



KED: A Symmetric Key Algorithm for Secured Information Exchange Using Modulo-69

Ms. Hima Bindu Rangala*¹, Mrs. G. Jyothi*²

¹MCA Student, Department of Master of Computer Applications, Vignan's Institute of Information Technology(A), Beside VSEZ, Duvvada, Vadlapudi Post, Gajuwaka, Visakhapatnam-530049.

²Assistant Professor, Department of Information Technology, Vignan's Institute of Information Technology(A), Beside VSEZ, Duvvada, Vadlapudi Post, Gajuwaka, Visakhapatnam-530049.

Abstract:

Securing information flow has emerged as a critical component of communication in the current digital era. It is crucial to have a strong encryption technique that can shield critical data from unwanted access given the rising number of cyber threats. Therefore, cryptography is essential for ensuring security. Symmetric Key and Asymmetric Key cryptography are the two fundamental types. Instead, then using many keys for encryption and decryption like Asymmetric Key does, Symmetric Key uses just one key. The most extensively used algorithms are those using symmetric keys. The difficulty of deciphering the original messages is what gives these algorithms their strength. Modulo69-based KED-A symmetric key is a cutting-edge encryption technique that offers secure data transfer. In this project data deduplication is a technique used to improve storage utilization by eliminating duplicate data. The technique of encoding plain information into an unintelligible format termed cipher text is known as encryption. Decryption is the procedure of turning encrypted text to plain text. Asymmetric key cryptography and symmetric key cryptography are the two forms of cryptography. Asymmetric key cryptography uses different keys, one for encryption and the other for decryption, as opposed to symmetric key cryptography, which uses the same key for both operations.

Keywords: Symmetric Key , Asymmetric Key Cryptography, De-ciphering, Encryption, Decryption.

1. INTRODUCTION

Encryption is the process of encoding plain text and converts it to non-readable format called cipher text. Decryption is the process of decoding cipher text converting it to plain text. There are two types of cryptography namely Symmetric Key Cryptography and Asymmetric Key Cryptography. In symmetric key cryptography same key is used both for encryption as well as decryption process where as in asymmetric key cryptography separate keys are used one for encryption process and the other for decryption process.

Cryptography: Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from reader and only the intended recipient will be able to convert it into original text. Its main goal is to keep the data secure from unauthorized access. It is the science of encrypting and decrypting information, dates as far back as 1900 BC when a scribe in Egypt first used a derivation of the standard hieroglyphics of the day to communicate. Every encryption and decryption process has two aspects: the algorithm and the key used for encryption and decryption.

In computer and communication systems security issues play a crucial role and must be addressed before hand to guard against illicit attacks. In the global communal world, where faster access to precise information is the most basic need; security of confidential data during transfer from one place to another place is a major concern. There are a lot of sheltered approaches that can be applied inside the organization's premises to keep the data safe. But when this confidential data or information comes out of the company's premises, it becomes susceptible to the unauthorized attacks by hackers or opponent. There can be various techniques that can be used to attain secure transfer of data like firewalls, proxy servers, and steganography, data security plans against worms, viruses or denial-of-service attacks but cryptography proves itself as a central tool for achieving data and software protection. The best cryptographic algorithm is the one that strikes a good balance between security and performance.

Cryptography can be defined as the art or science of altering information or change it to a chaotic state, so that the real information is hard to extract during transfer over any unsecured channel. Latest advancements in technology and new concepts like quantum cryptography have added a completely new dimension to data security. The strength of this cryptographic technique comes from the fact that no one can read (or steal) the information without altering its content. This alteration alerts the communicators about the possibility of a hacker and thus promising a highly secure data transfer. Due to this advantage, quantum cryptography has grasped a great deal of attention and huge amount of research is being carried out on it for safeguarding of business-critical data. During the course of time, various encryption algorithms have been developed to achieve the ultimate aim of safe environment for information transmission. However, the principal objective guiding the design of an encryption algorithm must be security against all possible unauthorized attacks. However for all practical applications, performance and the cost of implementation are also important concerns. The best cryptographic algorithm is the one that strikes a good balance between security and performance.

Apart from the well-known division of private-key and public-key cryptography, there is another way to categorize the encryption process depending upon the input size. One approach encrypts data bit wise i.e., one unit at a time. The second approach takes a block of data and encrypt in it one go. The former is called stream cipher and latter is called block cipher. Block encryption is the faster way but produces same cipher text for the same plaintext and encryption key. However stream ciphers does not have any such pitfall and is considered more secure. Stream ciphers have lower hardware complexity as compared to block ciphers. An important point to note is not to use the same starting state twice. Though stream ciphers are comparatively take more time to process and hence are not widely used in real time applications.

1.2 Secret Key Cryptography:

In secret key cryptography [4, 5] a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography.

It is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

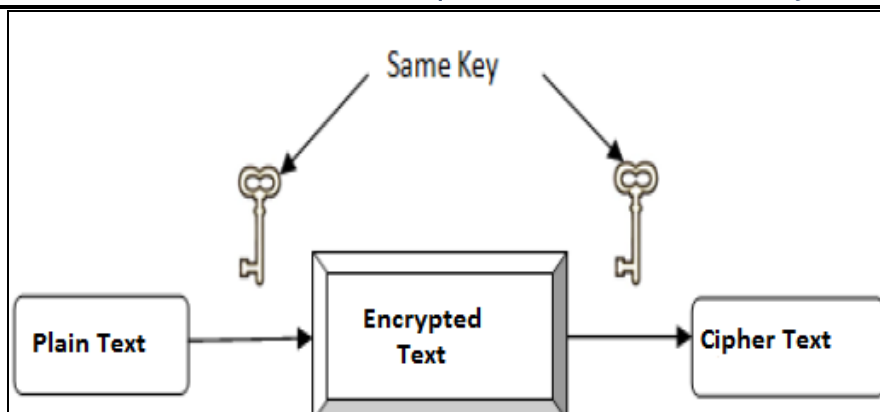


Fig 2.1 Secret Key Cryptography or Symmetric Key Cryptography

A single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message.

1.3 Public Key Cryptography:

Public or asymmetric key cryptography consist of two keys or of key pairs: one private key and one public key [1]. One is used for encryption and the other for decryption. The private key is private and is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public.

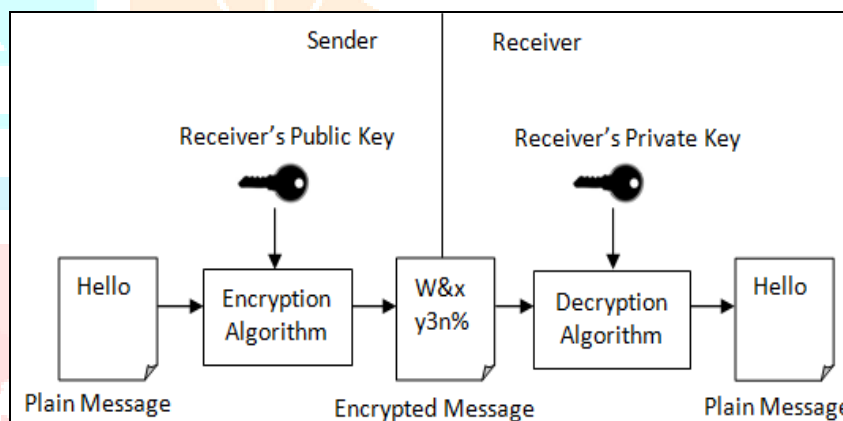


Fig 2.2 Public Key Cryptography or Asymmetric Key Cryptography

Public key cryptography intends for public keys to be accessible to all users. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. Public key cryptography [2] intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, without a prior key distribution arrangement.

2. LITERATURE SURVEY

2.1 A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security

AUTHOR: M. A. Al-Shabi

This paper discusses several important algorithms used for the encryption and decryption of data in all fields, to make a comparative study for most important algorithms in terms of speed (implementation) and security (special keys) determine whether an encryption algorithm is good. What is more, computational resources, such memory (RAM) size, are an integral consideration since they affect algorithm efficiency, hence the need to ensure optimal resource allocation, etc. Particularly, encryption is the process of transforming plain text into ciphered-text, which cannot be understood or altered easily by undesirable people. This encrypted result is encoded and has immunity against attacks and unauthorized access and manipulation. Encryption algorithms often use private keys that are used to revert the encrypted data to its original meaningful format. Such an algorithm, such as Blowfish,

RC5, or RC4, is basically a set of mathematical procedures that make it hard for malicious attackers to understand or use the original data. In symmetric key algorithms, a single key is used to encrypt and decrypt text. On the contrary, the asymmetric key algorithm uses two discrete keys, where both the sender and receiver have access to one of them. These security measures and systems eliminate possible internal and external threats to ensure integrity, correctness, confidentiality, and safety of data and infrastructures are controlled.

2.2 A Brief History of Cryptography

AUTHORS: WA Kotas, *Giovan Battista Bellaso*, Huzaifa Sidhpurwala

Though it has been used for thousands of years to hide secret messages, systematic study of cryptology as a science (and perhaps an art) just started around one hundred years ago. The first known evidence of the use of cryptography (in some form) was found in an inscription carved around 1900 BC, in the main chamber of the tomb of the nobleman [Khnumhotep II](#), in Egypt. The scribe used some unusual hieroglyphic symbols here and there in place of more ordinary ones. The purpose was not to hide the message but perhaps to change its form in a way which would make it appear dignified. Though the inscription was not a form of secret writing, but incorporated some sort of transformation of the original text, and is the oldest known text to do so. Evidence of some use of cryptography has been seen in most major early civilizations.

2.3 Computer and Network security

AUTHORS: J Wang, JM Kizza

Computer network security consists of measures taken by business or some organizations to monitor and prevent unauthorized access from the outside attackers.

Different approaches to computer network security management have different requirements depending on the size of the computer network. For example, a home office requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks.

Network Administrator controls access to the data and software on the network. A network administrator assigns the user ID and password to the authorized person.

3. EXISTING SYSTEM

Many cryptographic algorithms have already been proposed and implemented to provide security to the user that his message would remain safe at the time of communication over the web. But now a day's hacking has become a common practice in society which made such cryptographic algorithms no longer safe. In this project I have studied number of such symmetric key algorithms and selected one of them for reference in the proposed algorithm.

Problems in the Existing System:

1. Introduction of a New Algorithm: We introduce a novel algorithm that operates under the symmetric key mechanism.

2. Symmetric Key Cryptography Defined:

- Symmetric key cryptography involves an encryption system where both the sender and the receiver share a single, common key.

3. Functionality of Symmetric Key Cryptography:

- This shared key is utilized for both the encryption and decryption processes of a message.

4. Contrast with Asymmetric Key Cryptography:

- In contrast to asymmetric key cryptography, which involves two keys (public and private), symmetric key systems rely on a single key for both encryption and decryption.

5. Simplicity and Speed:

- Symmetric key systems are known for their simplicity and speed, making them advantageous for certain applications.

6. Terminology:

- Symmetric key cryptography is often referred to as secret key cryptography due to the shared secret key between the communicating parties.

4. PROPOSED SYSTEM

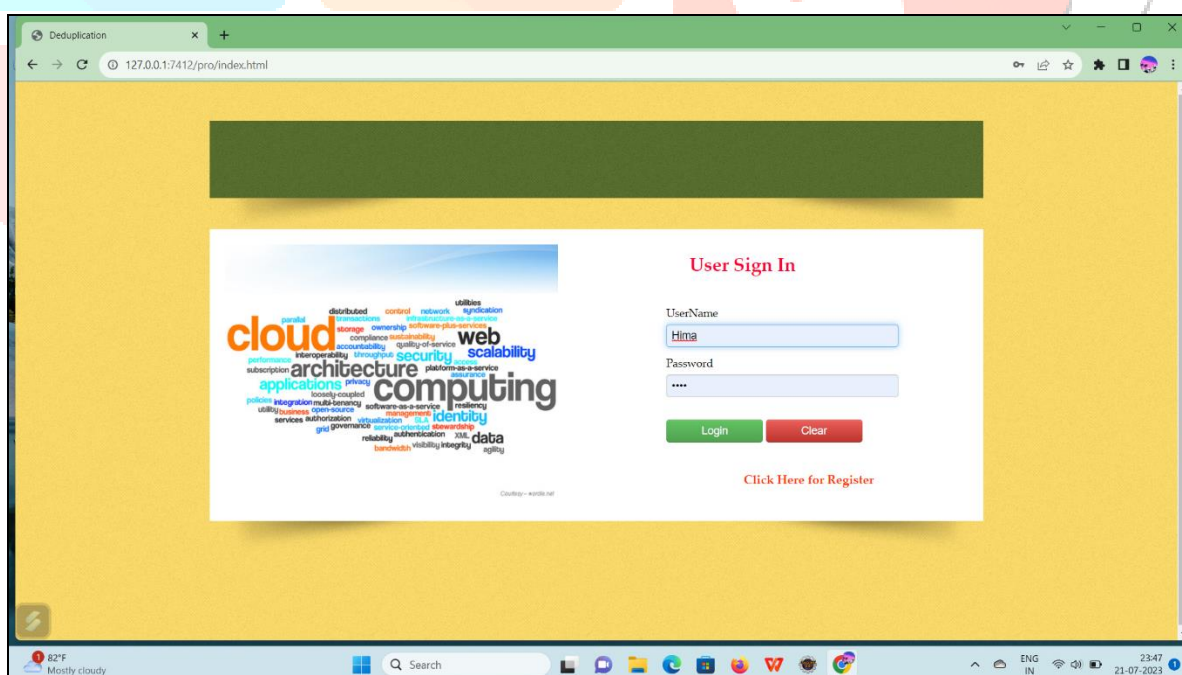
The strength of these algorithms is based on the difficulty to break the original messages. In this paper, a new Symmetric Key algorithm called as KED (Key Encryption Decryption) using modulo69 is proposed. Here not only alphabets and numbers are used, but special characters have also been included.

Two keys are used in which one is a natural number which is relatively prime to 69 and finding the inverse modulo69 of it and the other key is a random number generated by the proposed key generation method.

Many cryptographic algorithms have already been proposed and implemented to provide security to the user that his/her message would remain safe at the time of communication over the web. But now a day's hacking has become a common practice in society which made such cryptographic algorithms no longer safe.

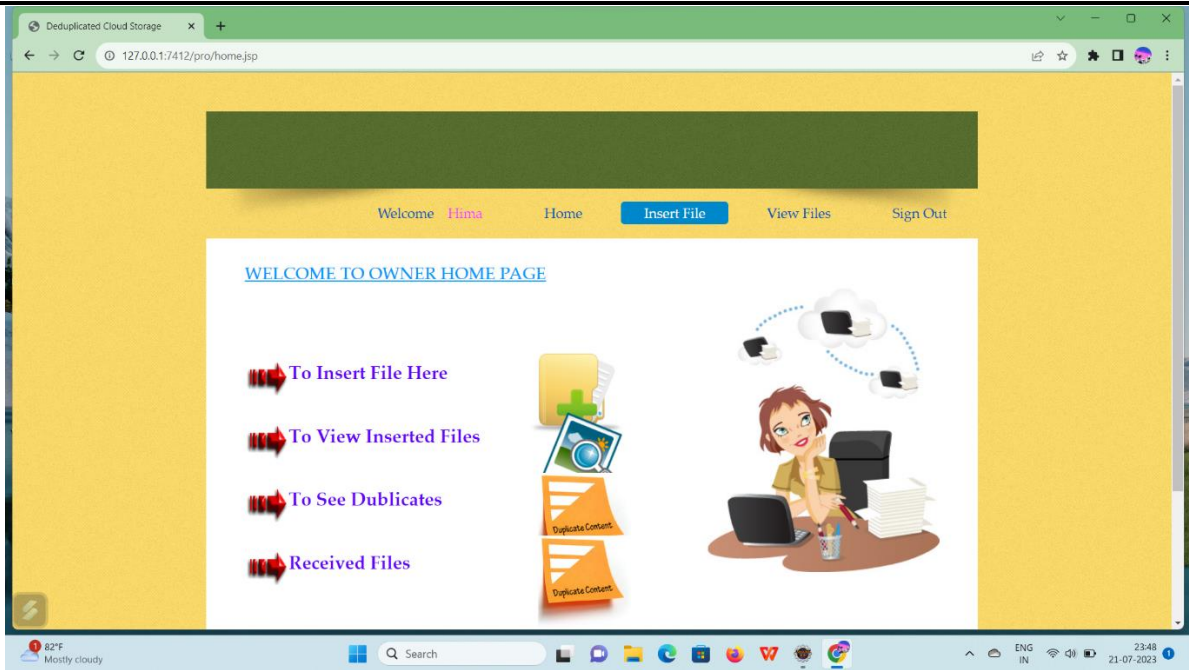
5. EXPERIMENTAL RESULTS

From the below figures it can be seen that proposed model is more accurate in order to prove our proposed system.

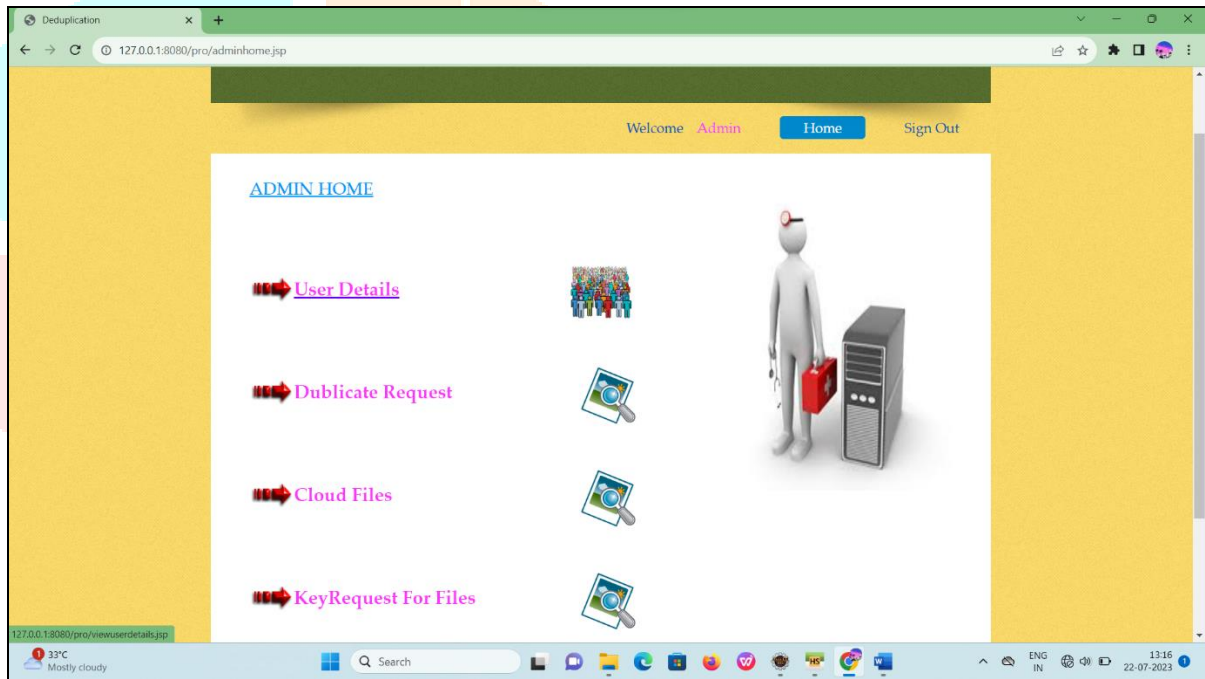


Screen 5.1: Screen shows the Home Page and the Login Page for the user.

User login by entering his login id and password.



Screen 5.2: Screen shows Users Home Page.

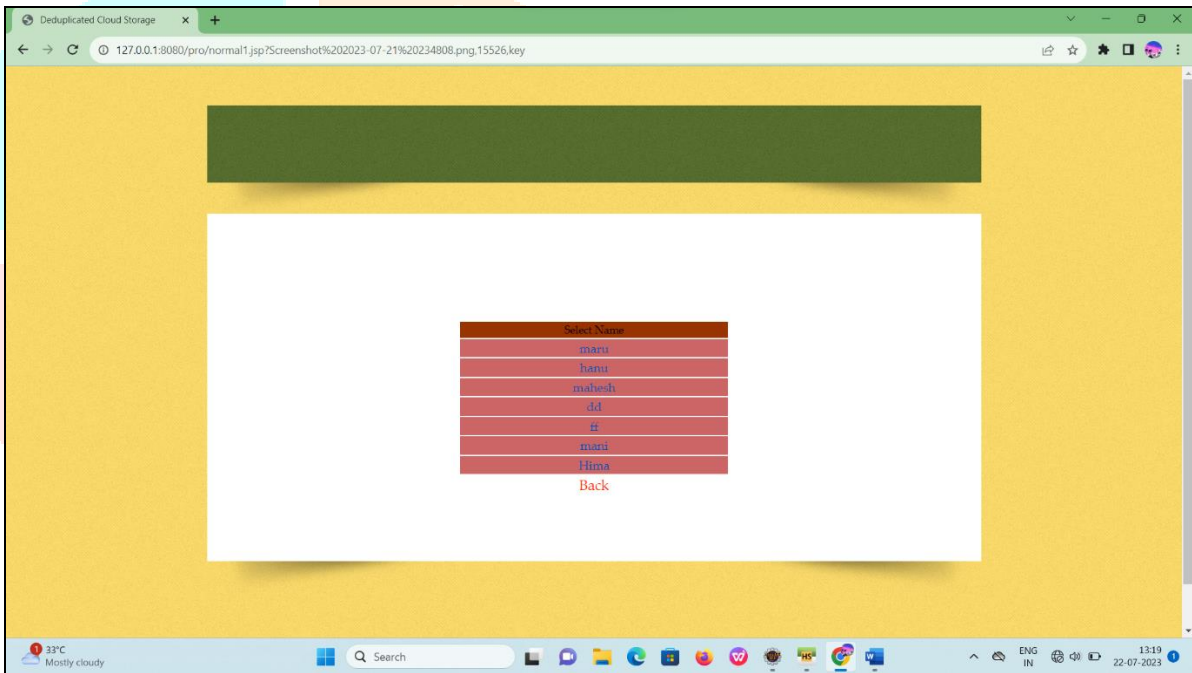


Screen 5.3: Admin Home Page.



File Name	File Size	File KEY	Uploaded By	Shared Type
dell.jpg	6kb	33223	mahesh	Normal Key
c.jpg	11kb	43213	mahesh	Normal Key
l.jpg	7kb	27378	dd	Normal Key
img05.jpg	7kb	25621	mahesh	Normal Key
c.jpg	11kb	42571	mahesh	Normal Key
2_13_eng.pdf	752kb	88105	ff	Normal Key
2_13_eng.pdf	752kb	3113	ff	Normal Key
1.txt	14kb	62447	maruthi	Normal Key
document.jpg	6kb	43795	maruthi	Normal Key
5thfile.txt	7kb	40843	hanuman	Normal Key
2_13_eng.pdf	752kb	78503	hanuman	Normal Key
2_13_eng.pdf	752kb	53001	mani	Normal Key
1.pdf	285kb	62296	mani	Normal Key
img05.jpg	7kb	52193	mani	Normal Key
Screenshot (1).png	1722kb	15743	mani	Normal Key
q&ans OS.txt	45kb	2546	null	Normal Key
q&ans OS.txt	45kb	86330	null	Normal Key

Screen 5.4: It is used to share the key.



Select Name

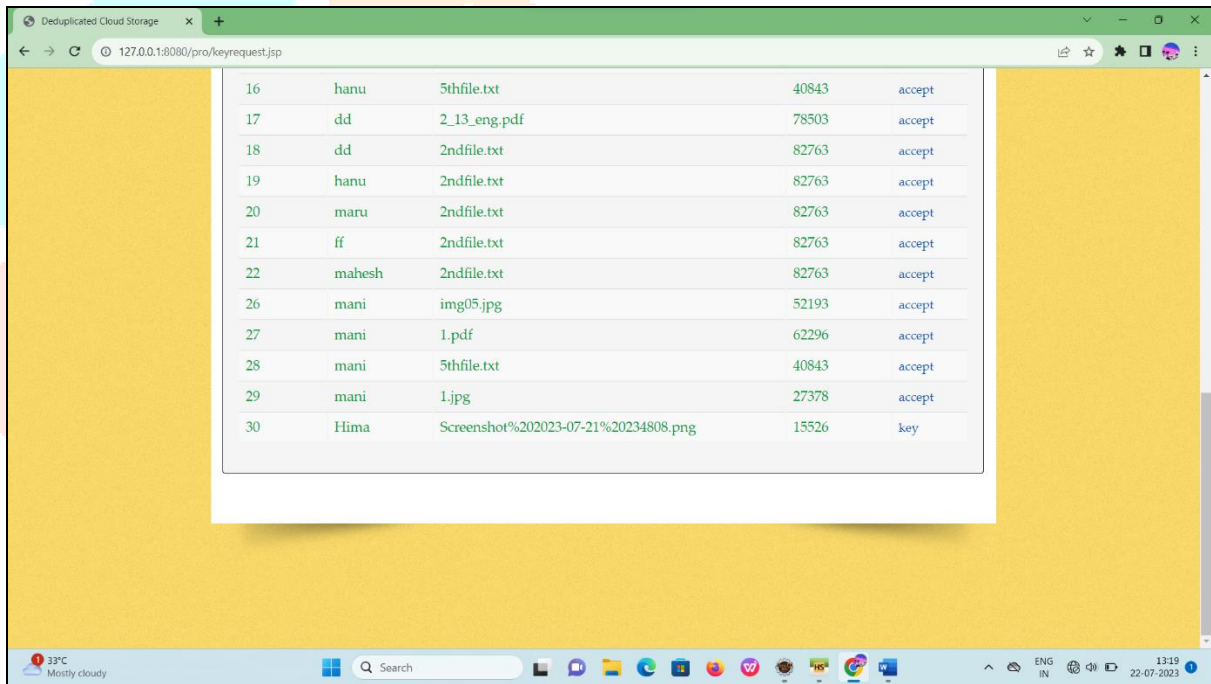
- manu
- hanu
- mahesh
- dd
- ff
- mani
- Hima
- Back

Screen 5.5: Screen shows who requested for duplication and admin has to press user name.



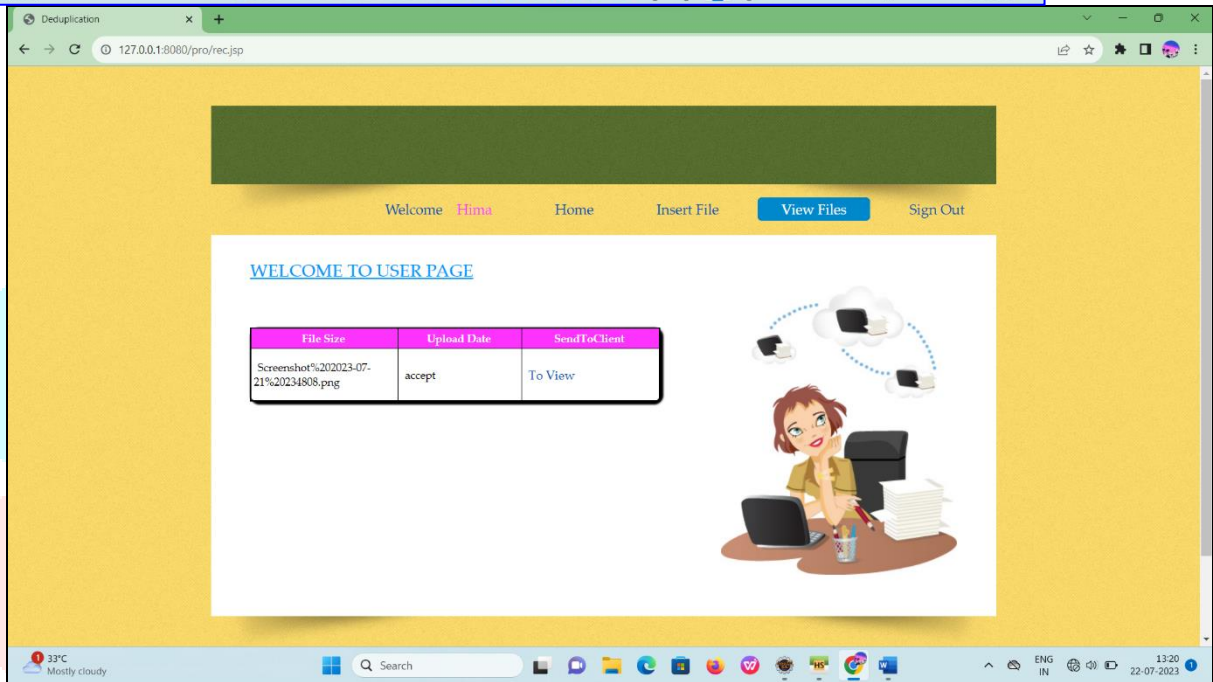
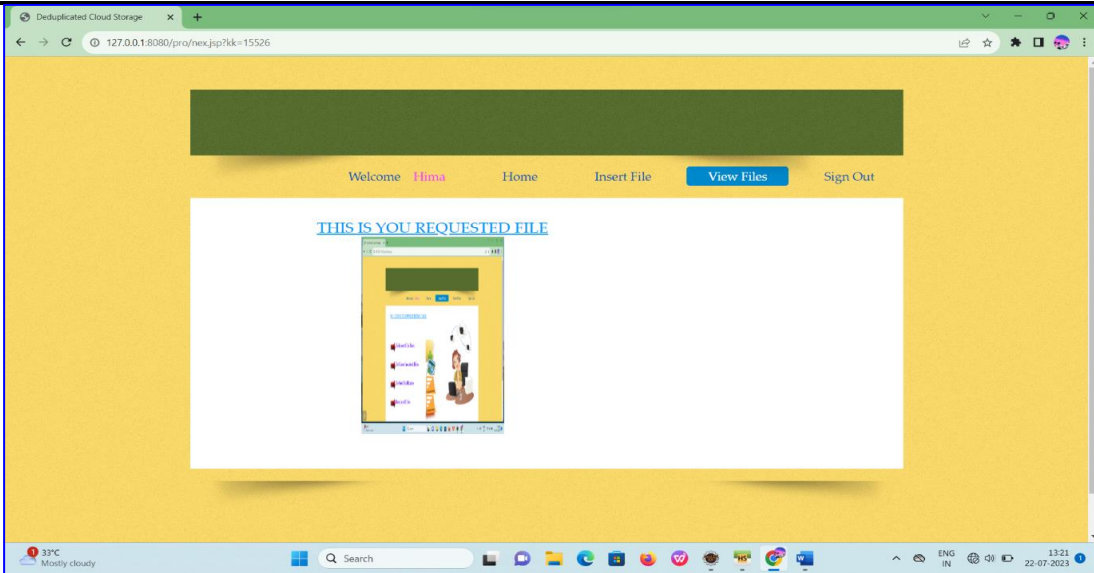
File_ID	Uploader	File	File_KEY	Status
1	mahesh	c.jpg	42571	normal
2	dd	c.jpg	42571	normal
3	dd	c.jpg	42571	key
4	mahesh	c.jpg	42571	accept
5	mahesh	c.jpg	42571	accept
6	ff	2_13_eng.pdf	3113	accept
7	maru	1.txt	62447	accept
8	maru	1.txt	62447	accept
9	maru	1.txt	62447	accept
10	hanu	2_13_eng.pdf	78503	accept
11	hanu	2_13_eng.pdf	78503	accept
12	dd	2_13_eng.pdf	78503	accept
13	hanu	2_13_eng.pdf	78503	accept
14	mahesh	2_13_eng.pdf	78503	accept
15	maru	2_13_eng.pdf	78503	accept
16	hanu	5thfile.txt	40843	accept
17	dd	2_13_eng.pdf	78503	accept

Screen 5.6: It shows Key status and accept the key request to Encrypt the File.



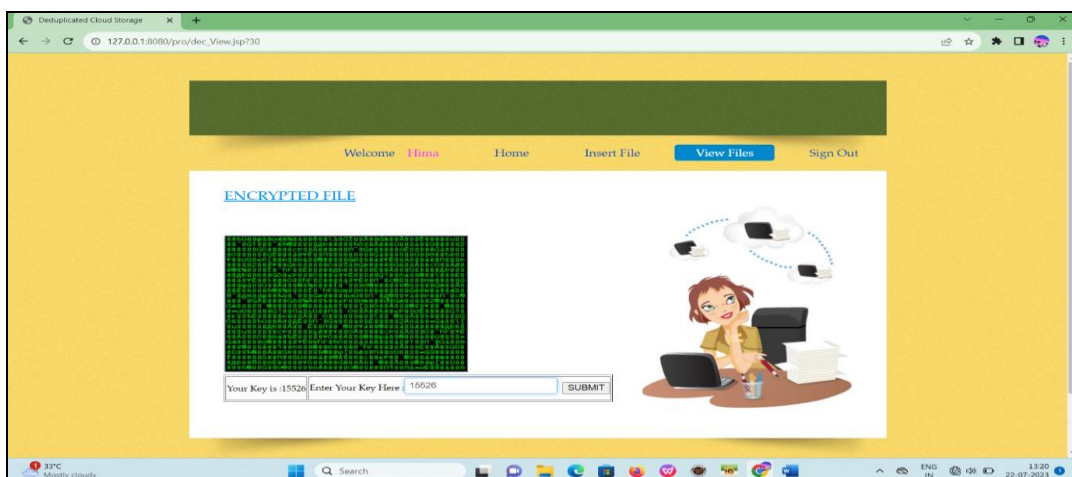
16	hanu	5thfile.txt	40843	accept
17	dd	2_13_eng.pdf	78503	accept
18	dd	2ndfile.txt	82763	accept
19	hanu	2ndfile.txt	82763	accept
20	maru	2ndfile.txt	82763	accept
21	ff	2ndfile.txt	82763	accept
22	mahesh	2ndfile.txt	82763	accept
26	mani	img05.jpg	52193	accept
27	mani	1.pdf	62296	accept
28	mani	5thfile.txt	40843	accept
29	mani	1.jpg	27378	accept
30	Hima	Screenshot%202023-07-21%20234808.png	15526	key

Screen 5.7: Screen shows the Encryption process using algorithm.



Screen 5.8: User got the duplicated file with secret key.

Screen 5.9: Screen shows the Decryption Page where the user decrypts the data.



Screen 5.10: The file which is decrypted.**6. CONCLUSION**

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the data which has been sent to the receiver from the sender. Now, in order to achieve these goals various cryptographic algorithms are developed by various people. The aim of this paper was to design and implement an algorithm to address this issue. Here we have used inverse modulo69 function and generated a key using the proposed key generation method. The proposed work has many advantages than the existing methods.

References

- [1] S. William, "Cryptography and Network Security: Principles and Practice", 2nd edition, Prentice-Hall, Inc., 1999.
- [2] S. Hebert, "A Brief History of Cryptography", an article available at <http://cybercrimes.net/aindex.html>.
- [3] ATUL KAHATE, "Computer and Network security".
- [4] K. Gary, "An Overview of Cryptography", an article available at www.garykessler.net/library/crypto.html.
- [5] E. Surya, C. Divya, "A Survey on Symmetric Key Encryption Algorithms", International Journal of Computer Science & Communication Networks, Vol 2(4), 475-477.
- [6] Tony M. Damico, "A Brief History Of Cryptography", an article available at <http://www.studentpulse.com/articles/41/a-briefhistory-of-cryptography>.
- [7] Cryptography, <http://www.newworldencyclopedia.org/entry/Cryptography>.
- [8] Oded Goldreich, "Foundations of cryptography: basic tools", 2001.