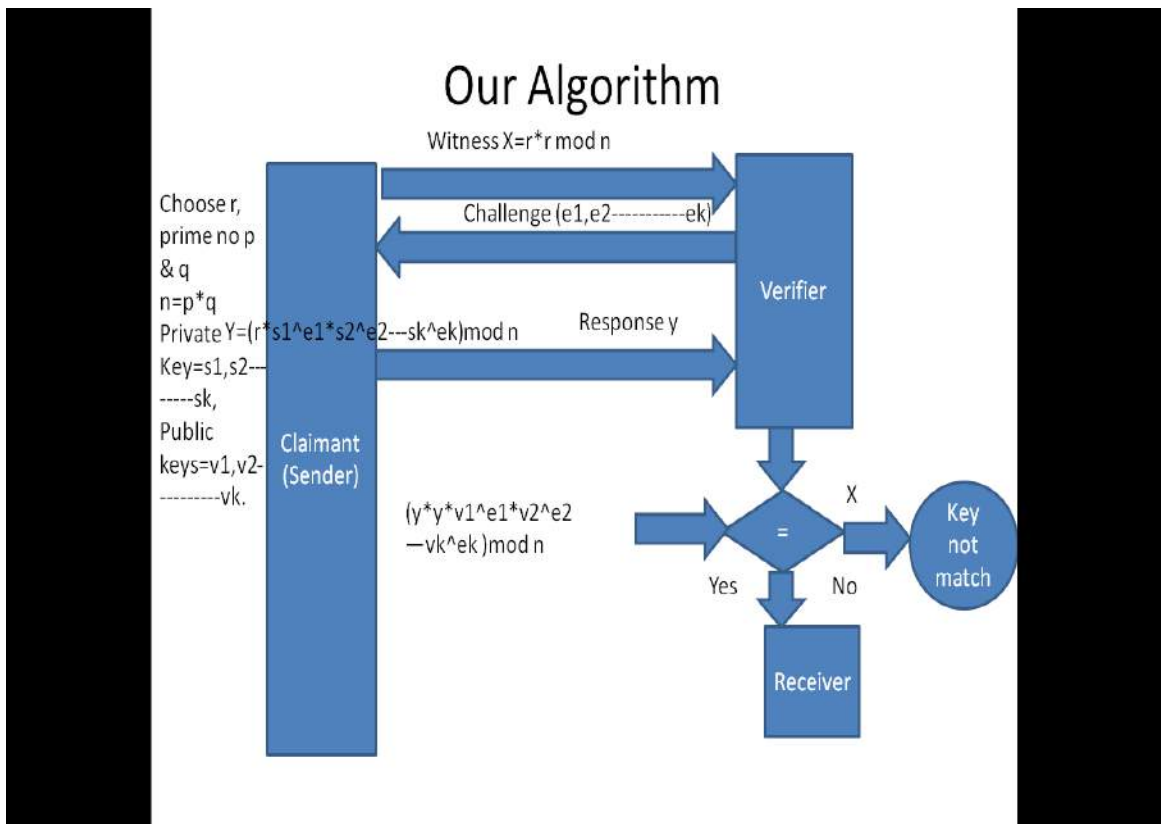


Figure 48 Snapshot 20

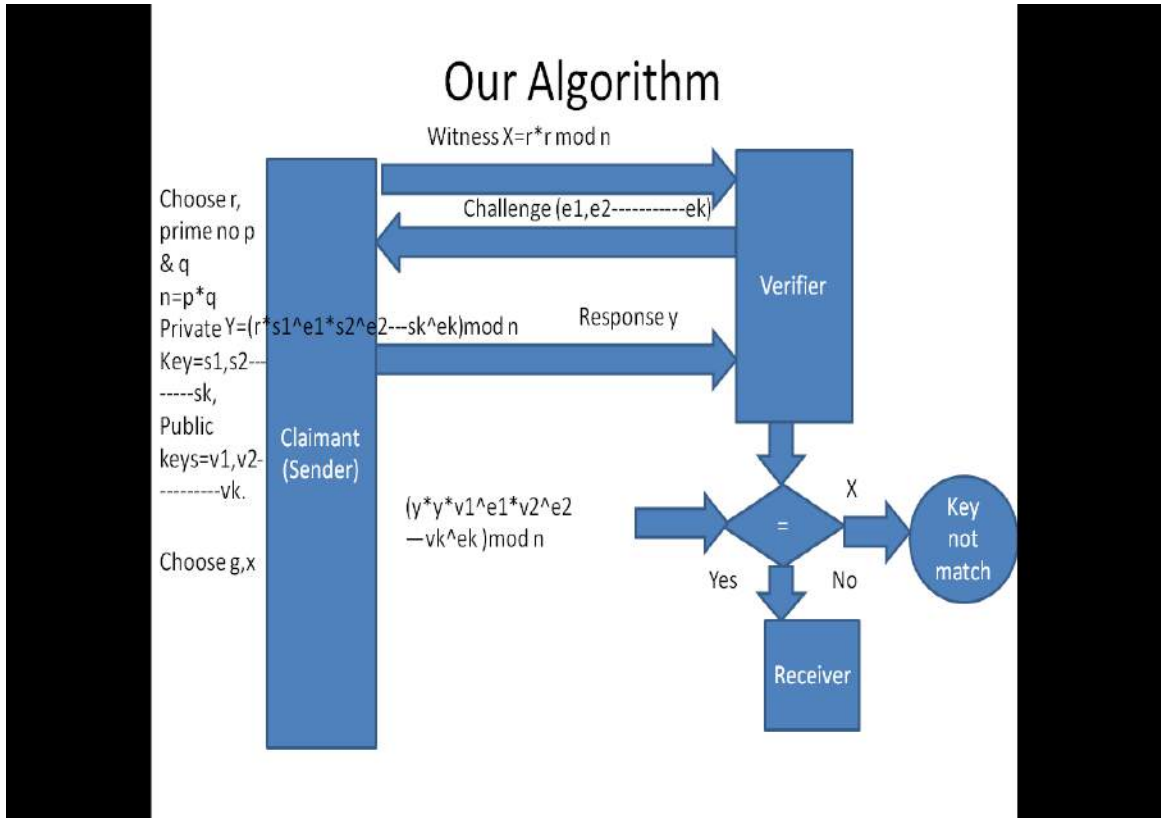


Figure 49 Snapshot 21

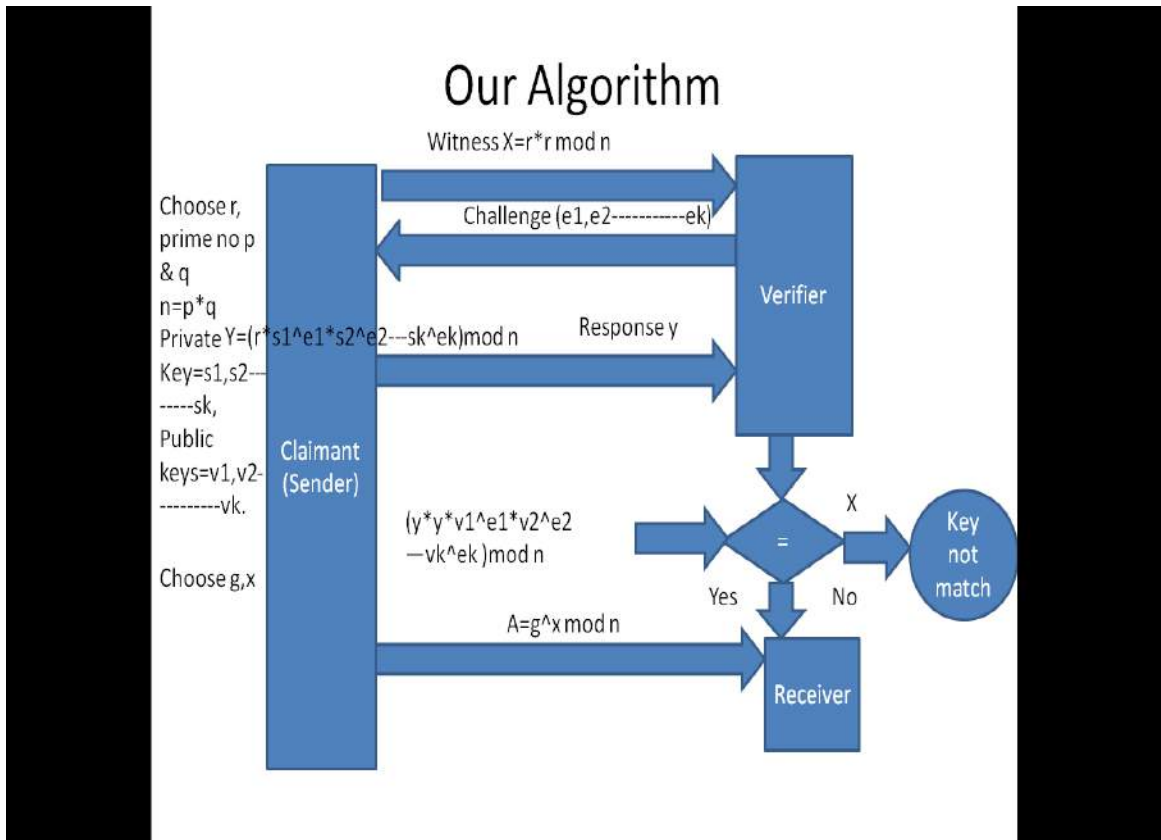


Figure 50 Snapshot 22

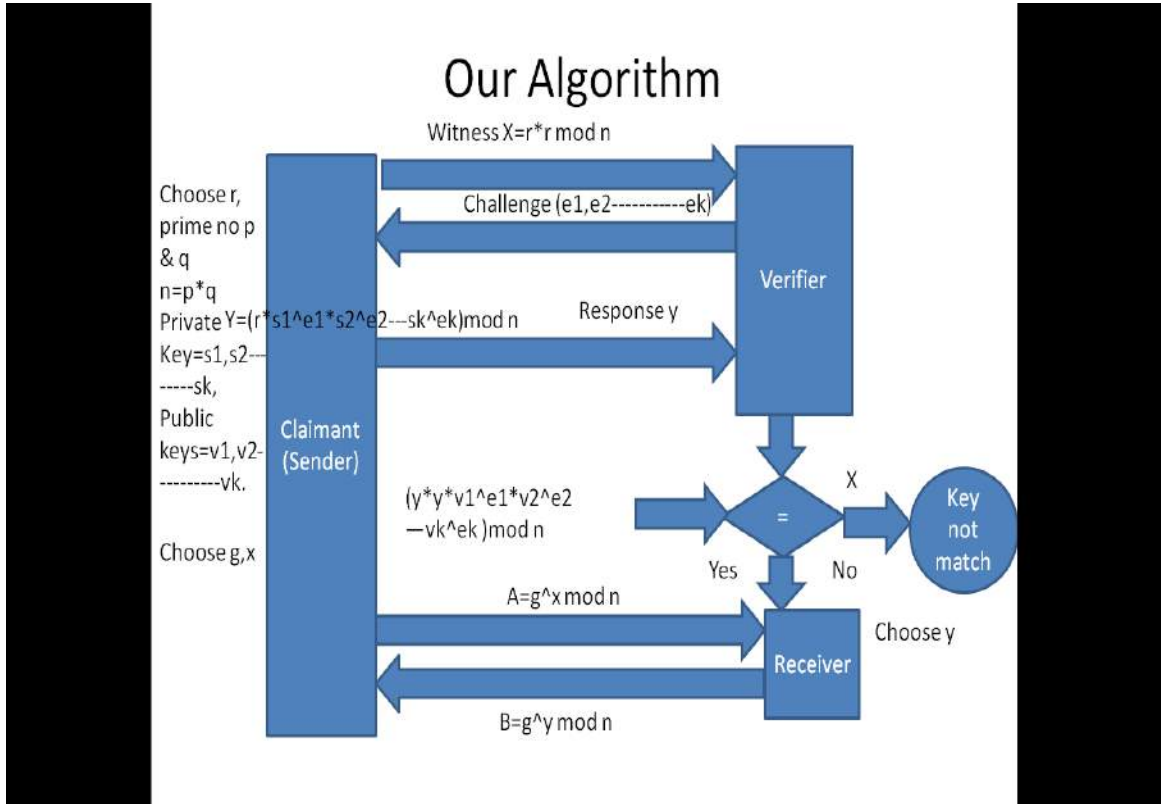


Figure 51 Snapshot 23

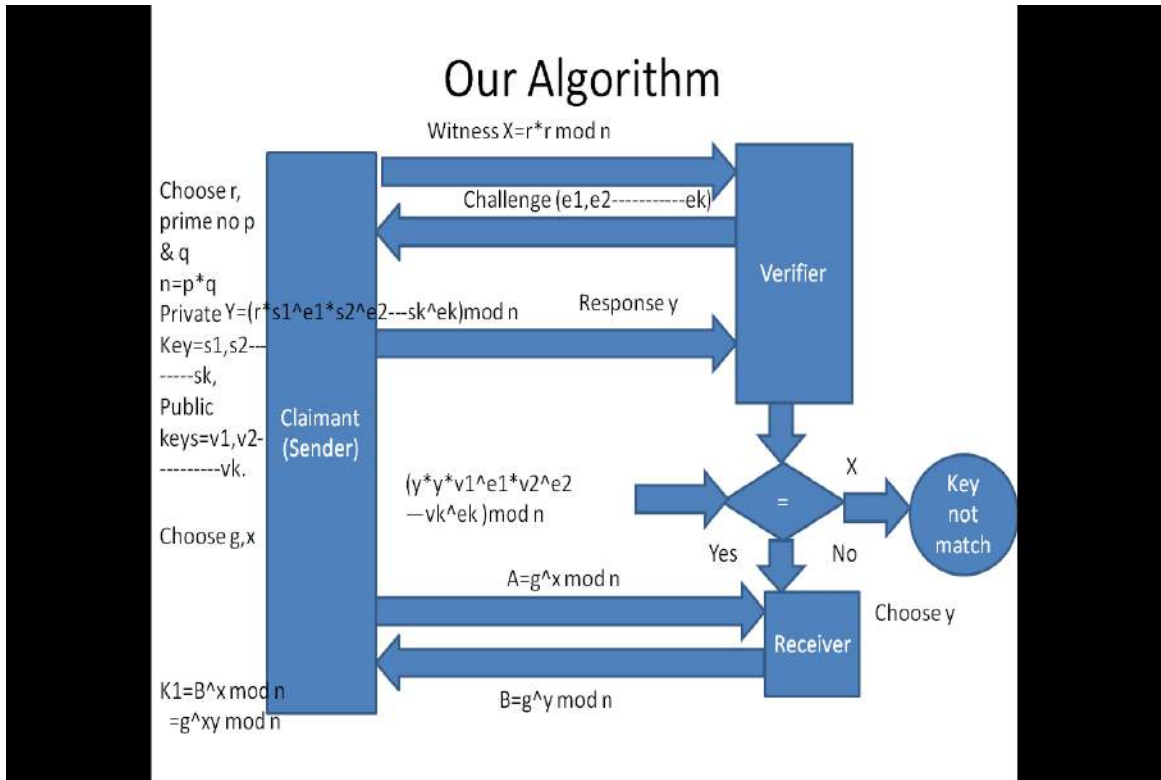


Figure 52 Snapshot 24

Our Algorithm

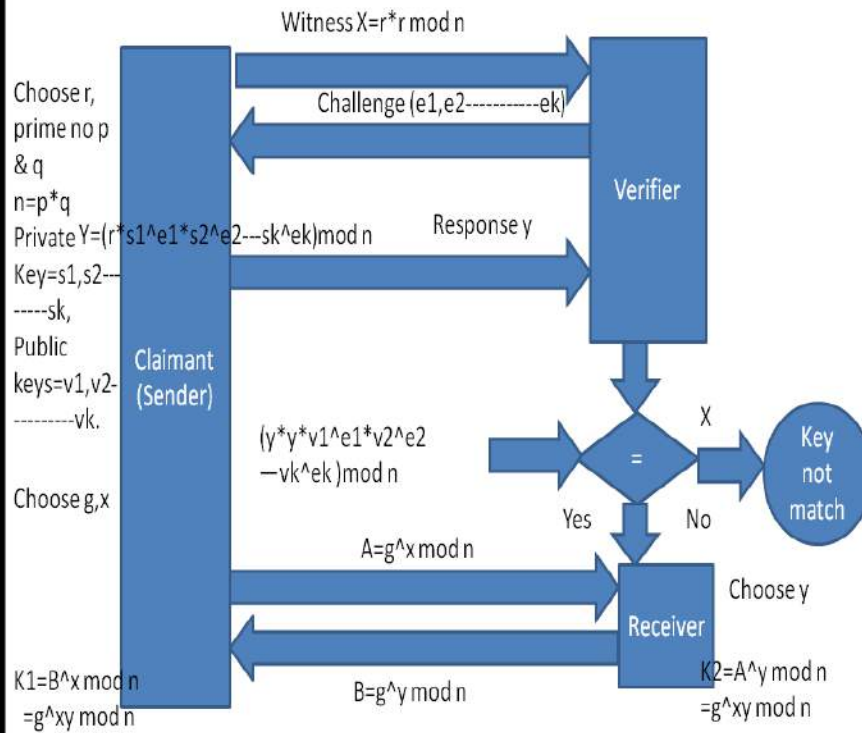


Figure 53 Snapshot 25

Our Algorithm

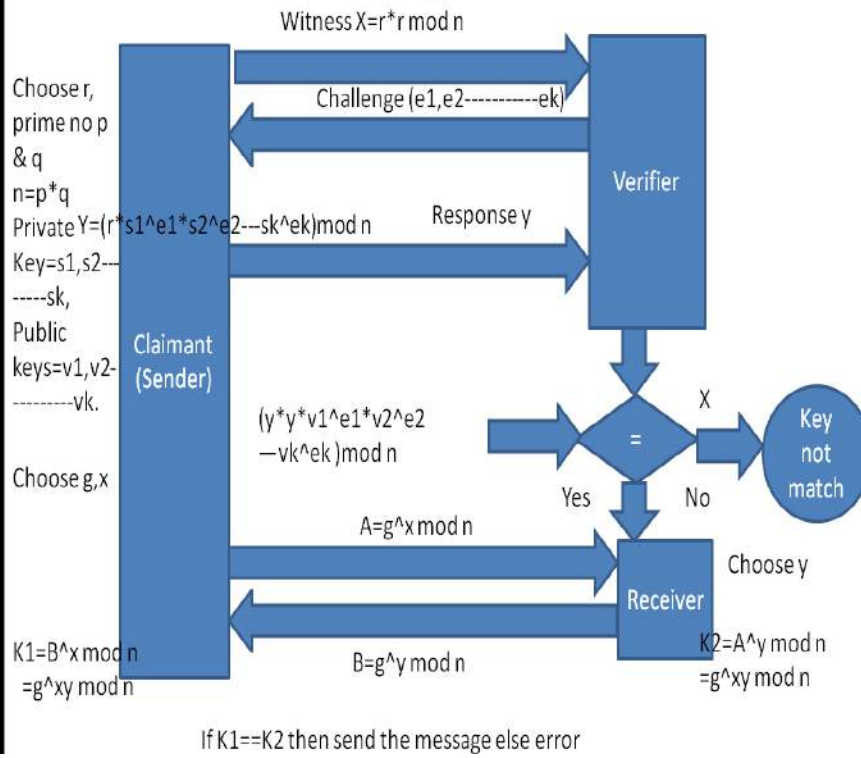


Figure 54 Snapshot 26

CONCLUSION AND FUTURE SCOPE

Diffie-Hellman key exchange protocol is used to share the secret key between the users involved in the communication. But an opponent can guess the secret and get the information shared between the users. There can be password guessing attack, replay attack and man-in-the-middle attack over D-H protocol. To make information confidential between the users authentication protocol is used. In authentication protocol, only authorized users can access the data shared between the parties. To prevent the authentication protocol from MITM attacks Feige-fiat-Shamir algorithm is used. By using this algorithm attacker will not get the information shared between the parties. By using this technique attack can be removed from the protocol. Security can be increased using this technique. By using this technique, D-H protocol can be safer.

FUTURE SCOPE:-in the previous section, result and discussion we have seen the graph between the array size X and evaluation time (wtime). In that graph we have seen that evaluation time increased with the increment of array size. There is no continuous relationship of time and array size. So we can use this problem in future research work. To reduce the evaluation time of the algorithm with the increment in array size can be used in future research work.

LIST OF REFERENCES

Research papers

- Albina. N, U. J. Raju, K. G. Revathi, K. Raghava Rao."Protection against man-in-the-middle attack in banking transaction using steganography" 2010 IEEE.
- C. Krishna Kumar, G. Jai Arul Jose, C. Sajeev and C. Suyambulingom 1.Sathyabama University, Chennai, India 2.Department of Mathematics, TAU, Coimbatore, India"SAFETY MEASURES AGAINST MAN-IN-THE-MIDDLE ATTACKIN KEY EXCHANGE" 2006-2012 Asian research Publishing Networks (February 2012)
- David Houcque Northwestern University."Introduction to MATLAB for engineering students" ICON 2014.
- Daniele Raffo" Digital Certificates and the Feige-Fiat-Shamir zero-knowledge protocol" July 2002.
- Dhanya R. Sarath, Megha V. Ainapurkar."An improved parallel interactive Feige-Fiat-Shamir identification scheme with almost zero soundness error and complete zero-knowledge" 2014 First international conference on networks and soft computing. 2014 IEEE.
- JOSEPH M. KIZZA* Department of Computer Science and Engineering The University of Tennessee, Chattanooga" Feige-Fiat-Shamir ZKP Scheme Revisited" International Journal of Computing and ICT Research, Vol. 4, No. 1, june 2010.
- Kazuomi Oishi, Tsutomu Matsumoto. Graduate school of Environment and Information Sciences, Yokohama National University, Yokohama, Japan "An Efficient Verifiable Implicit Asking Protocol for Diffie-Hellman key exchange" 2011 workshop on Lightweight Security & Privacy: devices, protocols, and applications 2011 IEEE.
- Maryam Saeed, Ali Mackvandi, Mansour Naddafiun, Hamid reza Karimnejad."An enhanced password authenticated key exchange protocol without server public keys" ICTC 2012, 2012 IEEE.

- P. Bhattacharya, M. Debbabi and H. Otok. “Improving the Diffie-Hellman secure key exchange” 2005 international conference on wireless networks, communications and mobile computing. 2005 IEEE.
- Uriel Feige, Amos Fiat, 1 and Adi Shamir Department of Applied Mathematics, The Weizmann Institute of Science, Rehovot 76100, Israel” Zero-Knowledge Proofs of Identity”
- Zhao Hu, Yuesheng Zhu, and Limin Ma.”An improved Kerberos Protocol based on Diffie-Hellman-DSA key exchange”. ICON 2012. 2012 IEEE.

Books

- Andy H. Register (2007) a guide to MATLAB object oriented programming. SCITECH publishing
- Behrouz A. Forouzan.(2007) Cryptography and Network Security. McGraw Hill Education, 2nd edition
- Brian R. Hunt, Ronald S. Lipsman, Jonathan M. Rosenbarg, A guide to MATLAB for beginners and experienced users.
- Fredrik Gustafsson .(2003) MATLAB for engineers EXPLAINED. Springer publication
- William Stallings. (2003) Cryptography and Network Security. Pearson Education, 3rd edition.

Web Page.

- http://www.mes.edu.mn/files/matlab_tutorial.pdf.
- <http://www.tutorialspoint.com/matlab/>
- http://in.mathworks.com/help/pdf_doc/matlab/matlab_prog.pdf
- <http://www.math.utah.edu/~wright/misc/matlab/programmingintro.html>
- <https://www.coursera.org/course/matlab>
- http://en.wikibooks.org/wiki/MATLAB_Programming
- [http://en.wikibooks.org/wiki/MATLAB_Programming/GUI/Get File or Director y](http://en.wikibooks.org/wiki/MATLAB_Programming/GUI/Get_File_or_Directory)
- <http://crypto.stackexchange.com/questions/14539/simplified-fiat-shamir-example-generates-wrong-output>

- <http://download.com-document.ru/info.php?q=a%20diffie%20hellman%20key%20exchange%20protocol%20without%20random%20oracles%20pdf>
- <https://www.youtube.com/watch?v=7bnVx34yQf4>
- <https://www.youtube.com/watch?v=Y5KTmx--ckY>
- https://www.youtube.com/watch?v=U_xtwPtCWII

APPENDIX

D-H protocol	Diffie-Hellman Protocol
RSA	Rivest Shamir and Adleman
DSA	Digital signature algorithm
DOS	Denial of service
MITM	Man-in-the-middle
KDC	Key distribution centre
TGS	Ticket granting server
TGT	Ticket granting ticket
AS	Authentication server
HTTP	Hypertext transfer protocol
HTTPS	Secure hypertext transfer protocol
MSG	Message
TXT	Text Message
GCD	greatest common divisor
MOD	Modulo
POW	Power
NO.	Number
DES	Data Encryption standard
FFS	Feige-Fiat-Shamir

VIA	Verifiable implicit asking
PAKE	Password Authenticated Key Exchange
ZKP	Zero knowledge proofs
S-PF	Soundness proof
ET	Evaluation time
CTime	Completion time
SSH	Secure shell
SSL	Secure socket layer
IPSec	IP Security