International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 13 (2014), pp. 1305-1314

http://www. irphouse.com

Banking Authentication Technique

[1]Sankalp Jagga and [2]Puneet Sharma

[1]M.tech (spgoi, Rohtak), M.D.University, Rohtak, Haryana
[2]M.D.University, Rohtak, Haryana

Abstract

In this paper first we study about cryptography and its techniques and after that studied on various work done by other people on cryptography and from that taken idea of my proposed worked. Cryptography is the major element which is used to secure data or information while sharing confidential data. There are many techniques available to secure data but still improvements and establishment of new techniques is required. So in my proposed work, I tried to make a new encryption technique by using different techniques in order to make more secure way to communicate and share data or information. In my work, I applied symmetric keys, hash functions, digital signature and token based encryptions together for providing more data security.

Keywords: Cryptography, symmetric keys, hash functions, data security**.**

I. INTRODUCTION

Today, security is the main concern in the every field of life and in every field, computer which is now become a major part of our daily work and also as a human part. Now, we all do our work on computer and also on internet while communicating with others. So, data security is the main concern for a secure communication and secured transformation of data over connected path. For security purpose cryptography is the term which comes in our mind although there are thousands of technique for securing the data but still cryptography is in continuous research.

Some basic introduction about cryptography: what is cryptography, what they do and what are the techniques.

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread

development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any un-trusted medium, which includes just about any network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

Authentication:
The process of proving one's identity. The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.

Privacy/confidentiality:
Ensuring that no one can read the message except the intended receiver.

Integrity:
Assuring the receiver that the received message has not been altered in any way from the original.

Non-repudiation:
A mechanism to prove that the sender really sent this message. [1]

Cryptography is the process of protecting the data as well as authenticating the user to use the services.

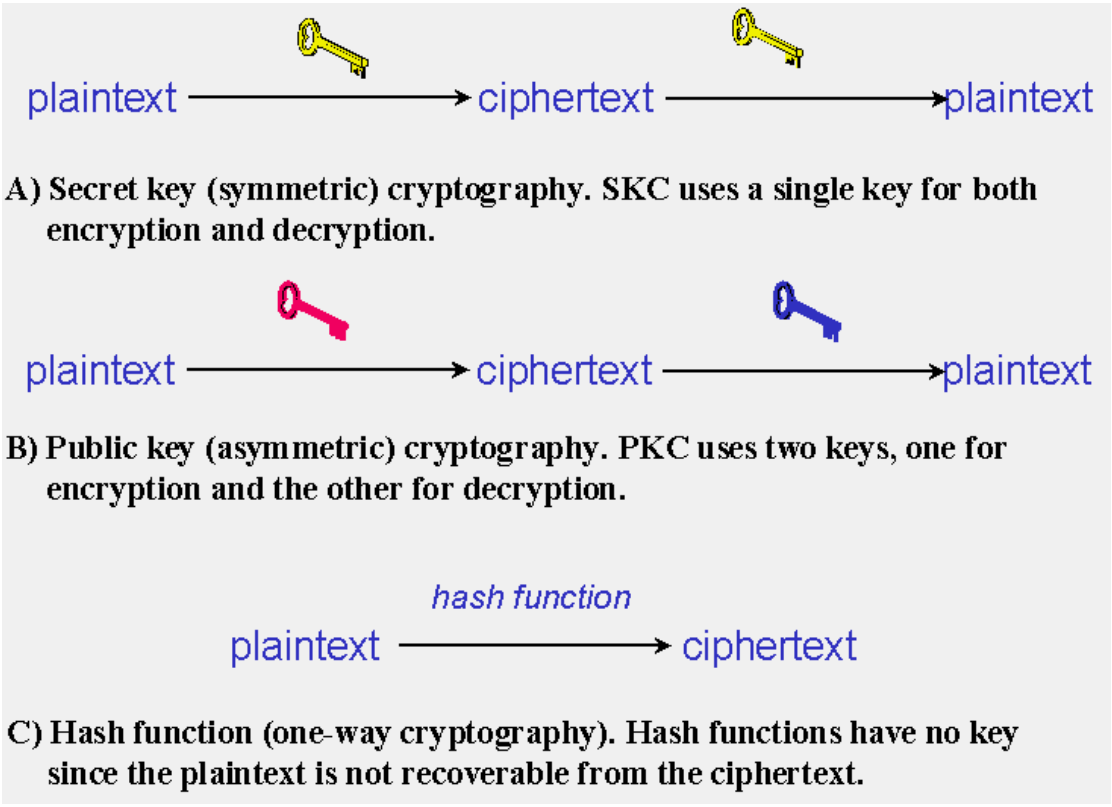
Basically, cryptography is the process in which the data is sent from one party to another party and they are called sender and receiver respectively. The unencrypted data sent from sender to receiver is called as plaintext and after applying any cryptographic technique then it called cipher text and also uses the same technique to decrypt it.

Types of Cryptographic Algorithms:
There are three types of cryptographic algorithms are (Figure 1):

Secret Key Cryptography (SKC):
In secret key cryptography only one common key is share between both the parties to encrypt and decrypt the data.

Public Key Cryptography (PKC):
In public key cryptography two different keys are use to authenticate the user and access the data. One is public key and second is private key.

Hash Functions:
In hash functions a mathematical transformation is used to encrypt and decrypt the data.



[1]

II. RELATED SURVEY

Design and implementation of a Network Security Model for cooperative Network:

In this paper of 2009, SALAH ALABADY design and implementation of a network security model by using routers and firewall. Also this paper was conducted the network security weakness in router and firewall network devices, type of threats and responses to those threats, and the method to prevent the attacks and hackers to access the network. Also this paper provides a checklist to use in evaluating whether a network is adhering to best practices in network security and data confidentiality. The main aim of this research is to protect the network from vulnerabilities, threats, attacks, configuration weaknesses and security policy weaknesses. [3]

Network Security Using Cryptographic Techniques:

In 2012, SUMEDHA KAUSHIK and ANKUR SINGHAL said

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Only one

particular element underlies many of the security mechanisms in use: Cryptographic techniques; hence our focus is on this area Cryptography. Cryptography is an emerging technology, which is important for network security. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured communication. [4]

Advance cryptography algorithm for improving data security:
In this 2012, VISHWA GUPTA, GAJENDRA SINGH and RAVINDRA GUPTA developed a new cryptography algorithm which is based on block cipher concept. In this algorithm I have used logical operation like XOR and shifting operation. Experimental results show that proposed algorithm is very efficient and secured. [5]

Ease and security of password protections improved:
In 2014, UNIVERSITY OF ALABAMA AT BIRMINGHAM proposed a new security technique which is based on hash cryptographic technique and a device called RSA ID which generate different codes which user have to put with different hash techniques in this proposed work they uses the four different hash functions and that RSA ID device which having continuous changing token on his display which user have to put to validate or authenticate themselves. [6]

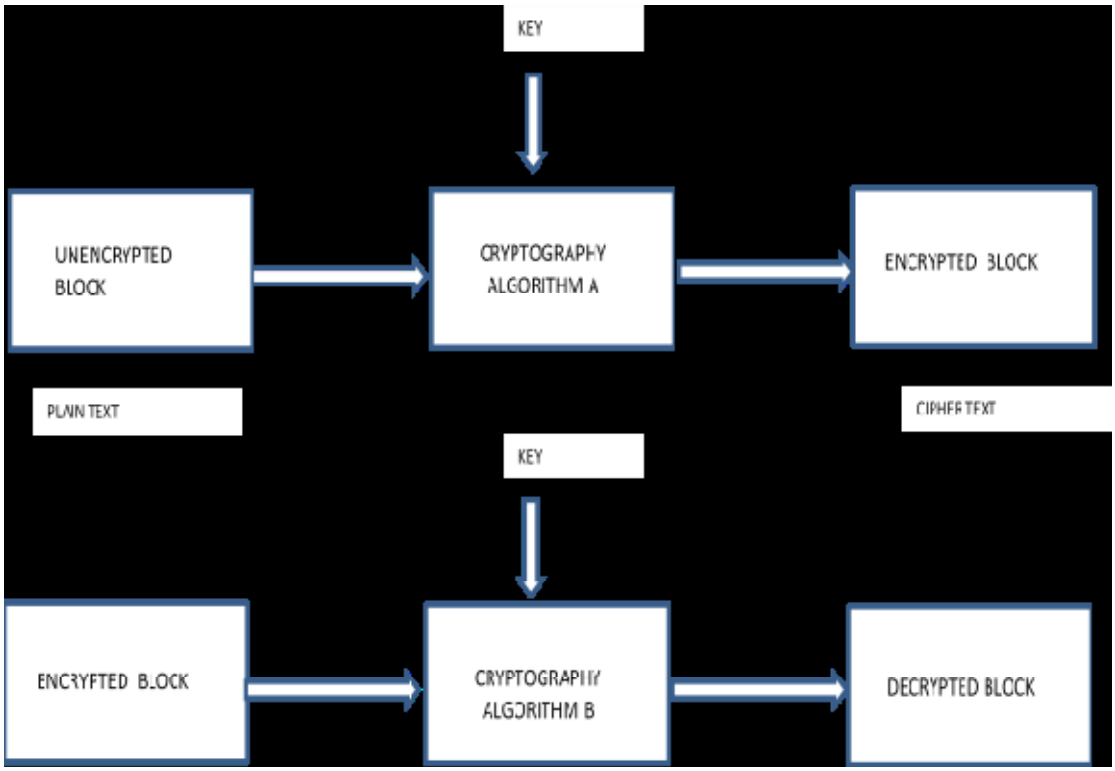
A hybrid cryptosystem based on vigenère cipher and columnar transposition cipher:
In 2013, QUIST-APHETSI KESTER presents the general body of knowledge in the area of classical cryptography by developing a new hybrid way of encryption of plaintext. The cryptosystem performs its encryption by encrypting the plaintext using columnar transposition cipher and further using the cipher text to encrypt the plaintext again using Vigenère cipher. At the end, cryptanalysis was performed on the cipher-text. The implementation will be done using java programming. [7]

III. PROPOSED WORK

In this section III, I am presenting the proposed work in which I am going to present the three way authentication method based on banking technique which is a real life security method, people use to store or secure their personal or expensive things. For example: gold in bank lockers. In my proposed work the three authentication techniques are:

- Symmetric encryption
- Asymmetric encryption with trusted certificate/digital signature
- Token based validation

Symmetric encryption:
In this symmetric encryption which is my first step we uses, the private key which is a unique key which is used by both the end nodes or communicating parties(sender and receiver).



[5]

Through this private key both the parties will encrypt and decrypt that information shared between them.

Reasons for Use of Symmetric Approach for Encryption and Decryption:

- Symmetric encryption is simple in nature.
- In symmetric encryption security is dependent on strength of key used.
- High rates of data throughput.
- In symmetric encryption same encryption algorithm is used no need to develop and exchange secret algorithm.

Asymmetric encryption with trusted certificate:

In asymmetric encryption in which secret keys are develop for security purpose. In this both the keys are different one is public key and second one is private key. In this first sender encrypt the data with their private key and send it through their public key and then receiver decrypt it bby their private key.

Token based validation:

In this, one code is send to receiver by sender on his/her registered cell phone number and every time this code vary for security purpose. This token or code will also validate that the code is send to authenticate persn and that person is trying to access that document or information.

Banking technique:
In this, two keys are used one by the customer and one by the bank member for the security of the locker and for the things placed in that locker, to open that locker both the keys are needed at the same time then only customer will able to open his/her locker.

In a same manner in my proposed work, both the keys or digital signature of sender as well as of receiver are needed to validate the receiver to open that document just like bank customer.[8]

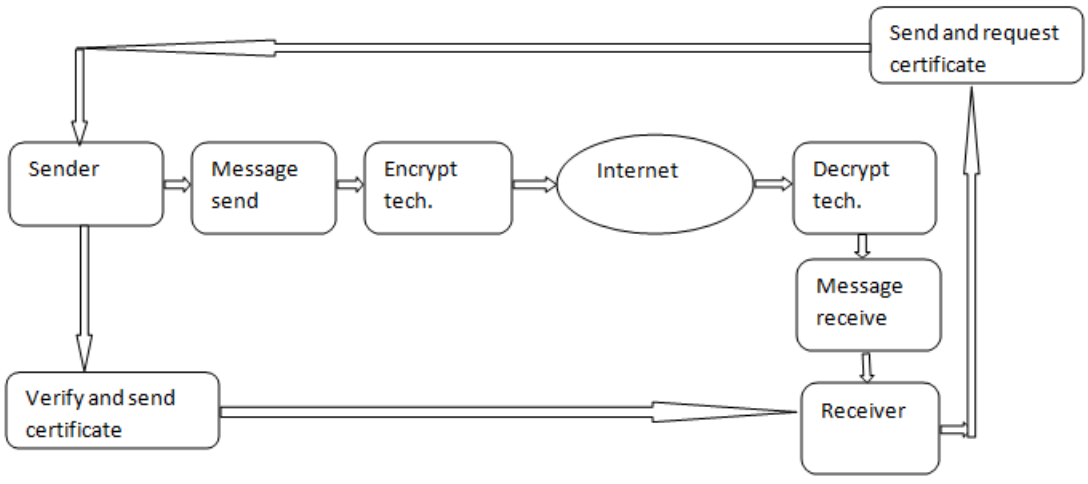
Proposed methodology:
In my proposed methodology, I am combining different techniques in order to make a new encryption technique so that data or information will share in a very secured way and can not be breach in middle of the way. In this, my main work is done in asymmetric technique in which I am using digital signature in place of key in banking form or banking security technique which is bank locker.

So, in my proposed work there are two different architectures on which I am working:

1. Two level architecture encryption technique
2. Three level architecture encryption technique

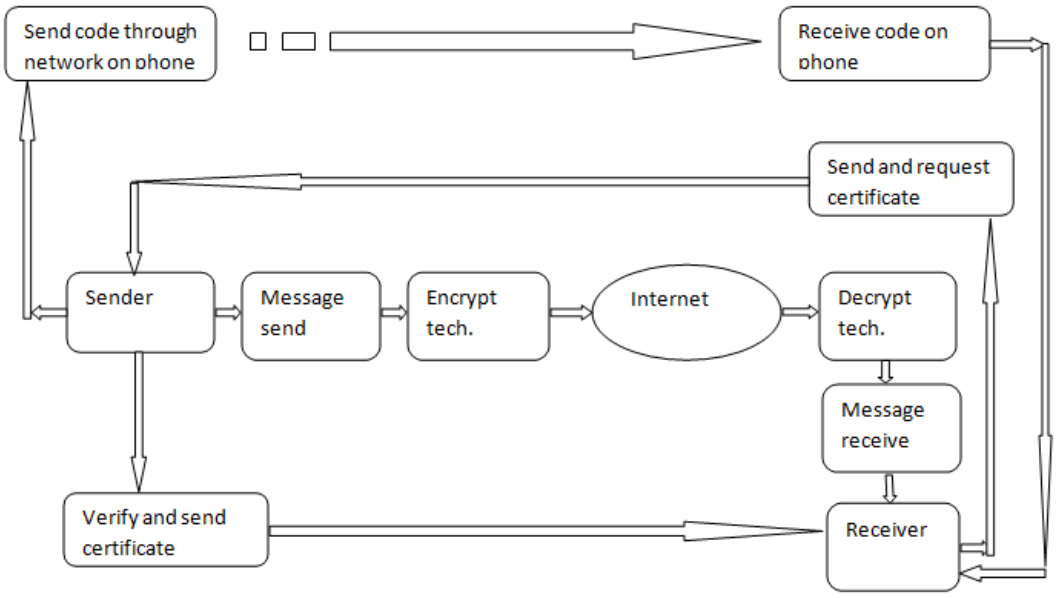
Working methodology of:
Two level architecture:

- In first step, a sender will use a symmetric encryption to convert the data or plain text into cipher text.
- In second step, receiver after receiving his encrypted information will send his certificates/digital signature for verification and ask for sending sender's certificates/digital signature.
- In last step, sender after verify receiver's certificates send his certificates to receiver so that receiver will use both certificates and encryption key to convert that encrypted document into plain readable form.



Three level architecture:

- Firstly, sender will send the data or information to receiver by using the encryption key.
- When receiver will receive that encrypted document then send a request to sender to send their digital dignature/certificates along with their digital signature/certificates for verification.



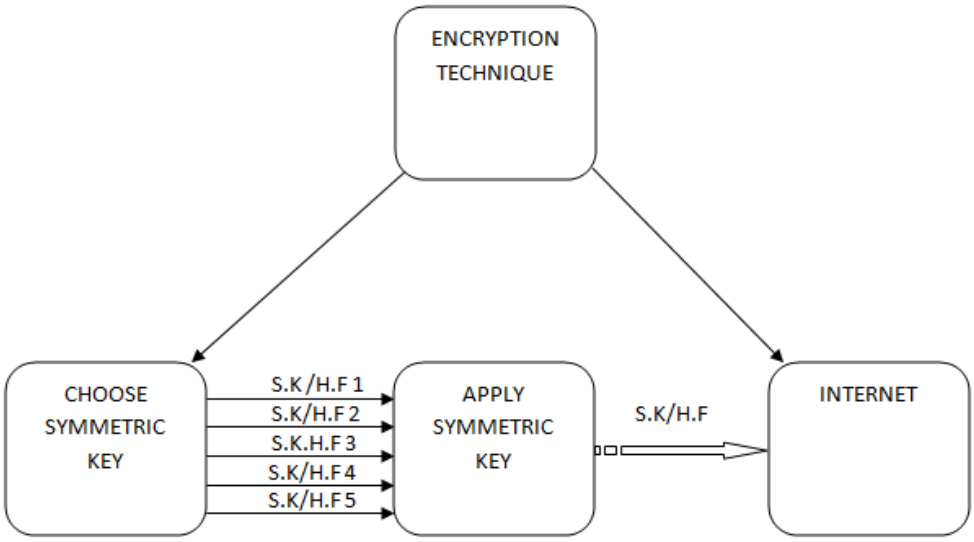
[8]

- After receiving of digital signature sender will verify their signature whether requesting person is authenticate or not. After verify sender will send his certificates to receiver.
- Then receiver will receive a code on his registered number and put all these keys together to decrypt.

Encryption technique:

In this three level architecture, there is also some work is done at time of encryption applied in first step. When encryption is applied then they are 5(five) different symmetric keys and 5(five) different hash functions are used. At the time of encrypting the document, the encryption technique is choosen randomly.

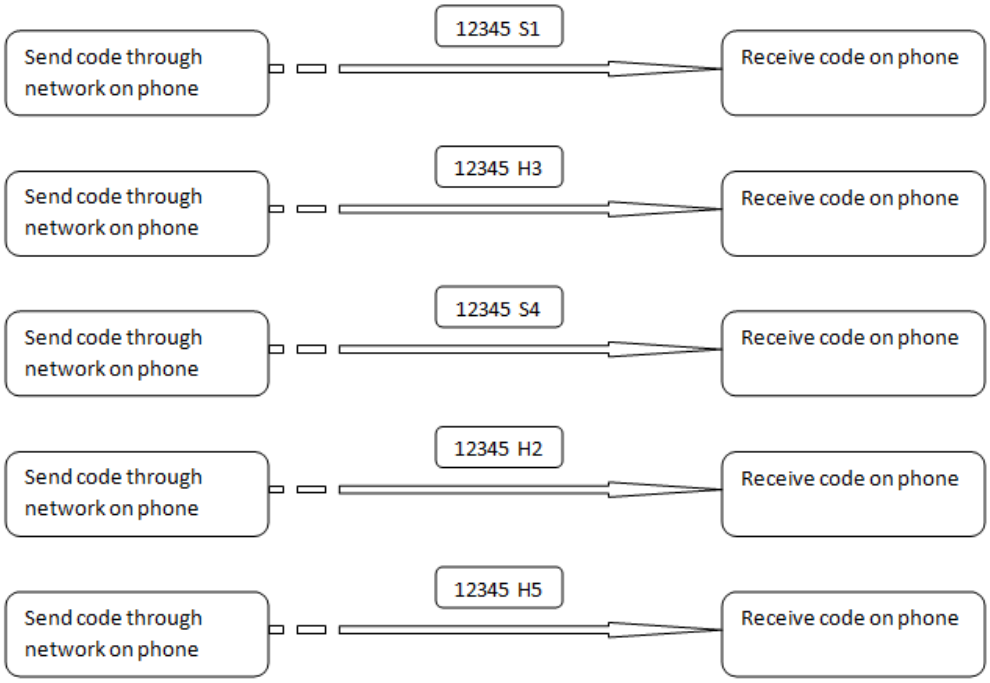
The purpose of using different symmetric keys and hash functions together to make strong encryption technique just like ‘one time pad’ in which there is a different encryption key for every line but here, we are not using different key for every line but uses a few keys randomly to encrypt.



Code:

In this, a code is sent by sender to receiver. In this code it contain two things:

- First, it contain a random five digit code
- Secondly, it contain a code which tells what encryption technique is used in first step.



In this code shown in figure first five digit random code has been put by receiver and next two words is showning which technique is used in this 'S1' means symmetric key 1, 'S4' means symmetric key 4, 'h2' means hash function 2, 'h3' means hash function 3 and 'h5' means hash function 5.

IV. COMPARISON

Existing Encryption technique v/s Banking Authentication Technique:

- In symmetric encryption single key is used and that key should be small and main problem is sharing of that key because if that key is come to an unauthorized person they have access to whole document. Security is less in symmetric encryption only. Therefore, in my proposed work I used different layers of encryption which make connection more secure.
- In token based only code is send and if it can be known to anyone then it will also access to document but I not only use the token based but also symmetric and trusted certificate security based on banking technique. Therefore, it is more secure.
- In password based encryption is less secure as password can be predictable as it people mostly put password which can be easily remembered. In my proposed work, I use digital signature instead of password with combination of random token based encryption which make it more secure.
- In one time pad technique it uses different key for every different line so, if we want to encrypt a document having thousands of line then it is not possible to keep in mind all those keys or to note down all those thousands of keys to one place and also apply those.
- So, in banking authentication technique only few symmetric keys are used with hash function so that no need of using many keys to keep in mind and also to store at any place, as code will tell what key is used by sender.

V. REFERENCES

[1] Gary C. Kessler, "An Overview of Cryptography", http://www.garykessler.net/library/crypto.html, 2014 [1]

[2] From Google, https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcR12QOMDZBjETOU-VqFWYIGk3W_m2VVCrBY7WGMP77uqAIc3ARPMQ [2]

[3] SALAH ALABADY, "Design and Implementation of a Network Security Model for Cooperative Network", 2009 [3]

[4] SUMEDHA KAUSHIK and ANKUR SINGHAL, "Network Security Using Cryptographic Techniques", 2012 [4]

[5] VISHWA GUPTA, GAJENDRA SINGH and RAVINDRA GUPTA, "Advance cryptography algorithm for improving data security",2012 [5]

[6] UNIVERSITY OF ALABAMA AT BIRMINGHAM, "Ease and security of password protections improved", 2014 [6]

[7] QUIST-APHETSI KESTER, “A hybrid cryptosystem based on vigenère cipher and columnar transposition cipher”, 2013 [7]
[8] SANKALP JAGGA, “Three way authentication based on banking technique”, 2014 [8]