CRYPTOGRAPHY PROJECT REPORT

NAME: ANSHU KUMAR

ROLLNO: 21CSB0A05

CHOSSEN CYPHER TEXT ATTACK (CCA ATTACK)

INTRODUCTION:

This project investigates the vulnerabilities of RSA encryption through the lens of Chosen Ciphertext Attacks (CCA), focusing on a scenario involving Alice, Bob, and Eve. By illustrating how Eve, the attacker, can exploit weaknesses in RSA encryption to intercept and manipulate ciphertexts, we shed light on the importance of addressing CCA vulnerabilities and propose countermeasures to mitigate their risks.

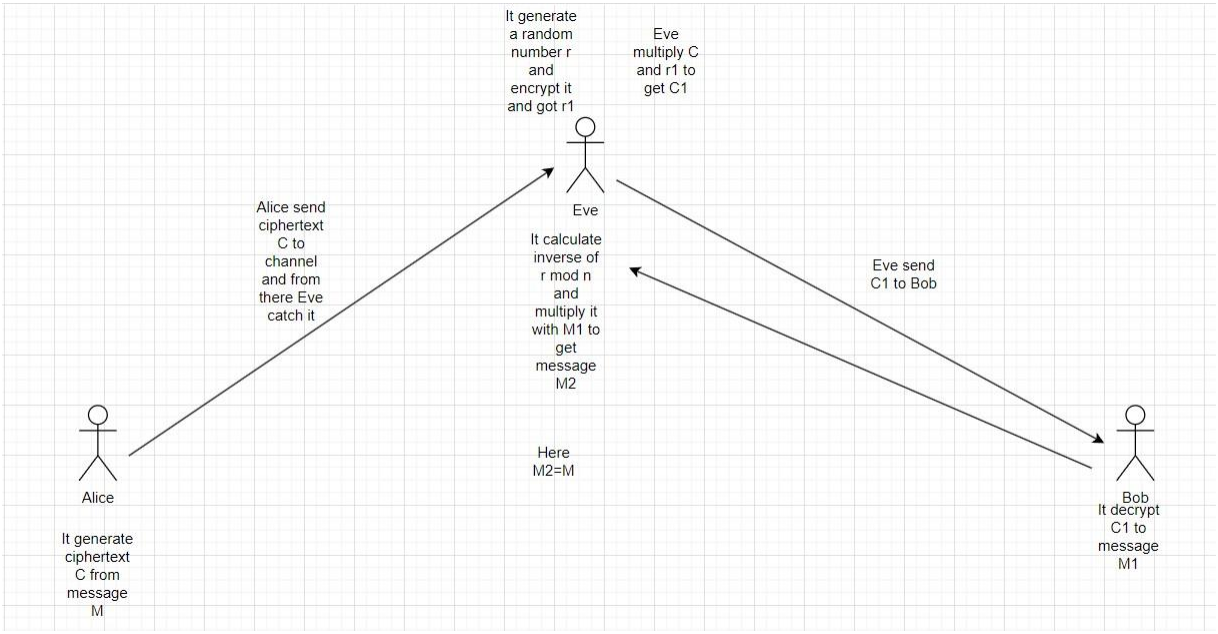
SCENERIO

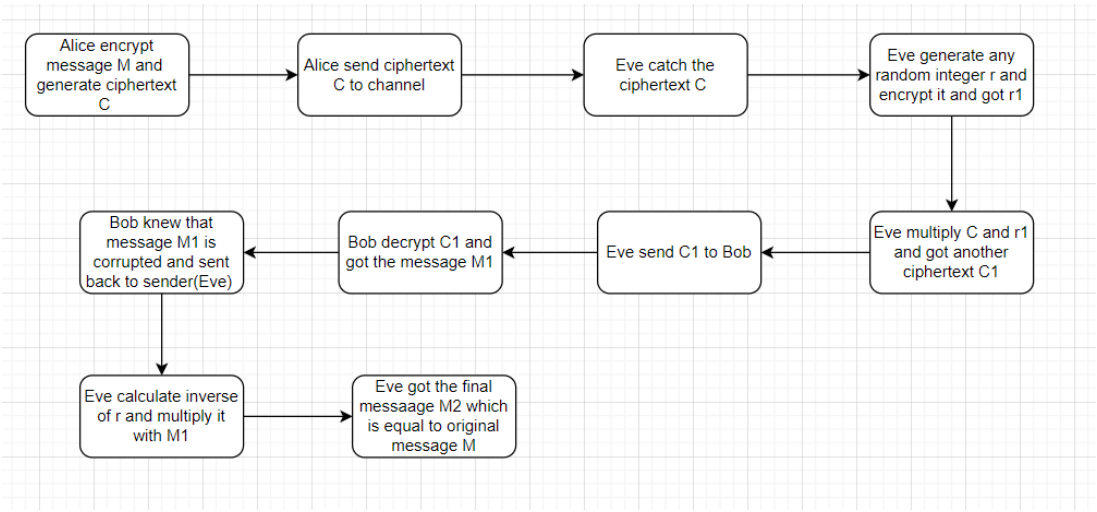
A legitimate user "Bob" sends a message that is intercepted by an attacker "Eve" Eve manipulates the message by multiplying it by a random number r raised to the power of e mod n (these are public values that are within the access of anybody including the attacker). Now Eve can use this manipulated message as a chosen ciphertext and send it to Bob decrypts the message, but from Bob's perspective the message is corrupt (the multiplication that Eve performed has changed the message and made it unintelligible), let that Bob uses a protocol that returns back corrupt messages (without encrypting it again, as it's no use to encrypt a corrupt message) to the one who sent it (to request re-transmission for example) Eve will calculate the inverse of r mod n using extended Euclidean algorithm and multiply the message returned from Bob with the inverse of r to retrieve the original message without the need of learning the key and regardless its size.

1. **Objectives:**
   1. To analyze the vulnerabilities of RSA encryption exposed by Chosen Ciphertext Attacks through a specific scenario.

   2. To propose effective countermeasures to mitigate the risks associated with CCA in

RSA encryption, thereby enhancing the security and integrity of encrypted communication systems.





Algorithm:

step1: Alice Encrypt message M and generate ciphertext **C=M^e % n.**

step2: Alice send the ciphertext C to the communication channel.

step3: Eve catch ciphertext C from the channel.

step4: Eve generates a random integer r and encrypt it and got **r1=r^e mod n.**
step5: Eve multiply r1 with ciphertext C and got another ciphertext C1.
step6: Eve send C1 to Bob.
Step7: Bob decrypt C1 and got the message **M1=C1^d mod n.**
step8: Bob knew that message M1 is corrupted and sent it back to Sender (Eve).
step9: Eve calculates the **inverse of r mod n** and multiply it with M1.
step10: Eve got the final message **M2=M1 * Inverse of r and here M2 = M.**

Result Analysis:

The result of the project demonstrates a vulnerability in RSA encryption known as a Chosen Ciphertext Attack (CCA). This scenario illustrates how Eve, the attacker, can intercept and manipulate ciphertexts exchanged between Alice and Bob, ultimately allowing Eve to decipher the original message without possessing the private decryption key. By exploiting weaknesses in the encryption process, Eve successfully deceives Bob into decrypting a corrupted message, highlighting the importance of implementing robust security measures to mitigate the risks posed by CCA in RSA encryption.

2. **Conclusion:**

The scenario exemplifies the **vulnerability of RSA encryption to Chosen Ciphertext Attacks (CCA).** By exploiting weaknesses in the encryption process, an attacker like Eve can intercept and manipulate ciphertexts, compromising the confidentiality and integrity of encrypted communication. This underscores the critical importance of implementing robust security measures to mitigate the risks posed by CCA in RSA encryption. Moving forward, continued research and advancements in cryptographic protocols are essential to bolstering the resilience of encryption algorithms against evolving threats and ensuring the security of digital communication in an increasingly interconnected world.

3. **Learning outcomes**
    a. Understanding of the vulnerability of RSA encryption to Chosen Ciphertext Attacks (CCA).
    b. Recognition of the importance of robust encryption schemes in safeguarding sensitive information.
    c. Awareness of the implications of insecure communication practices

in cryptographic systems.

d. Appreciation of the need for stringent security measures to mitigate risks in digital communication.
e. Insight into the ongoing research and advancements in cryptographic protocols to enhance security.

4. **Source code:** [click here]

Proof:

$$c1 = c * r^{e} \bmod n$$
$$c1 = m^{e} \bmod n * r^{e} \bmod n$$
$$c1 = (m * r)^{e} \bmod n$$

$$m1 = c1^{d} \bmod n$$
$$m1 = ((m * r)^{e} \bmod n)^{d} \bmod n$$
$$m1 = (m * r)^{e*d} \bmod n$$
$$m1 = (m * r) \bmod n$$

$$m2 = m1 * r^{-1} \bmod n$$
$$m2 = ((m * r) \bmod n) * r^{-1} \bmod n$$
$$m2 = (m * r * r^{-1}) \bmod n$$
$$m2 = m \bmod n$$