SECRET COMMUNICATION

A screenshot of a computer

Description automatically generated with low confidence A Mini Project Report

INFORMATION TECHNOLOGY

By

R.SAI SATHVIK

1602-20-737-035

2022A picture containing text

Description automatically generated

Department of Information Technology

Vasavi College of Engineering (Autonomous)

(Affiliated to Osmania University)

Ibrahimbagh, Hyderabad-31

2022

Vasavi College of Engineering (Autonomous)

(Affiliated to Osmania University)

Hyderabad-500-031

Department of Information Technology

DECLARATION BY THE CANDIDATE

I, R.SAI SATHVIK, bearing hall ticket number, 1602-20-737-035, hereby declare that the project report entitled “SECRET COMMUNICATION” Department of Computer Science & Engineering, VCE, Hyderabad, is submitted in partial fulfilment of the requirement for the award of the degree of Bachelor of Engineering in Information Technology.

This is a record of bonafide work carried out by me and the results of this project report have not been submitted to any other university or institute for the award of any other degree or diploma.

R.SAI SATHVIK,

1602-20-737-035.

Vasavi College of Engineering (Autonomous)

(Affiliated to Osmania University)

Hyderabad-500-031

A picture containing text

Description automatically generated Department of Information Technology

BONAFIDE CERTIFICATE

This is to certify that the project entitled “SECRET COMMUNICATION” being submitted by R.SAI SATHVIK, bearing 1602-20-737-035, in partial fulfilment of the requirements for the award of the degree of Bachelor of Engineering in Information Technology is a record of bonafide work carried out by him/her under my guidance.

SECRET COMMUNICATION

A screenshot of a computer

Description automatically generated with low confidence A Mini Project Report

INFORMATION TECHNOLOGY

By

J. SHYAM PRASAD YADAV

1602-20-737-042

2022A picture containing text

Description automatically generated

Department of Information Technology

Vasavi College of Engineering (Autonomous)

(Affiliated to Osmania University)

Ibrahimbagh, Hyderabad-31

2022

Vasavi College of Engineering (Autonomous)

(Affiliated to Osmania University)

Hyderabad-500-031

Department of Information Technology

DECLARATION BY THE CANDIDATE

I, J. SHYAM PRASAD YADAV, bearing hall ticket number, 1602-20-737-042, hereby declare that the project report entitled “SECRET COMMUNICATION” Department of Computer Science & Engineering, VCE, Hyderabad, is submitted in partial fulfilment of the requirement for the award of the degree of Bachelor of Engineering in Information Technology.

This is a record of bonafide work carried out by me and the results of this project report have not been submitted to any other university or institute for the award of any other degree or diploma.

J. SHYAM PRASAD YADAV,

1602-20-737-042.

Vasavi College of Engineering (Autonomous)

(Affiliated to Osmania University)

Hyderabad-500-031

A picture containing text

Description automatically generated Department of Information Technology

BONAFIDE CERTIFICATE

This is to certify that the project entitled “SECRET COMMUNICATION” being submitted by J. SHYAM PRASAD YADAV, bearing 1602-20-737-042, in partial fulfilment of the requirements for the award of the degree of Bachelor of Engineering in Information Technology is a record of bonafide work carried out by him/her under my guidance.

SECRET COMMUNICATION

A screenshot of a computer

Description automatically generated with low confidence A Mini Project Report

INFORMATION TECHNOLOGY

By

M. SAI LAXMI

1602-20-737-034

2022A picture containing text

Description automatically generated

Department of Information Technology

Vasavi College of Engineering (Autonomous)

(Affiliated to Osmania University)

Ibrahimbagh, Hyderabad-31

2022

Vasavi College of Engineering (Autonomous)

(Affiliated to Osmania University)

Hyderabad-500-031

Department of Information Technology

DECLARATION BY THE CANDIDATE

I, M. SAI LAXMI, bearing hall ticket number, 1602-20-737-034, hereby declare that the project report entitled “SECRET COMMUNICATION” Department of Computer Science & Engineering, VCE, Hyderabad, is submitted in partial fulfilment of the requirement for the award of the degree of Bachelor of Engineering in Information Technology.

This is a record of bonafide work carried out by me and the results of this project report have not been submitted to any other university or institute for the award of any other degree or diploma.

M. SAI LAXMI,

1602-20-737-034.

Vasavi College of Engineering (Autonomous)

(Affiliated to Osmania University)

Hyderabad-500-031

A picture containing text

Description automatically generated Department of Information Technology

BONAFIDE CERTIFICATE

This is to certify that the project entitled “SECRET COMMUNICATION” being submitted by M. SAI LAXMI, bearing 1602-20-737-034, in partial fulfilment of the requirements for the award of the degree of Bachelor of Engineering in Information Technology is a record of bonafide work carried out by him/her under my guidance.

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompanies the successful completion of any task would be incomplete without the mention of the people made it possible and whose encouragement and guidance have made our efforts with success.

We are indebted to the Internal Guide, Mrs.L.Divya and Mrs.S.Rajyalakshmi, PROFESSOR, Information Technology, VASAVI COLLEGE OF ENGINEERING, Ibrahimbagh, hyd-31 for her support and guidance throughout the project.

We are also indebted to the Head of the Department, Mr.K.Rammohan, PROFESSOR, Information Technology, VASAVI COLLEGE OF ENGINEERING, Ibrahimbagh, hyd-31 for her support and guidance throughout the project.

We extend our deep sense of gratitude to the Principal, S.V.RAMANA RAO, VASAVI COLLEGE OF ENGINEERING, Ibrahimbagh, hyd-31 permitting us to undertake this project.

TABLE OF CONTENTS:

|  |  |  |
| --- | --- | --- |
| S.NO. | CONTENT | PAGE NO. |
| 1 | INTRODUCTION | 1 |
| 2 | ABSTRACT | 2 |
| 3 | TECHNOLOGY | 3 |
| 4 | MODULES | 4-7 |
| 5 | LIBRARIES | 8-9 |
| 6 | DESIGN | 10-14 |
| 7 | IMPLEMENTATION | 15-24 |
| 8 | TESTING AND RESULTS | 25-31 |
| 9 | ADDITIONAL KNOWLEDGE | 32 |
| 10 | CONCLUSION AND FUTURE WORK | 33 |
| 11 | REFERENCES | 34 |

INTRODUCTION

In this project, we will develop a secret communication flow which helps us in improving new perspective regarding the developing technology. The user gives a combination of any numbers ,letters and symbols which we consider as a string.

Our project receives the information given by user and encodes it and then decodes it such that the information is confined only between the user and the receiver.

The secret communication project is very useful in departments like cyber security also.

In this Python project ,our goal is to build an interface which can do both encoding and decoding of a string.

\*Encoding and Decoding of statement using different standard coding methods which are widely used.

\*Helps in understanding how a text is changed to secret message in order to send them as signal.

\*Changing of text is given highest importance in present online communication in order to make it personal or secret.

\*Used in all types of communication based instruments.

\*It gives a vague idea how many complications happen when we just type a text.

ABSTRACT

Encoding is a method of converting a statement into combination of numbers and letters in a specific method.

Whereas Decoding is breaking down of specific combination and obtaining the statement.

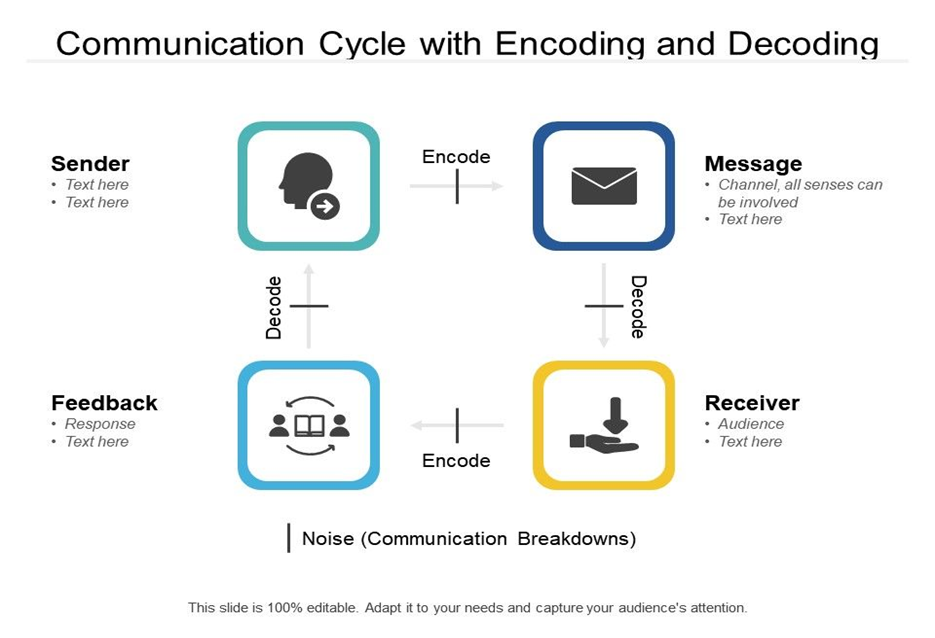
FEATURES

\*Contains a vide range of variety types of Encoding and Decoding.

\*Explains the working of that specific type of coding.

\*Specific details variables that are used are being explained.

\*The user gets to analyse and understand it’s working.



TECHNOLOGY

SOFTWARE

Cryptography is used in order to encrypt and decrypt the message to avoid the revealation of personal messages to the outsiders or inappropriate users and safely reach the receiver.

From cryptography we imported fernet .

\* Fernet guarantees that a message encrypted using it cannot be manipulated or read without the key.

\*Fernet is an implementation of symmetric (also known as “secret key”) authenticated cryptography.

Hardware

\*A computer running either macOS or the Linux operating system (for those on Windows, try setting up a Virtual Machine with a Linux image)

\*A stable internet connection

\*A GPU (preferably)

MODULES

Cryptography

Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries

. So, to protect the message, user first convert his readable message to unreadable form. Here, he converts the message to some random numbers. After that, he uses a key to encrypt his message, in Cryptography, we call this ciphertext.

User sends this ciphertext or encrypted message over the communication channel, he won’t have to worry about somebody in the middle of discovering his private messages. Suppose, an unknown person here discover the message and he somehow manages to alter it before it reaches receiver.

Now, receiver would need a key to decrypt the message to recover the original plaintext. In order to convert the ciphertext into plain text, receiver would need to use the decryption key. Using the key he would convert the ciphertext or the numerical value to the corresponding plain text.

After using the key for decryption what will come out is the original plaintext message, is an error. Now, this error is very important. It is the way receiver knows that message sent by user is not the same as the message that he received. Thus, we can say that encryption is important to communicate or share information over the network.

Text

Description automatically generated

Encryption Algorithms

Cryptography is broadly classified into two categories: Symmetric key Cryptography and Asymmetric key Cryptography (popularly known as public key cryptography.

Graphical user interface, text, application

Description automatically generated

You can install cryptography with:

$ pip install cryptography

Building cryptography on Windows

The wheel package on Windows is a statically linked build (as of 0.5) so all dependencies are included. To install cryptography, you will typically just run

pip install cryptography

If you prefer to compile it yourself you’ll need to have OpenSSL installed. You can compile OpenSSL yourself as well or use a binary distribution. Be sure to download the proper version for your architecture and Python (VC2015 is required for 3.6 and above). Wherever you place your copy of OpenSSL you’ll need to set the LIB and INCLUDE environment variables to include the proper locations. For example:

C:\> \path\to\vcvarsall.bat x86\_amd64

C:\> set LIB=C:\OpenSSL-win64\lib;%LIB%

C:\> set INCLUDE=C:\OpenSSL-win64\include;%INCLUDE%

C:\> pip install cryptography

You will also need to have Rust installed and available.

If you need to rebuild cryptography for any reason be sure to clear the local wheel cache.

LIBRARIES

Fernet is a system for symmetric encryption/decryption, using current best practices. It also authenticates the message, which means that the recipient can tell if the message has been altered in any way from what was originally sent.

USING FERNET

Fernet is included in the cryptography library.

To encrypt and decrypt data, we will need a secret key that must be shared between anyone who needs to encrypt or decrypt data. It must be kept secret from anyone else, because anyone who knows the key can read and create encrypted messages. This means we will need a secure mechanism to share the key. The same key can used multiple times.

CREATING A KEY

We can create a key like this:

from cryptography.fernet import Fernet

key = Fernet.generate\_key()

The key is a random value and will be completely different each time you call the generate\_key function.

ENCRYPTING A MEASSAGE

To encrypt a message, we must first create a Fernet object using the key created previously. We than call the encrypt function, passing the data we wish to encrypt is the form of a bytes array.

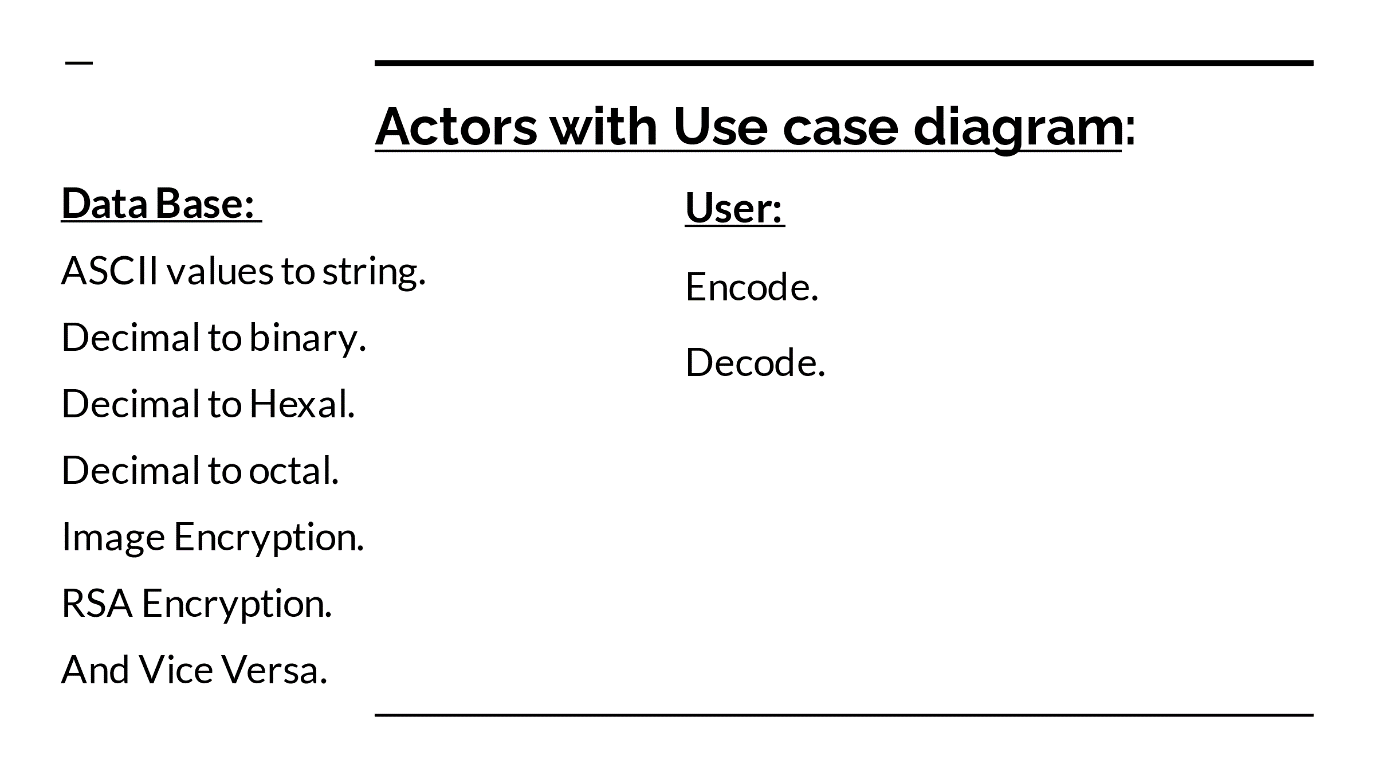
Notice that we use the encode method to convert our message string into a bytes array. If we want to encrypt an image or other data, we must load it into memory as a byte array.

DECRYPTING A MESSAGE

To decrypt a message, we must again create a Fernet object using the same key that was used to encrypt the data. We than call the decrypt function, passing the data we wish to decrypt is the form of a bytes array. The function returns the decrypted original message.

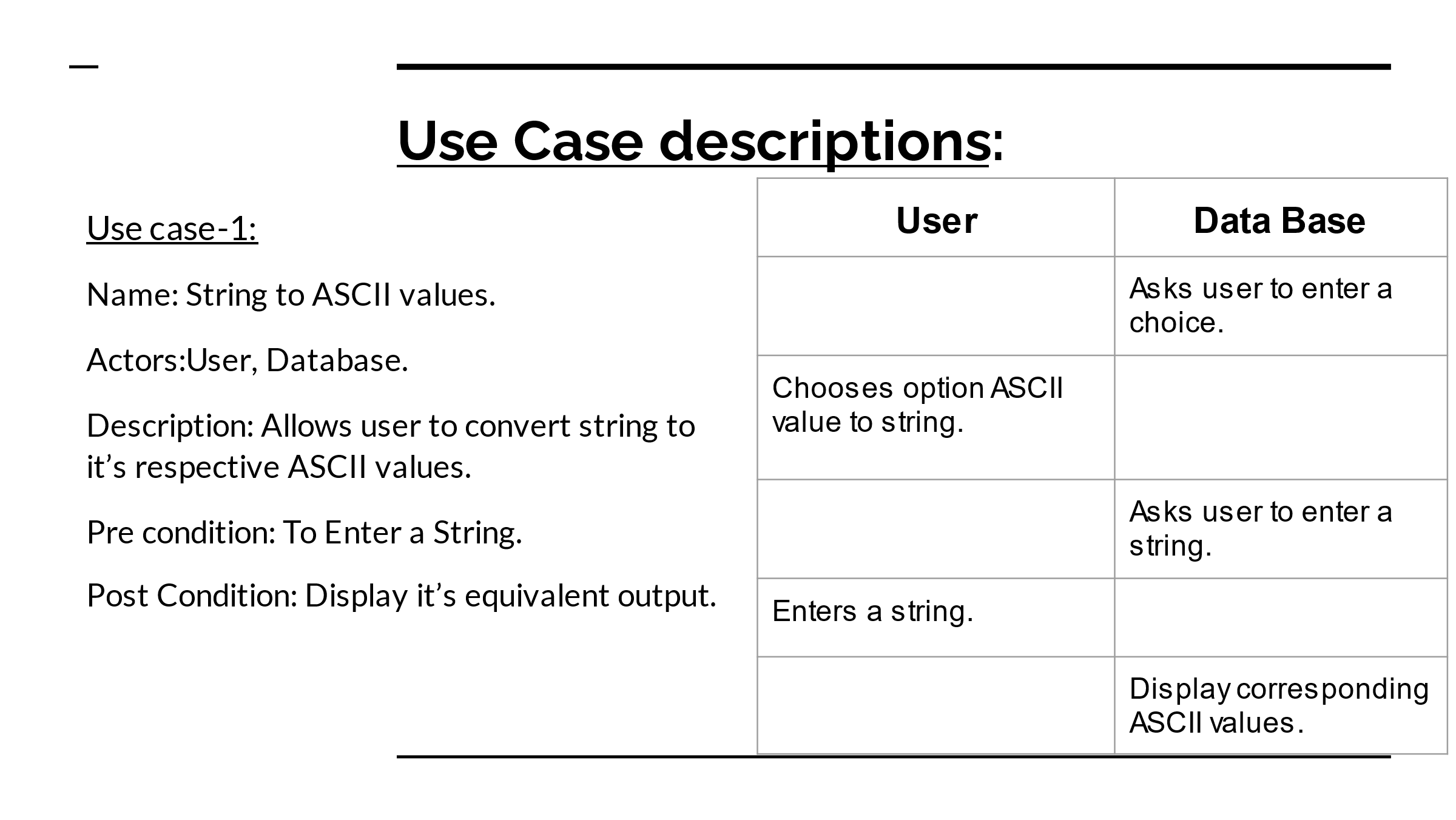
decrypt will raise an exception if it cannot decode token for any reason.

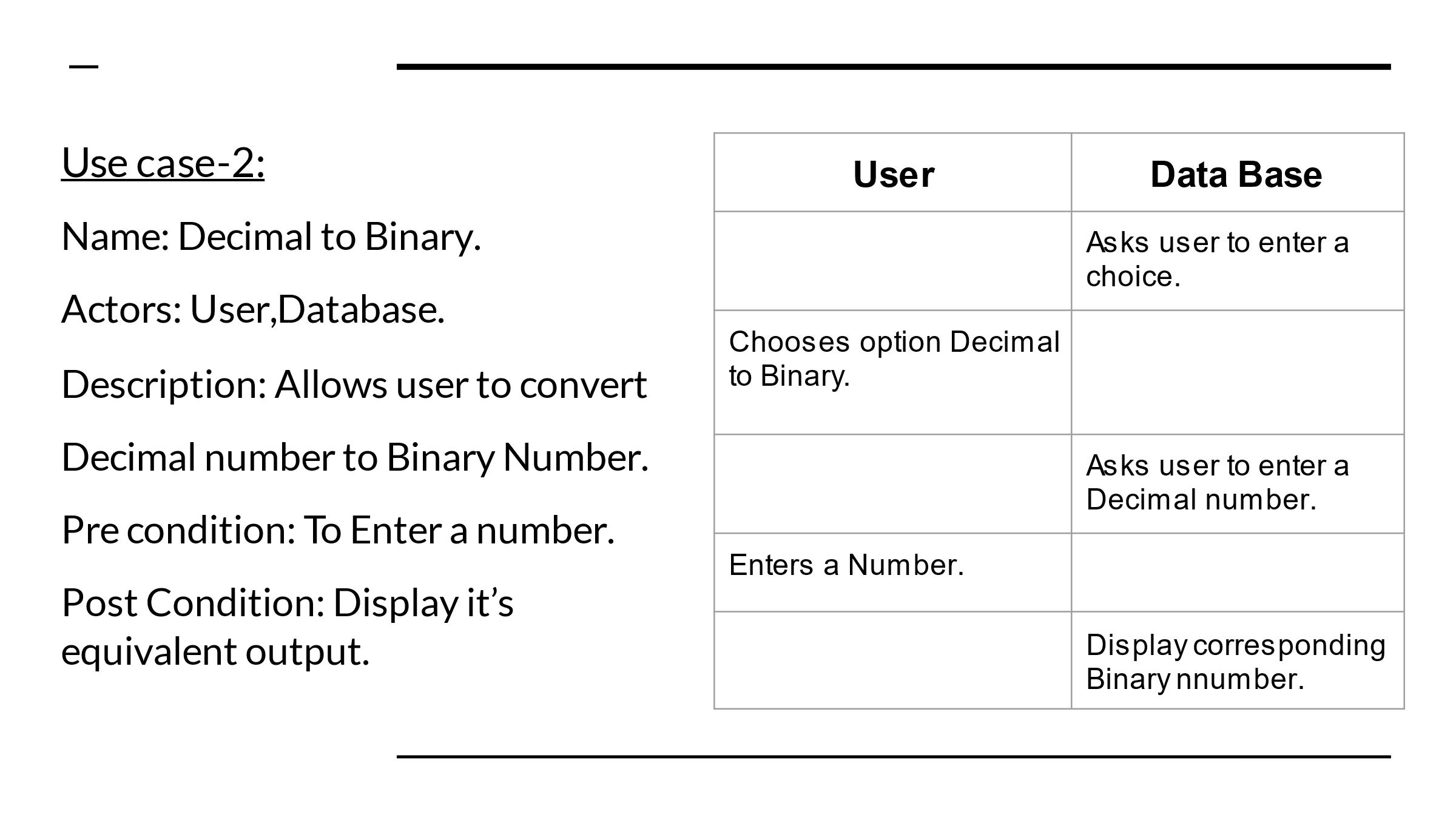
DESIGN

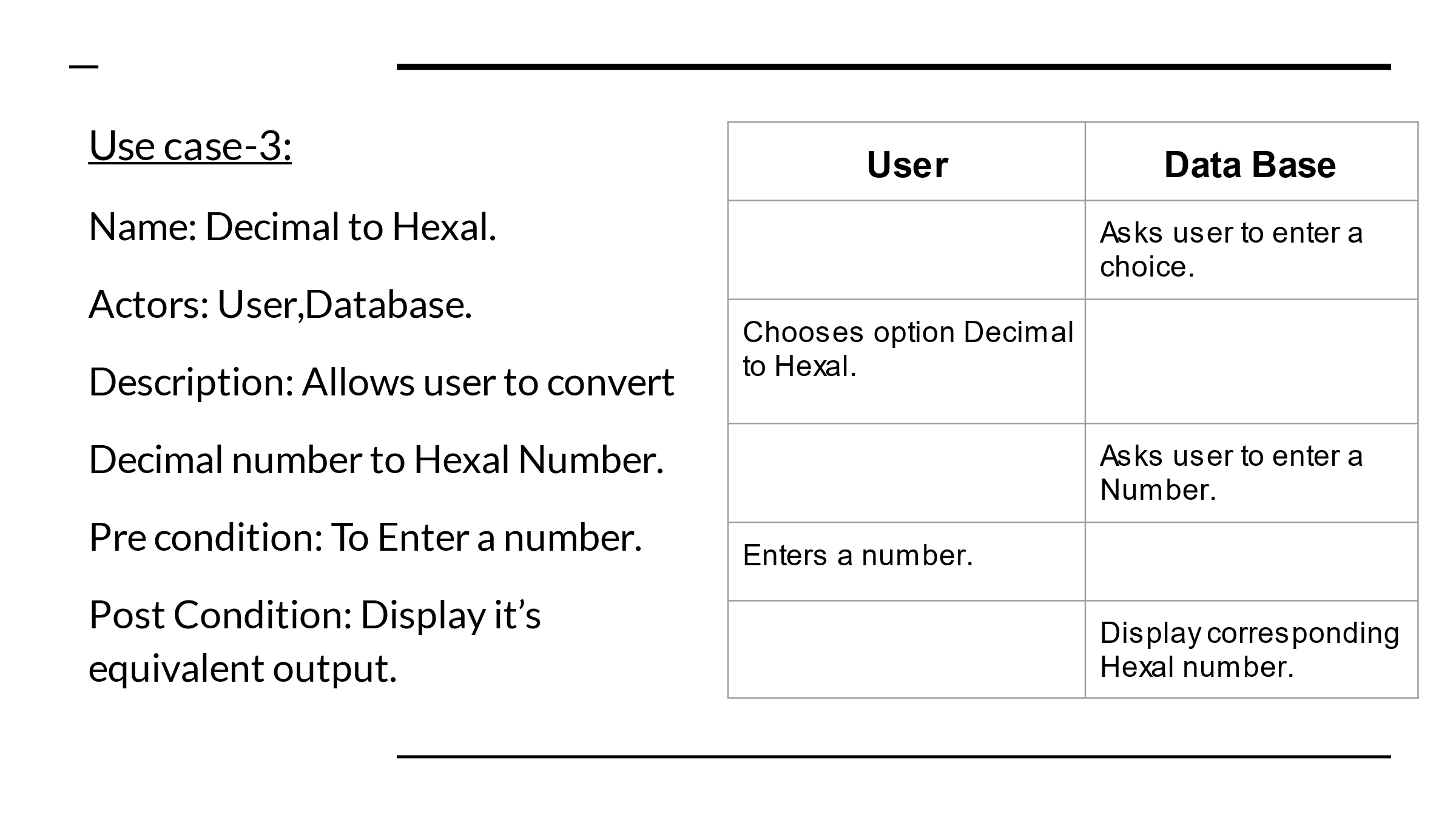


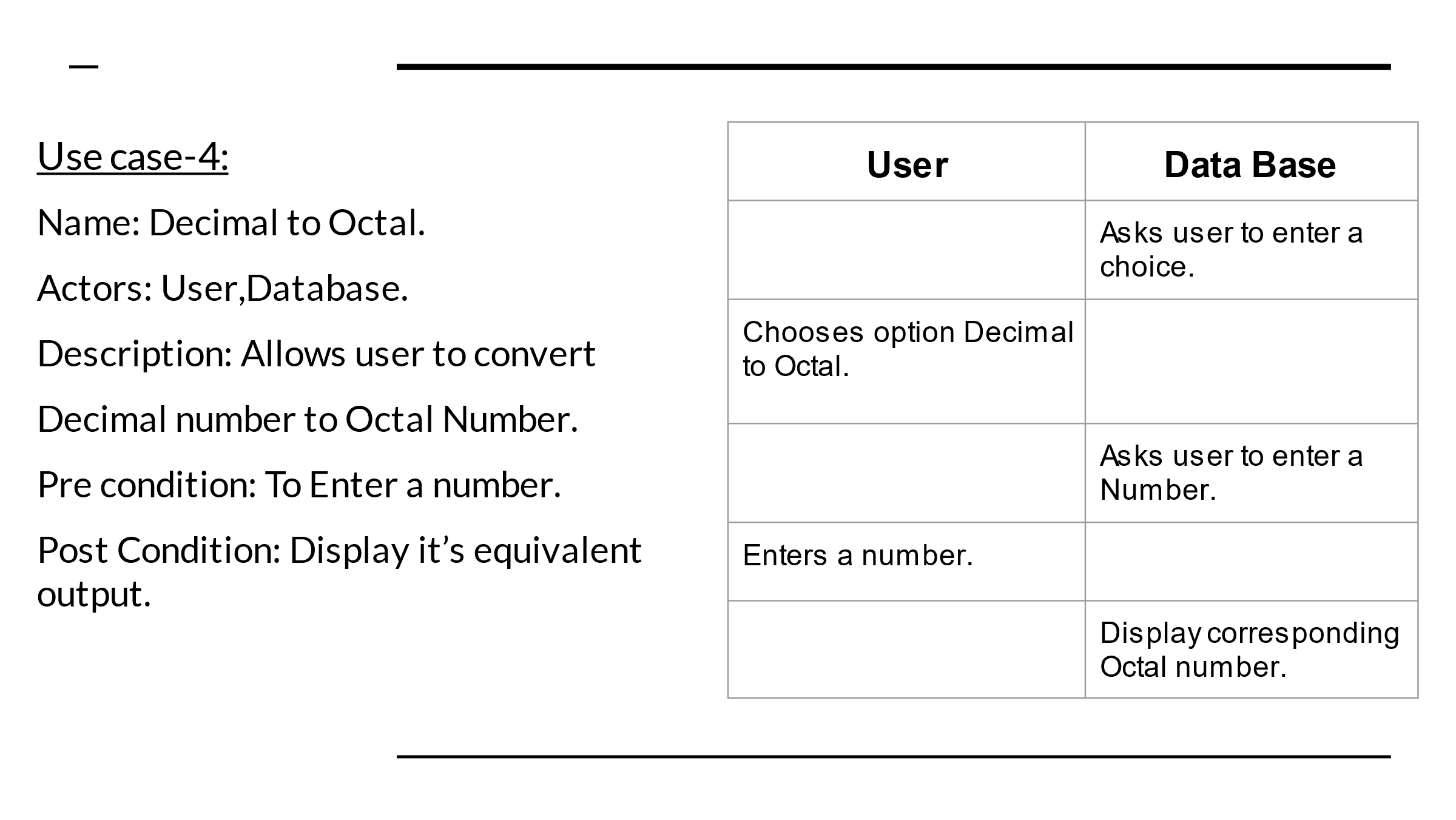
Diagram

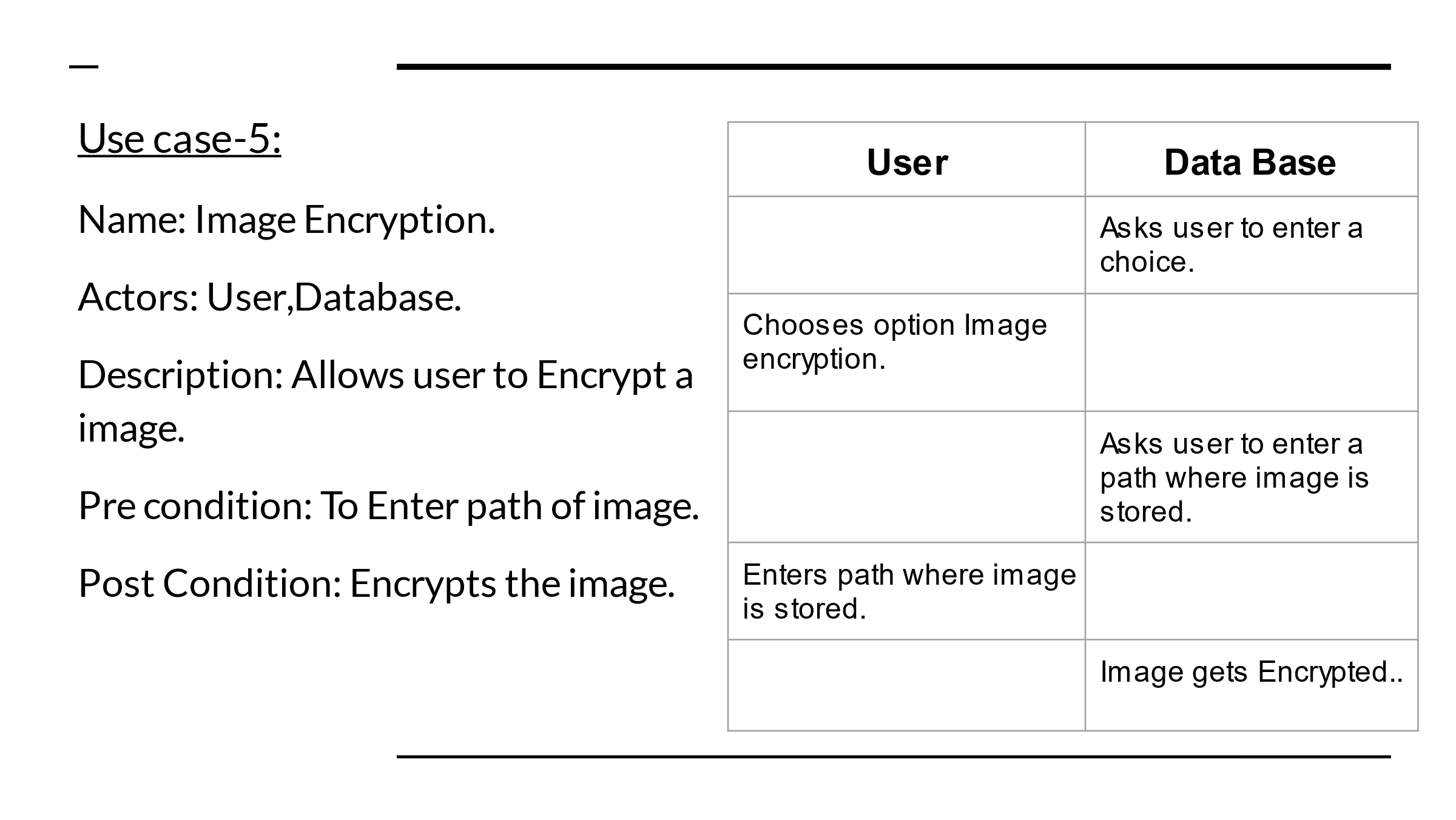
Description automatically generated USECASE DIAGRAM:

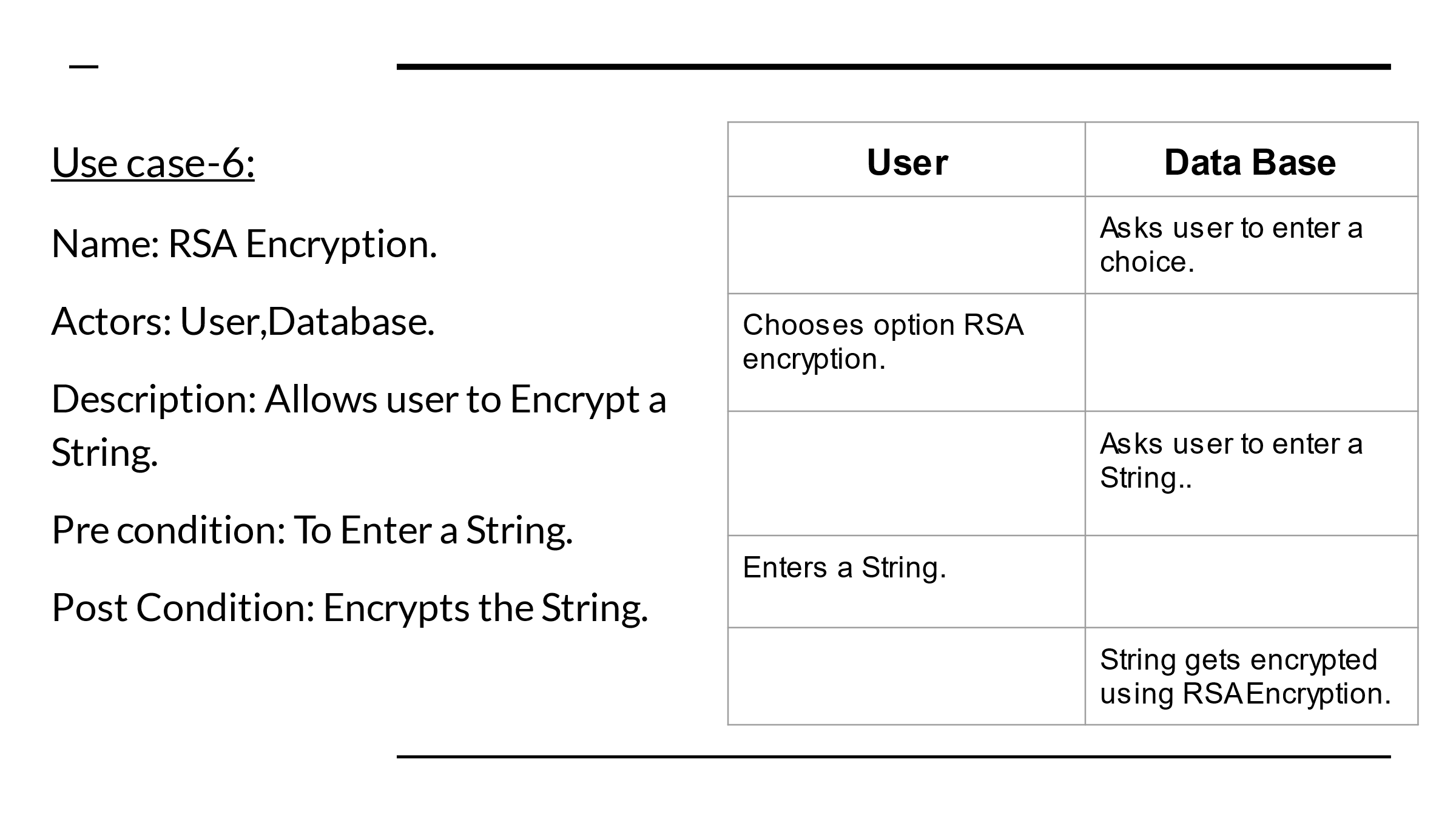












ACTIVITY DIAGRAM

Chart, box and whisker chart

Description automatically generated

IMPLEMENTATION

#install cryptography using the following command in command prompt

#pip install cryptography

from cryptography.fernet import Fernet

#ENCRYPTIONS

#Converstion of string characters to their respective ASCII values

def string\_ascii():

try:

text = input("enter a string to convert into ascii values:")

ascii\_values = []

for character in text:

ascii\_values.append(ord(character))

print("Ascii values characters in string are ",ascii\_values)

except Exception:

print('Error caught : ', Exception.name)

#Converstion of decimal number to a binary number

def decimalToBinary(n):

try:

if(n >= 1):

decimalToBinary(n//2)

print(n%2, end=' ')

except Exception:

print('Error caught : ', Exception.name)

#Converstion of Decimal to a Hexal number

def decimalToHexal(decimal):

try:

conversion\_table = {0: '0', 1: '1', 2: '2', 3: '3', 4: '4',5: '5', 6: '6', 7: '7',8: '8', 9: '9', 10: 'A', 11: 'B', 12: 'C',13: 'D', 14: 'E', 15: 'F'}

hexadecimal = ''

while(decimal > 0):

remainder = decimal % 16

hexadecimal = conversion\_table[remainder] + hexadecimal

decimal = decimal // 16

print(hexadecimal)

except Exception:

print('Error caught : ', Exception.name)

#Converstion of Decimal to octal number

def decimaltoOctal(deciNum):

try:

octalNum = 0

countval = 1

dNo = deciNum

while (deciNum != 0):

remainder = deciNum % 8

octalNum += remainder \* countval

countval = countval \* 10

deciNum //= 8

print(octalNum)

except Exception:

print('Error caught : ', Exception.name)

#Encryption of a Image using XOR operation on byte array of image

def imageEncrypt():

try:

path = input(r"Enter path of Image : ")

key = int(input("Enter Key for encryption of Image : "))

print("The path of file : ", path)

print("Key for encryption : ", key)

fin = open(path, 'rb')

image = fin.read()

fin.close()

image = bytearray(image)

for index, values in enumerate(image):

image[index] = values ^ key

fin = open(path, 'wb')

fin.write(image)

fin.close()

print("Encryption Done...")

except Exception:

print("Error caught : ", Exception.name)

#Encryption of string using symmetric-key encryption generated by using fernat generation of 32 bit key

def stringEncrypt():

try:

message = input("Enter a string:")

key = Fernet.generate\_key()

fernet = Fernet(key)

encMessage = fernet.encrypt(message.encode())

print("Key:",key,"\n")

print("original string: ", message)

print("encrypted string: ", encMessage)

except Exception:

print('Error caught : ', Exception.name)

#DECRYPTIONS #Converstion of ASCII values to its resulting string

def ascii\_string():

try:

i=0

l=[]

while(i!=-1):

i=int(input("Enter ascii value(-1 to end): "))

if(i!=-1):

l.append(i)

res = ""

for val in l:

res = res + chr(val)

print("String is "+res)

except Exception:

print('Error caught : ', Exception.name)

#Converstion of Binary number to a Decimal number

def binaryToDecimal(binary):

try:

binary1 = binary

decimal, i, n = 0, 0, 0

while(binary != 0):

dec = binary % 10

if(dec > 1):

print("Illegal Entry")

return

decimal = decimal + dec \* pow(2, i)

binary = binary//10

i += 1

print(decimal)

except Exception:

print('Error caught : ', Exception.name,"Enter only numbers")

#Converstion of Hexal number to decimal number

def hexalToDecimal(string):

try:

print("Decimal value of the string is",int(string, 16))

except Exception:

print('Error caught : ', Exception.name)

#Converstion of Ocatal number to Decimal number

def octalToDecimal(n):

try:

print(int(n, 8))

except Exception:

print('Error caught : ', Exception.name)

#Decrypting of image using same key used for encryption(Symmetric key/XOR)

def imageDecrypt():

try:

path = input(r'Enter path of Image : ')

key = int(input('Enter Key for encryption of Image : '))

print('The path of file : ', path)

print('Note : Encryption key and Decryption key must be same.')

print('Key for Decryption : ', key)

fin = open(path, 'rb')

image = fin.read()

fin.close()

image = bytearray(image)

for index, values in enumerate(image):

image[index] = values ^ key

fin = open(path, 'wb')

fin.write(image)

fin.close()

print('Decryption Done...')

except Exception:

print('Error caught : ', Exception.name)

#Decryption of String using symmetric-key cryptography generated by using fernat generation of 32 bit key used for encryption

def stringDecrypt():

try:

message = input("Enter Encrypted string: ")

print("meassage: ",message)

encMessage=message.encode()

key = (input("Enter the key generated:")).encode()

fernet = Fernet(key)

decMessage = fernet.decrypt(encMessage).decode()

print("encrypted string: ", encMessage)

print("decrypted string: ", decMessage)

except Exception:

print('Error caught : ', Exception.name)

print("\t\t\t---SECRET COMMUNICATION---")

while True:

print("\tMAIN MENU\n1. Encode.\n2. Decode.\n3. Exit")

ch = int(input("Enter Your Choice: "))

if(ch == 1):

while True:

print("\tEncoding\n1. String to ASCII values\n2. Base Conversions\n3. Image Encryption\n4. String Encryption\n5.Return\n")

ch1 = int(input("Enter your choice: "))

if(ch1==1):

string\_ascii()

elif(ch1==2):

while True:

print("\tBase Convertions\n1. Decimal number to Binary number\n2. Decimal number to Hexal number\n3. Decimal number to Octal number\n4. Return")

ch2 = int(input("Enter your choice: "))

if(ch2 == 1):

num = int(input("Enter a number: "))

print("Binary number is: ",end="")

decimalToBinary(num)

print("\n")

elif(ch2 == 2):

num = int(input("Enter a number: "))

print("Hexal number is: ",end="")

decimalToHexal(num)

elif(ch2 == 3):

num = int(input("Enter a number: "))

print("Octal number is: ",end="")

decimaltoOctal(num)

elif(ch2 == 4):

break

else:

print("Enter a valid choice")

elif(ch1 == 3):

imageEncrypt()

elif(ch1 == 4):

stringEncrypt()

elif(ch1 == 5):

break

else:

print("Enter a valid choice")

elif(ch == 2):

while True:

print("\tDecoding\n1. ASCII values to String\n2. Base Conversions\n3. Image Decryption\n4. String Decryption\n5. Return\n")

ch1 = int(input("Enter your choice: "))

if(ch1 == 1):

ascii\_string()

elif(ch1 == 2):

while True:

print("\tBase Convertions\n1. Binary number to Decimal number\n2. Hexal number to Decimal number\n3. Octal number to Decimal number\n4. Return\n")

ch2 = int(input("Enter your choice:"))

if(ch2 == 1):

num = int(input("Enter a Binary number: "))

print("Decimal number is: ",end="")

binaryToDecimal(num)

elif(ch2 == 2):

num = input("Enter a Hexal number: ")

print("Decimal number is: ",end="")

hexalToDecimal(num)

elif(ch2 == 3):

num = int(input("Enter an Octal number: "))

print("Decimal number is: ",end="")

octalToDecimal(num)

elif(ch2 == 4):

break

else: print("Enter a valid choice")

elif(ch1 == 3):

imageDecrypt()

elif(ch1 == 4):

stringDecrypt()

elif(ch1 == 5):

break

elif(ch == 3):

print("\t\t\t---END OF EXECUTION---")

break

else:

print("Enter a valid choice")

#THE END

Github Link

<https://github.com/SaiSathvik26/Secret-Communication>

TESTING AND RESULTS

Text

Description automatically generatedFirstly after executing the code ,we get a main menu as shown below

Now we have to enter our choice whether to encode or decode or exit.

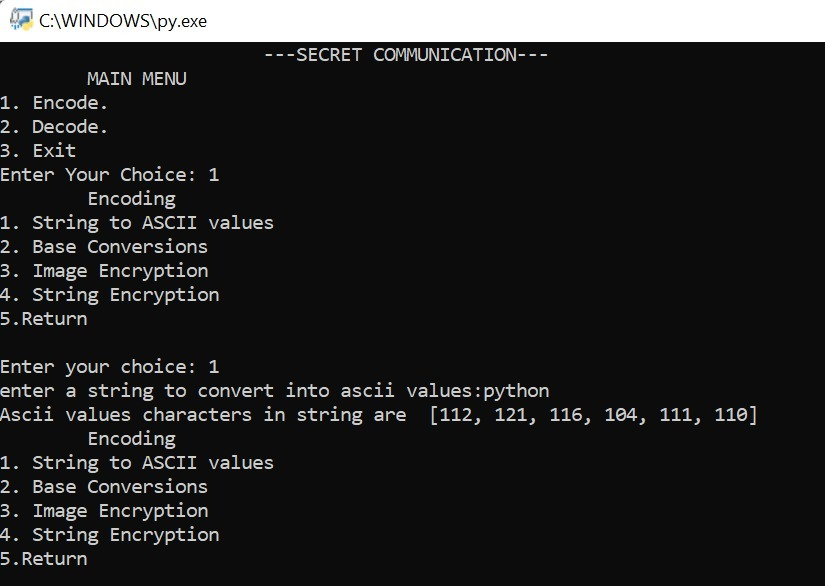
Case-1:

And let us consider that user chose to encode i.e; entered choice as 1.

Now again we are asked to enter the choice as shown below:

Text

Description automatically generatedNow we choose 1 i.e; string to ASCII values then given string is changed into ASCII value:



CASE-2

Let us consider user chose 2 i.e, base conversions ,there are again three choices here :

1.Decimal number to Binary number

2.Decimal number to Hexal number

3.Decimal number to Octal number

According to our choice it is converted as shown below:

Text

Description automatically generated

CASE-3

Now user wants to do image encryption so he can enter his choice as 4 as return to encoding menu then again enter his choice as 3 for image encryption as shown below:

Text

Description automatically generated

Now if we choose 5, control returns to main menu and then if user enter his/her choice as 2 control goes to decoding as shown below:

Text

Description automatically generated

And according to the choice we enter control goes and does the decoding:

Text

Description automatically generated

Graphical user interface, application

Description automatically generatedText

Description automatically generated

Text

Description automatically generated

ADDITIONAL KNOWLEDGE GAINED

\*From this project, we can learn and enter into a new field of communication and can explore new ways to cryptography in additional to the traditional ones.

\*We can also gain the project experience which boosts our speed and skills in the field of management.

\*At the end of the project, an accurate analysis of the project is accomplished in order to improve experience base as needed.

CONCLUSION

\*Finally, our conclusion is that our project can be widely used in sending secret messages in the field of communication.

\* It even helps students in dealing with digital circuits.

\*It can be widely used in the field of cybersecurity also and crime patrols as well.

\*As cybersecurity is the evolving field in present era, “secret communication” can be considered as an vital part of it.

FUTURE SCOPE

\*In future we want to implement it as a data encryptor and decryptor by storing mmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmm all the data in files or any Database.

References

<https://www.pythoninformer.com/python-libraries/cryptography/fernet/>

<https://www.codetd.com/en/article/12570588>