# **CMR COLLEGE OF ENGINEERING & TECHNOLOGY**

AN AUTONOMUS INSTITUTION WITH NAAC ACCREDITAION (A+ GRADE)

APPROVED BY AICTE, PERMANENTLY AFFILIATED TO JNTUH, NBA ACCREDITATION

### KANDLAKOYA (V), MEDCHAL ROAD, HYDERABAD -501401.

**COURSE NAME : MATRICES AND CALCULUS**

**COURSE CODE : A400001**

**ROLL NUMBER :22H51A7334**

**22H51A7335**

**22H51A7336**

**TEAM MEMBERS :K SHARATH NAIK**

**PAVANI KILARI**

**SRIRAM KOMMA**

**BRANCH & SECTION :AIM-A**

**SEMESTER : I**

**ACADEMIC YEAR : 2022-23**

**CASE STUDY ON :MATRIX INVERSION METHOD**

1. **IDENTIFICATION OF THE PROBLEM:**

Security: The security of cryptography systems that use matrix inversion can be threatened by attacks such as brute-force attacks and mathematical attacks. In a brute-force attack, an attacker tries all possible keys until the correct key is found, while in a mathematical attack, an attacker uses mathematical techniques to find the private key and decrypt messages.

1. **METHODOLOGY:**

The security of cryptography systems that use matrix inversion can be threatened by different types of attacks, including brute-force attacks and mathematical attacks.

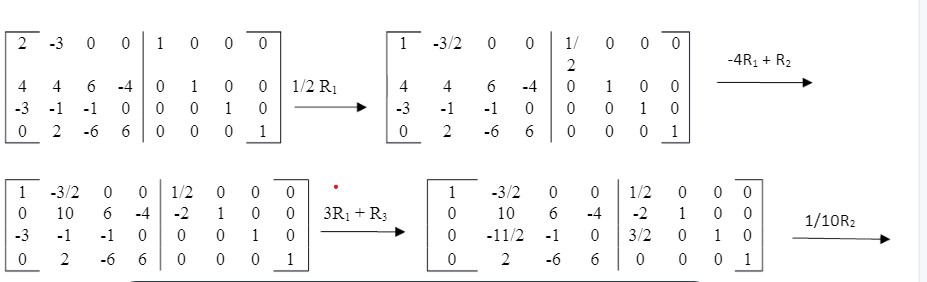
In a brute-force attack, an attacker tries all possible keys until the correct key is found. This type of attack can be time-consuming, especially for large keys, but it is still a potential threat to cryptography systems.

In a mathematical attack, an attacker uses mathematical techniques to find the private key and decrypt messages. This type of attack is more sophisticated and can be more effective than a brute-force attack. For example, attackers may use algorithms such as the RSA Factoring Challenge or the Integer Factorization Algorithm to find the private key and decrypt messages.

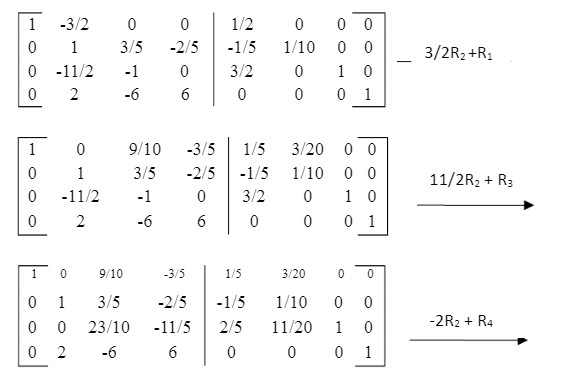
In order to counter these types of attacks, cryptography systems that use matrix inversion must be designed with security in mind. This may involve using secure key-generation techniques, implementing secure protocols for key exchange, and using secure encryption algorithms. Additionally, it is important to regularly update and improve cryptography systems to stay ahead of evolving threats and attacks

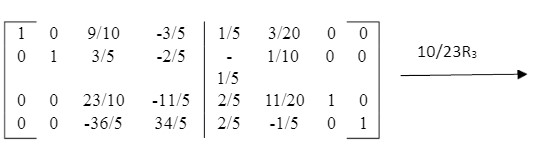
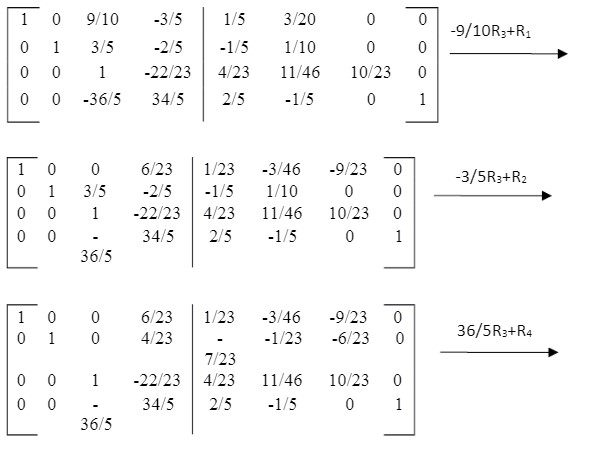
To solve the question, we used inverse matrix and basic matrix operation which is matrix multiplication. Below are the steps that we used to solve the question.

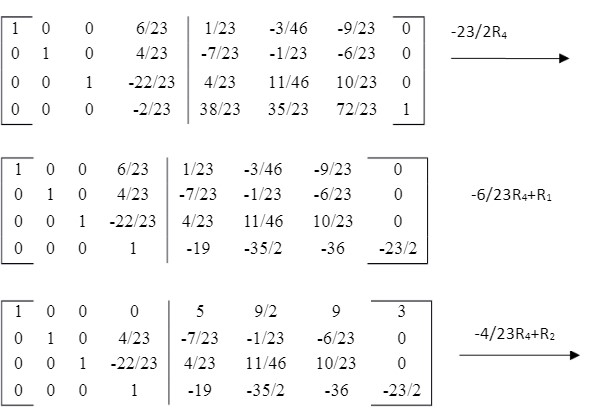
STEP 1 : Inverse the given Matrix B.

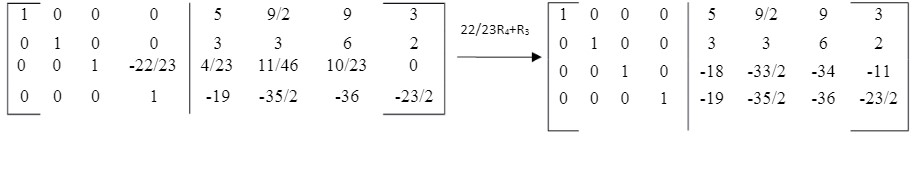


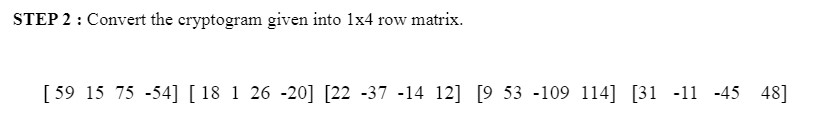
––––

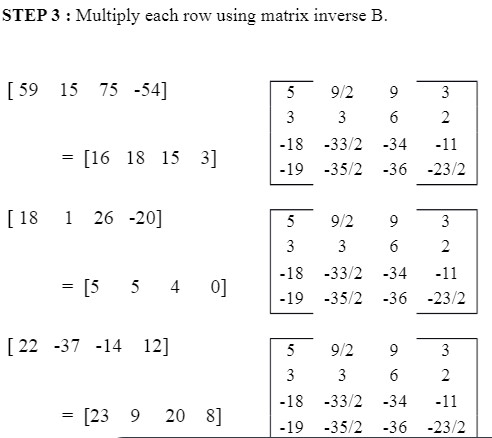


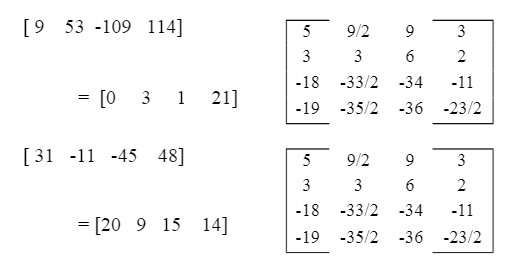


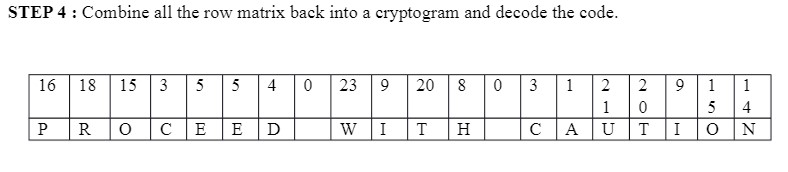












1. **EFFECTIVE SOLUTIONS:**

There are several solutions to address the security issues associated with cryptography systems that use matrix inversion:

Key length: Increasing the key length can make brute-force attacks much more difficult and time-consuming, as the number of possible keys increases exponentially with key length. This is a common solution to improve the security of cryptography systems.

Key generation: Implementing secure key-generation techniques, such as using secure random number generators, can help ensure the security of the keys used in cryptography systems.

Key exchange: Using secure protocols for key exchange, such as Diffie-Hellman key exchange, can help ensure the confidentiality of the keys used in cryptography systems.

Cryptography algorithms: Implementing secure encryption algorithms, such as Advanced Encryption Standard (AES) or the Rivest-Shamir-Adleman (RSA) algorithm, can help ensure the security of cryptography systems that use matrix inversion.

Regular updates: Regularly updating and improving cryptography systems to stay ahead of evolving threats and attacks is an important part of maintaining the security of cryptography systems that use matrix inversion.

Post-Quantum Cryptography: With the rise of quantum computing, it's important to consider post-quantum cryptography, which are cryptographic algorithms that are resistant to quantum computing attacks.

1. **RESULTS & DISCUSSIONS:**

In conclusion, there are several solutions to address the security issues associated with cryptography systems that use matrix inversion, including increasing key length, implementing secure key-generation techniques, using secure protocols for key exchange, implementing secure encryption algorithms, regularly updating cryptography systems, and using post-quantum cryptography. These solutions can help ensure the security and confidentiality of communication systems that use matrix inversion.

**~THANKYOU**