INTEGRITY CHECKER

TEAM MEMBERS AND THEIR CONTRIBUTION

S.NO	NAME	Registration NUMBER
1)	Yakkala Tarun Sai	AP18110010469
2)	B.V.S.Neeraj	AP18110010474
3)	M.Sri Krishna Kumar	AP18110010506

ABSTRACT:

Our project “Integrity Checker” targets in developing a chat system with data integrity and sender identification validation.We used different cryptographic techniques and algorithms in this project to show valid output.This is a chat system in which message is passed between the sender and receiver.The process between this sending and receiving is being created and monitored in this project.This project can be implemented in chat applications like whatsapp,messenger,telegram etc. By implementation of this project all the CIA(confidentiality , integrity and authentication)triads can be maintained.

INTRODUCTION:

Integrity checker can be formally defined, as, if person-A is sending a message to person-B, then there shouldn't be any kind of third person's view or access is not allowed. So we basically involve three main triads i.e, Integrity

Authenticity

Confidentiality

If the message should carry forward in a proper way or that message should convey in a proper way integrity carries its own role, suppose if the message (hi) should be sent from person-A to person-B without any change like(ih)then triad (integrity) is used.And in between the process of message transmission there shouldn't be any access to any third party community, so this job is accomplished with the help of confidentiality. If we have to know whether the message was sent by a person or some software systems the triad mainly used here is (authenticity).So these triads are base for the implementation of the project and also very much needed for the whole cyber security .

Finally authenticity and integrity are used for message authenticity and confidentiality is also maintained in the project so that the third person is not allowed to view our messages or information.

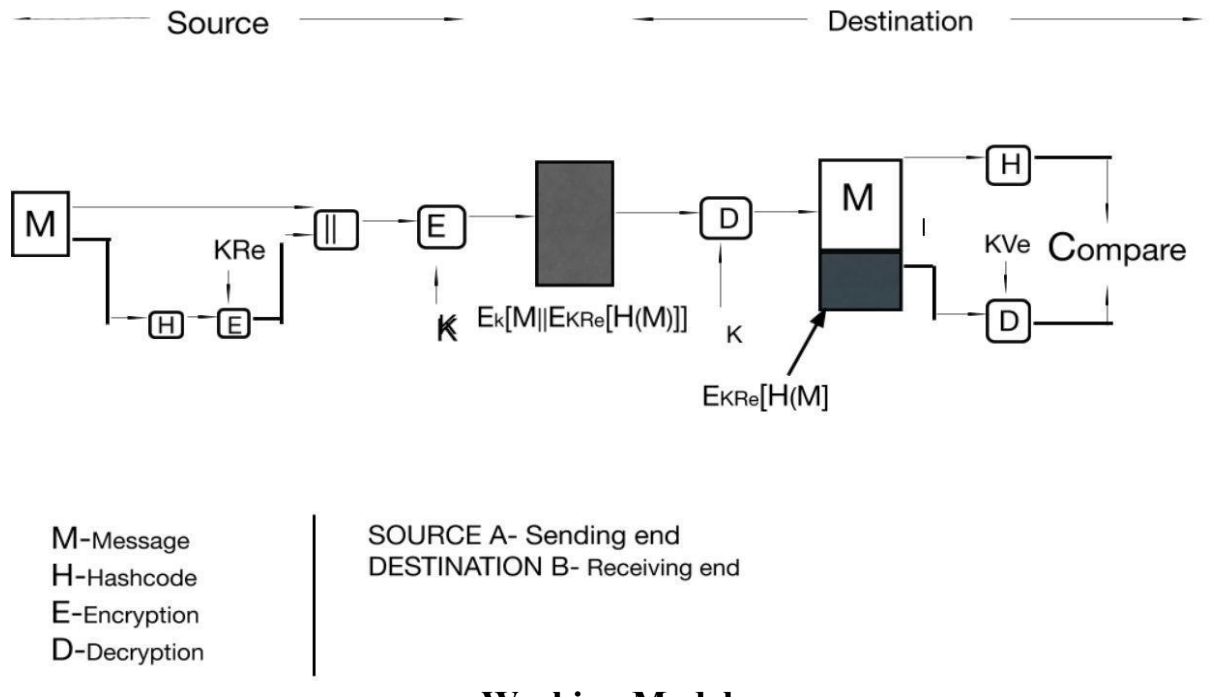
In the subsequent pages the working model of the project is explained.

WORKING:

Hashing is a technique that creates a sequence of bytes by performing cryptographic calculations on a block of data. Hashes are constant in size and do not expand or contract based on the content of the input data. Also, hashes are one-way functions, which means they can't be reversed.

When a block of data is hashed, it can't be decrypted and returned to its original state. Applications use hash functions to protect sensitive information such as passwords.

The regular method may be faster but the encryption and decryption using hash functions provides an additional layer of security.



Working Model

This application deals with a Source and Destination, i.e, here Source refers to sender and Destination refers to receiver, when message is sent

from sender to receiver then the message will goes through the hash function, and the generated output undergoes RSA encryption using the private key of the sender. Then in the next step the original message given as input is appended with the output generated from the RSA encryption.

After appending the output will be encrypted using the AES algorithm. By using TCP/IP Server and Client system message will be transferred to the receiver then the sent message will be decrypted using AES algorithm then we get the decrypted output that will be divided into two parts. The first part which is the original message is sent into the hash function and the rest half part undergoes RSA decryption using a public key. Both the generated outputs i.e, the output generated from RSA decryption and the output generated from the hash function are compared. If both the outputs are the same then we say that the integrity is maintained.

PROPOSED SYSTEM:

This project is implemented using python(3.7 and above)

Inbuilt Libraries used in project: socket
crypto
hashlib
binascii
base64

Algorithm(Without TCP/IP):

STEP-1: Take the input/Plain Text from the User.

STEP-2: Implement Different Cryptographic Algorithms for Encryption of the Plain Text

i) Implement Hash Function on the Plain Text given by the user.

ii) Implementation of RSA Encryption is done on the output generated from the hash function.

iii)RSA Encryption is implemented on the output of Hash function and the output of the RSA Encryption is appended to the original input/Plain Text.

*** Output of the RSA Encryption is appended to the original input/Plain Text=Cipher Text***

STEP-3: Implement the Decryption process of the above mentioned Cryptographic Algorithms in the following order:

i) AES Decryption is implemented on the Cipher Text.

ii)After AES Decryption we get original message/Plain Text appended with the output generated from the RSA Encryption as output.

iii)Implement hash function on the original message/Plain Text which is generated after the AES Decryption.---> 1

iv)Implement RSA Decryption on the RSA encrypted hash value of the input message from the output generated by AES Decryption--->2

STEP-4: Compare both 1 and 2 and: if

there are equal:

Successful implementation

else:

Error in the code.

Algorithm(With TCP/IP):

STEP-1: Take the input/Plain Text from the User

STEP-2: Implement Different Cryptographic Algorithms for Encryption of the Plain Text

i) Implement Hash Function on the Plain Text given by the user.

ii) Implementation of RSA Encryption is done on the output generated from the hash function.

iii)RSA Encryption is implemented on the output of Hash function and the output of the RSA Encryption is appended to the original input/Plain Text.

*** Output of the RSA Encryption is appended to the original input/Plain Text=Cipher Text***

STEP-3: Using TCP\IP protocol we send the message from one device to another device.

STEP-4: Implement the Decryption process of the above mentioned Cryptographic Algorithms in the following order:

i) AES Decryption is implemented on the output of the TCP\IP protocol.

ii) After AES Decryption we get original message/Plain Text appended with the output generated from the RSA Encryption as output.

iii)Implement hash function on the original message/Plain Text which is generated after the AES Decryption.---> 1

iv)Implement RSA Decryption on the RSA encrypted hash value of the input message from the output generated by AES Decryption--->2

STEP-5: Compare both 1 and 2 and: if

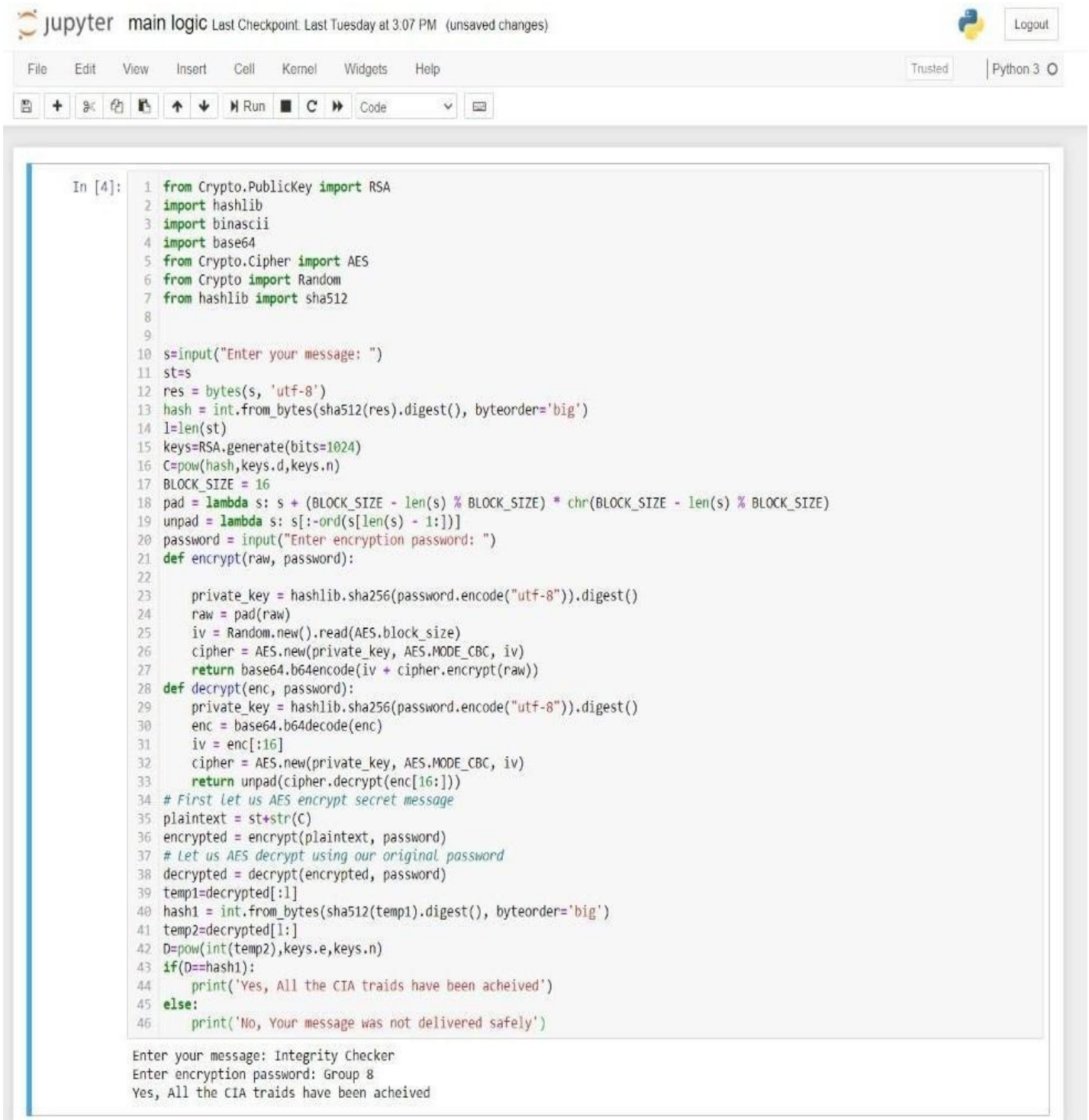
there are equal:

Successful implementation

else:

Error in the code.

PERFORMANCE ANALYSIS:



OUTPUT SCREENSHOTS:

```
Enter your message: This is Crytopgraphic project
Enter encryption password: Secret
Yes, All the CIA traids have been acheived

Enter your message: Integrity Checker
Enter encryption password: Group 8
Yes, All the CIA traids have been acheived
```

Problems Faced:

We faced a problem while transmitting the encrypted message from sender to receiver using TCP/IP Server and Client.

- We are getting an error while we are decrypting the message on the receiver side that was sent from the sender.