# Secure Storage of Crime Data Using Modern Cryptography

By Code Discussion

## 1.Problem Definition

In Police departments , data of criminals is highly confidential. But for the purpose of department, that data is transferred from one department to another. In this process that data can hacked by supporters of the criminals and can be corrupted. In order to keep this data secured we propose a solution Modern Cryptography.

### 1.1 INTRODUCTION

Cryptography is a technique to hide the data over communication channel. Securing Crime data over communication channel is very essential and it needs to be secured. At present, Police department stores data of crime records in cloud database. Although the cloud database improves the efficiency of use, it also poses a huge impact and challenge to the secure storage of data. We try to implement combination of Symmetric encryption using AES and DES to safely send the data over channel so that no crime data gets leaked.



## 2.List of Objectives to be achieved

- We propose a Modern cryptography which was suitable for encryption and decryption of a message. We use symmetric encryption technique.
- Here DES and AES algorithms are used for encryption and decryption of the message.
- We make sure that Receiver decrypts the encrypted symmetric key using AES algorithm by allowing the created key to decrypt it. With obtained key, receiver further decrypts the encrypted message and he gets access to the message.

- We try to implement combination of Symmetric encryption (AES and DES) to safely send the data over channel so that no crime data gets leaked.

## 3.Survey of the Literature

| S.No | NAME | AUTHOR | SUMMARY |
|---|---|---|---|
| 1. | Implementation Of Modern Cryptography Algorithm | Mr. Mahavir Jain Mr. Arpit Agrawal | At present, various types of cryptographic algorithms provide high security to information on networks, but they are also have some drawbacks. To improve the strength of these algorithms, we propose a new Modern cryptographic algorithm in this paper. In this paper two cryptography techniques were used(DES , IDEA). |
| 2. | Privacy Preserving in Data Mining Using Modern Approach | Savita lohiya Lata ragha | we propose a method called Modern approach for privacy preserving. First we randomizing the original data. Then we apply generalization on randomized or modified data. This technique protect private data with better accuracy, also it can reconstruct original data and provide data with no information loss, makes usability of data. |
| 3. | A Survey Paper on Data security in Cloud Computing | Sajjan R.S., Vijay Ghorpade and Vishvajit Dalimbkar | Data is not secure in the cloud because the unauthorized user can try to use of the private data. So providing the data security it uses the different encryption method to protect the data. So that in the proposed study it use the multilevel encryption algorithm. In the multilevel encryption it combines two different algorithms for providing the better security |

| | | | |
|---|---|---|---|
| 4. | A Survey Paper on Data Storage & Security in Cloud Computing | Shradha Parmeshwar Awatari et. al. | *Data is not secure in the cloud because the unauthorized user can try to use of the private data. So providing the data security it uses the different encryption method to protect the data. So here we use multilevel encryption which combines two different algorithms for providing the better security..* |
| 5. | Improving the security by using various cryptographic techniques in cloud computing | Gaurav Jain ; Vikas Sejwar | This paper describes in which A network, there is no complete security solution to secure data and applications or services, but satisfactory risk management can reduce the stage of risks. In our work, we used various techniques like AES, RSA and DES for proposed achieving higher security a cloud. |
| 6 | Modern Encryption Algorithms for Medical Data Storage Security in Cloud Database | Fenghua Zhang Yaming Chen Weiming Meng Qingtao Wu | In this paper The experimental results show that the Modern encryption algorithm has the advantages of fast encryption and decryption speed, high security, good processing ability for longer data, and can solve the data security problem in cloud database to a certain extent. |

| | | | |
|---|---|---|---|
| 7. | A Survey on Secure Cloud: Security and Privacy in Cloud Computing | Shyam Nandan Kumar , Amit Vajpayee | This survey paper introduces a detailed analysis of the cloud security problem. In this paper various existing approaches related to data encryption and message authentications are discussed. After study the existing approaches, issues and challenges are point out during data processing over the cloud. |
| 8. | Modern Cryptographic Based Approach for Privacy Preservation | Ajaysinh Rathod Vivaksha Jariwala | This paper explains User requires man important information based on their location to perform their task like location-based navigation, location-based information, and many more. The user has to give their important information like user identity and |

| | | | |
|---|---|---|---|
| | | | location information to the provider that are personalized. |
| 9. | A Review Paper of Data Security in Cloud Computing | Ravikant Gupta<br>Dr. Ravikant Kapoor | . These algorithm proposed by authors and researchers have their own advantages and disadvantages. Purpose of this paper is to do exhaustive survey to find out research gap and challenges for suggesting a feasible solution with a new approach and to set future research direction. |

| | | | |
|---|---|---|---|
| 10. | Secure cloud computing: Benefits, risks and controls | Mariana Carroll ; Alta van der Merwe ; Paula Kotzé | The focus of this paper is on mitigation for cloud computing security risks as a fundamental step towards ensuring secure cloud computing environments. |
| 11. | Security issues in cloud environments: a survey | Diogo A. B.Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire Pedro R. M. Inácio | This paper surveys the works on cloud securit / issues, making a comprehensive review of the literature on the subject. It addresses severa l key topics, namely vulnerabilities, threats, and attacks, proposing a taxonomy for their classification. |
| 12. | A survey of security issues for cloud computing | Minhaj AhmadKhan | In this paper, we present a survey of security issues in terms of security threats and their remediations. The contribution aims at the analysis and categorization of working mechanisms of the main security issues and the possible solutions that exist in the literature. |

| | | | |
|---|---|---|---|
| 13. | Secure Data Sharing in the Cloud | Danan Thilakanathan<br><br>Shiping Chen<br>Surya Nepal<br>Rafael A. Calvo | This paper explains about the enabling of data sharing capabilities |
| 14. | Cloud security issues and challenges: A survey | AshishSinghKakaliChatterjee | This paper discussed about the basic features of the cloud computing, security issues, threats and their solutions. Additionally, the paper describes several key topics related to the cloud, namely cloud architecture framework, service and deployment model, cloud technologies, cloud security concepts, threats, and attacks. |
| 15. | Security in Cloud Computing using Cryptographic Algorithms | Shobhankar Rajvanshi Himanshu Bansal | We aimed at analyzing different combinations of encryption algorithms, on the basis of different performance parameters to deduce a Modern algorithm which can secure data more efficiently on cloud. |

## 4.Techniques to be Used & Experimental Setup

**i**. PYTHON language



PYTHON Language will be used to write the code(pycrypto and numpy modules were used) **ii**. windows os **iii**. DES (Data Encryption Standard)

The Data Encryption Standard (DES) is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

**IV**. AES:

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The **AES algorithm** (also known as the Rijndael **algorithm**) is a symmetrical block cipher **algorithm** that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits.

## 5.Proposed Model and Techniques Used:

**Data Encryption Standard**

The Data Encryption Standard (DES) is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the Fig.

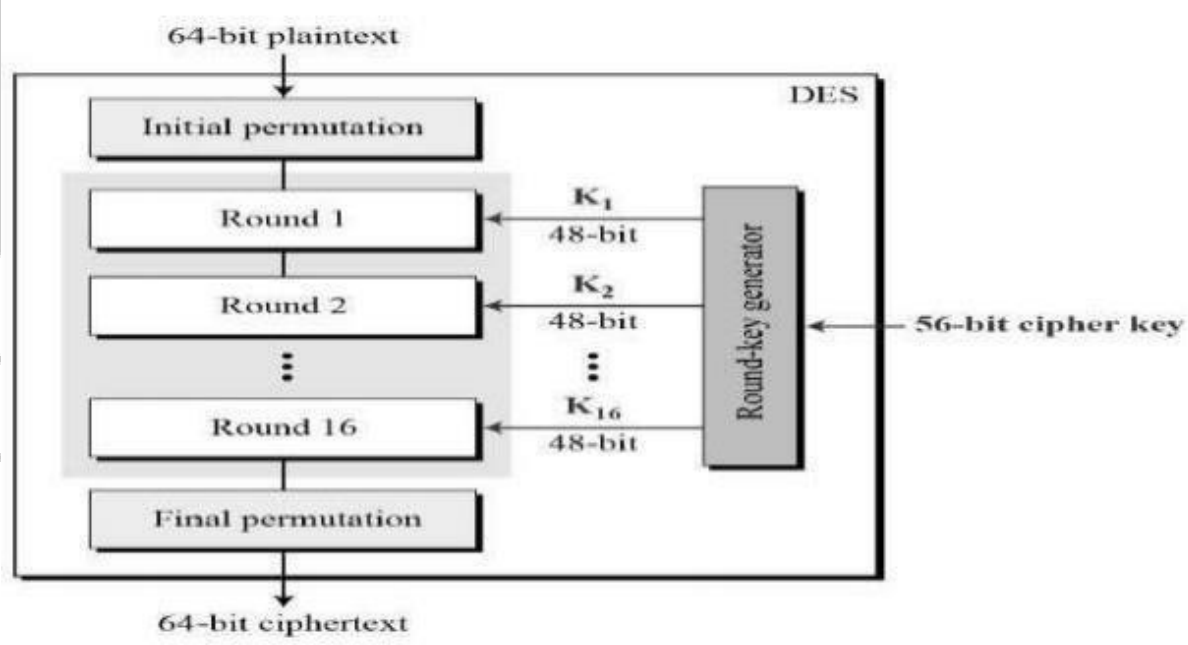



**Figure 3.1 DES Implementation Process Flow**

Since DES is based on the Feistel Cipher, all that is required to specify DES is –

• Round function • Key schedule • Any additional processing – Initial and final permutation

**Initial and Final Permutation**

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown in Fig

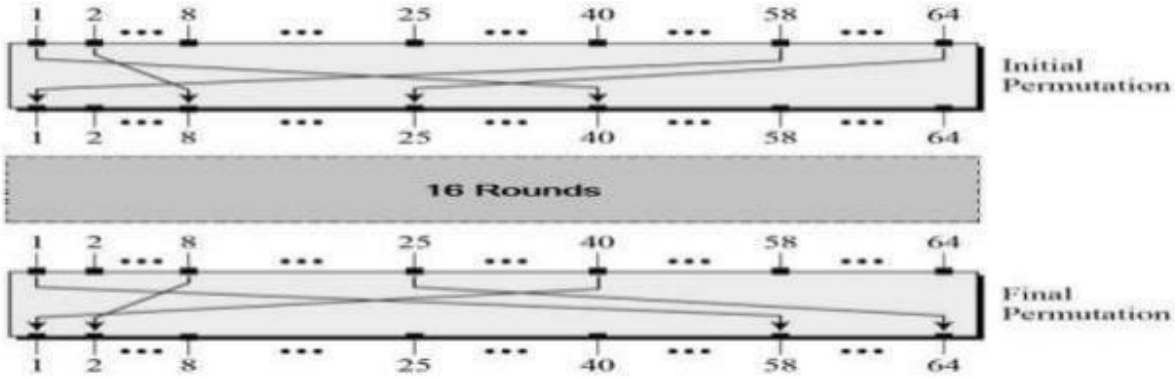



**Figure 3.2 Initial and Final Permutation Process Flow**

## Round Function

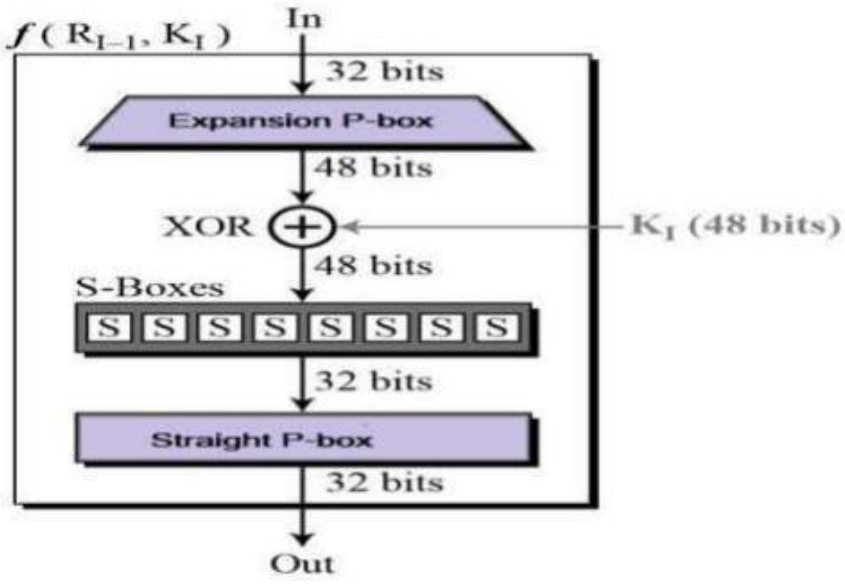


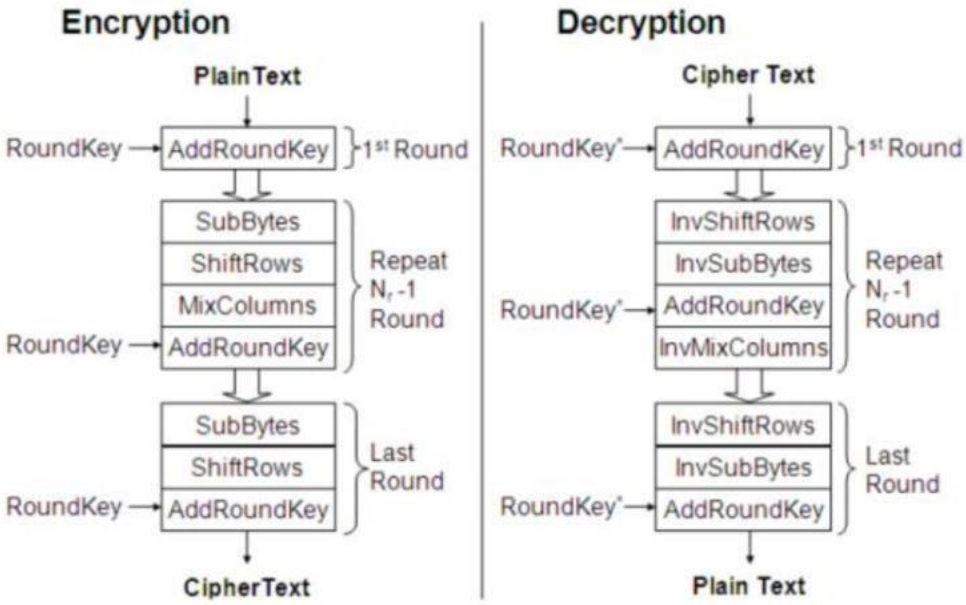

**Figure 3.3 Round function Process flow**

## AES:

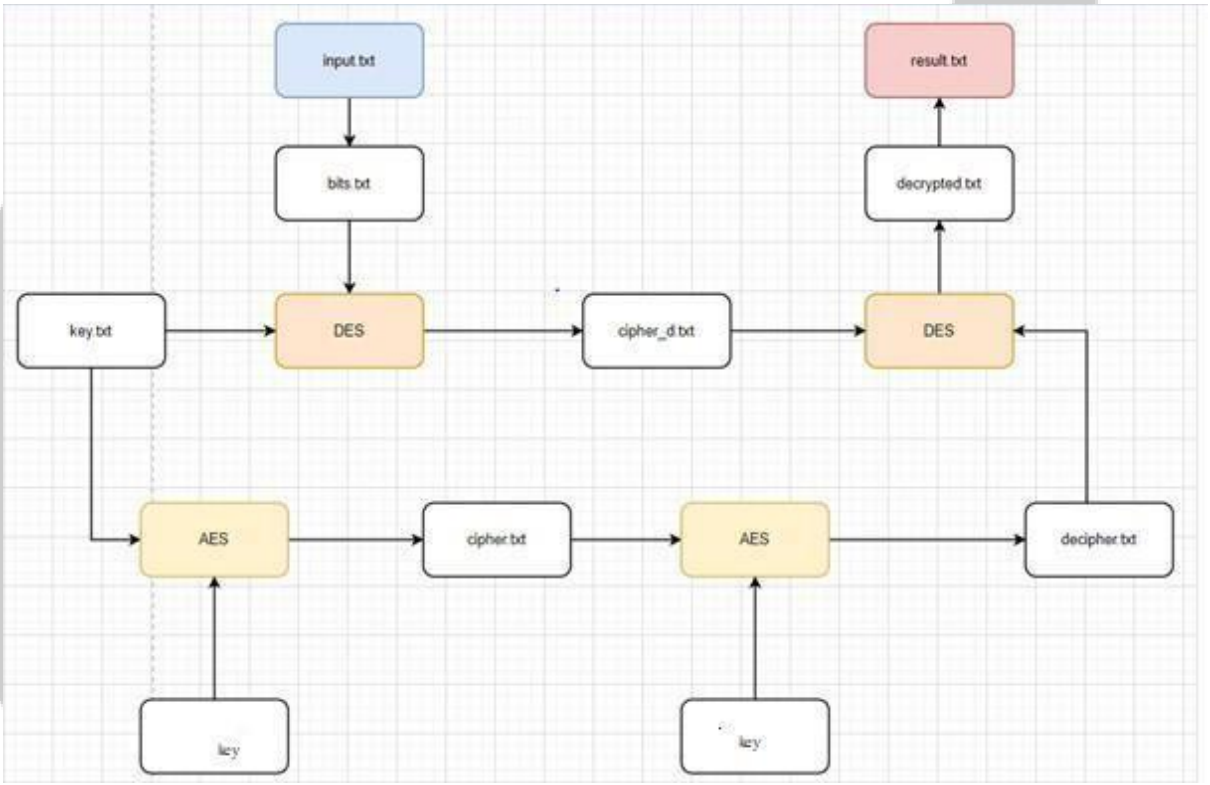
The cryptographic algorithm AES (Advanced Encryption Standard) uses any sized plain text and a 128, 192 or 256 bit key (32 bytes) and here the key size that we have taken is 256 bits that is 32 bytes which provides a stronger encryption over the 128 or 192 bits versions.

AES makes the encryption standard more powerful that can't be broken or hacked by the hackers or intermediates and they can't even see the credential details. AES is a subset of the Rijndael block cipher. AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits but here we are using only 256-bit key size.

The encryption and the decryption flowcharts of AES algorithm are shown below:



**Process flow diagram:**




(Process flow diagram)



## 7.List of objectives achieved

- DES encryption and Decryption
- AES encryption and Decryption
- Secure Data Transfer Between Client and Server

# Initialization vector (IV)

Your encrypted or decrypted message will be stored in the

output file within the directory you are in as well as displayed

within the terminal

- An Initialization Vector (IV) is being used for the extra credit nodes
- -If the IV is not set by the user it will be randomly generated
- -If it's randomly generated it will add it to the first bytes of the file
- -This means when decrypting the cipherText, you must select randomly
- generated so that it knows to strip the first bytes of the ciphertext

An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.

The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.



The ideal IV is a random number that is made known to the destination computer to facilitate decryption of the data when it is received. The IV can be agreed on in advance, transmitted independently or included as part of the session setup prior to exchange of the message data. The length of the IV (the number of bits or bytes it contains) depends on the method of encryption. The IV length is usually comparable to the length of the encryption key or block of the cipher in use.

# 9.Reference


1. Implementation Of Modern Cryptography Algorithm

https://ieeexplore.ieee.org/abstract/document/6375212/ 2. Privacy Preserving in Data Mining

Using Modern Approach

https://www.researchgate.net/profile/Rajani_Sajjan/publication/313647411_A_Survey_Paper_on_Data_security_in_Cloud_Computing/links/58a1664192851c7fb4bf50a5/A-Survey-PaperonDatasecurity-in-Cloud-Computing.pdf

3. A Survey Paper on Data security in Cloud Computing

http://www.gujaratresearchsociety.in/index.php/JGRS/article/view/3197 4.

A Survey Paper on Data Storage & Security in Cloud Computing

https://ieeexplore.ieee.org/abstract/document/8250721/

5. Improving the security by using various cryptographic techniques in cloud computing
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388492

6. Modern Encryption Algorithms for Medical Data Storage Security in Cloud Database
http://www.academia.edu/download/41895018/ajss-4-1-2.pdf

7. A Survey on Secure Cloud: Security and Privacy in Cloud Computing

https://link.springer.com/chapter/10.1007/978-3-030-11437-4_3

8. Modern Cryptographic Based Approach for Privacy Preservation

http://www.academia.edu/download/53949881/084.pdf 9. A Review Paper of Data Security in

Cloud Computing https://ieeexplore.ieee.org/abstract/document/6027519/

10. Secure cloud computing: Benefits, risks and controls
https://link.springer.com/content/pdf/10.1007/s10207-013-0208-7.pdf

11. Security issues in cloud https://www.sciencedirect.com/science/article/pii/S1084804516301060

12. environments: a survey
https://link.springer.com/chapter/10.1007/978-3-642-38586-5_2

13. A survey of security issues for cloud computing
https://www.sciencedirect.com/science/article/pii/S1084804516302983

14. Secure Data Sharing in the Cloud
http://www.ir.juit.ac.in:8080/jspui/bitstream/123456789/17046/1/131212%2C131217.pdf

15. Security in Cloud Computing using Cryptographic Algorithms

http://www.ir.juit.ac.in:8080/jspui/bitstream/123456789/17046/1/131212%2C131217.pdf