



Data Encryption using DMS and DSP

TEAM - 11



TEAM - 11

SHYAM [21149]

SIDESH [21150]

SABARINATH[21141]

SASANK [21160]

BHARADWAJ[21165]

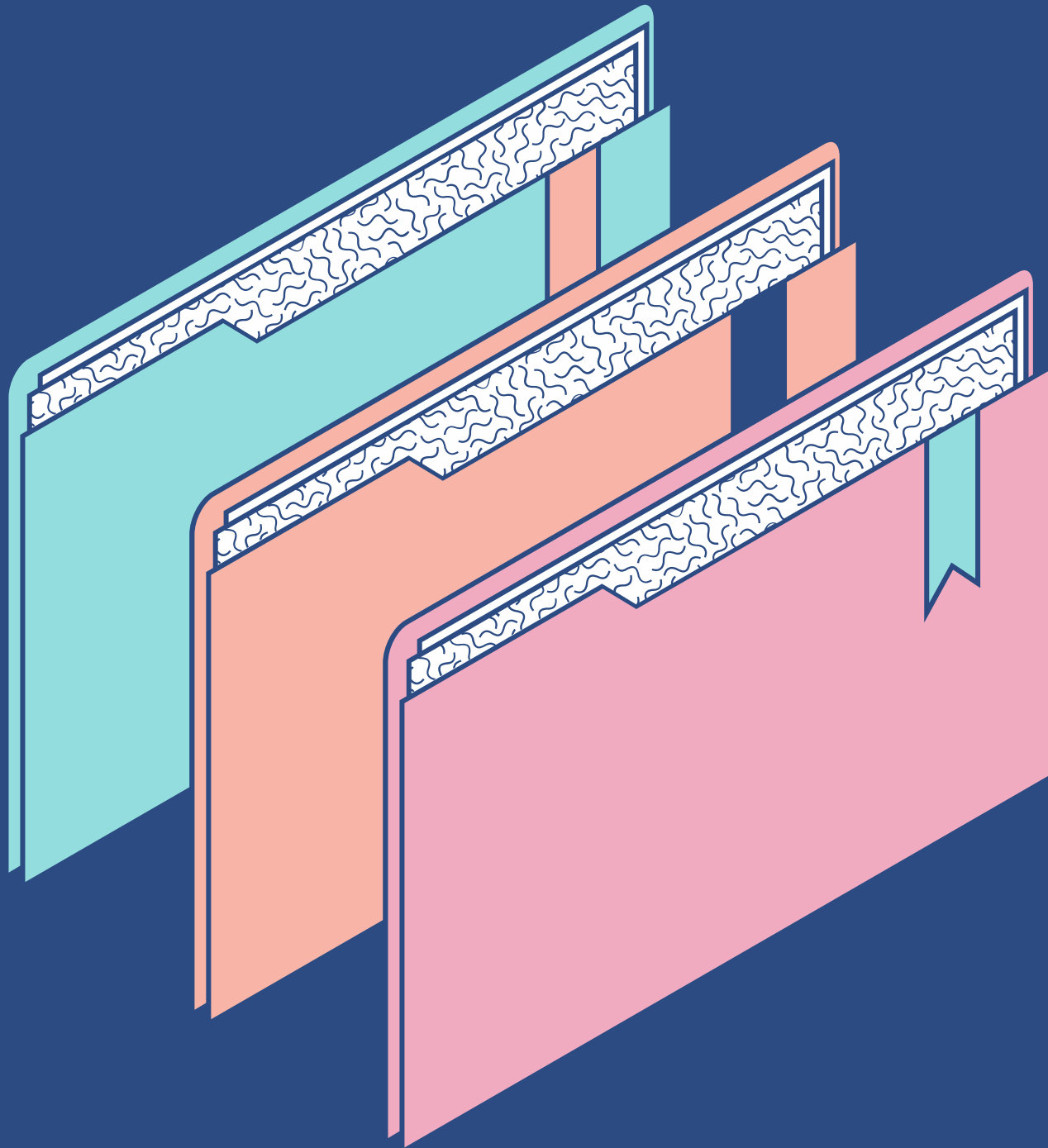
Individual contribution

SABARINATH J	REPORT AND INFORMATION COLLECTION
SHYAM GANESH	CODING
SIDESH SUNDAR	CODING
SASANK SAMI	REPORT AND PPT
BHARADWAJ V	INFORMATION COLLECTION

PROBLEM STATEMENT

OBJECTIVE OF THE PROJECT [AGENDA]

To encrypt the data using the custom AES which is an open source adaptable, strong and secure encryption technique which can stop numerous threats and is extremely reliable to ensure safe data transfer, this can further be extended into message signal transferring via applying Digital Modulation Techniques which ensures unreadable and secured data transfer via signal.





INTRODUCTION

- The daily demands of 60 percent of the world's population include the internet, which is a need in modern living.
- Data security and privacy are issues when using the internet because hackers can use this data.
- We proposed the advance custom configurable algorithm for AES in this project.
- Digital encryption plays a crucial role in today's digital environment in protecting electronic data transfers which then processed by DSP.
- No significant AES attacks have been identified so far.



DEFINITIONS



DMS :

Digital modulation is the process of encoding a digital information signal into the amplitude, phase, or frequency of the transmitted signal.

AES:

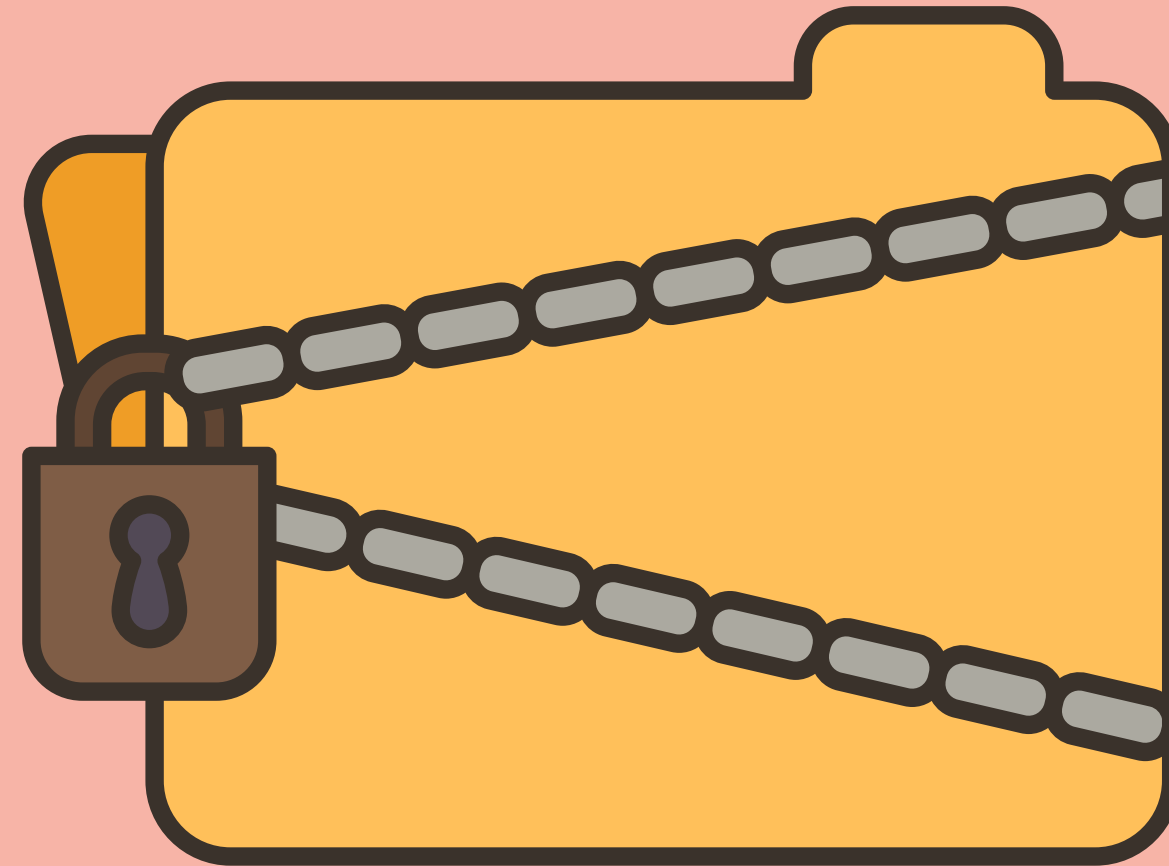
The AES algorithm is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits.

KEY TERMS USED



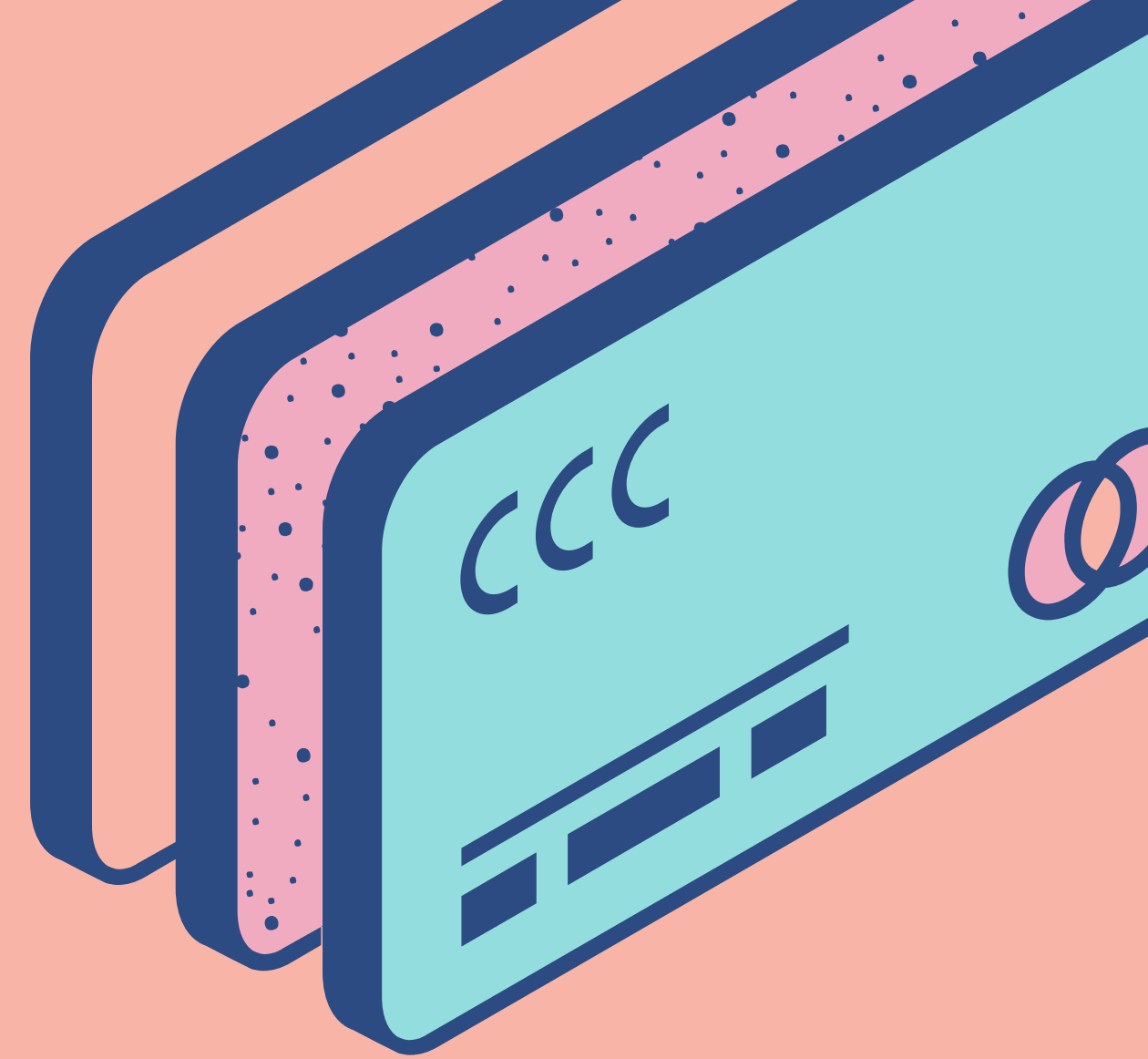
Cipher key

It is used to increase the complexity of the plain text so that it will be more hard for the hacker to crack it



Plain text

The data which is given as input.



Cipher text

The text which we get after mapping text with key.

LITERATURE REVIEW



The shortcomings of DES were addressed by the creation of a new encryption algorithm. Following that, AES was made available on November 26, 2001.

According to B.Nageswara Rao et al. (2017) in their article "Design of Modified AES Algorithm for Data Security," increasing the number of rounds (cycles) from 10 to 16 makes the algorithm (AES) more secure.

Ako Muhammad Abdullah used keys that were 128 bits, 192 bits, and 256 bits in block cipher to implement 10 rounds of AES encryption in their 2017 paper titled "AES Algorithm to Encrypt and Decrypt Data." His investigation reveals that AES is more secure than rival algorithms like DES and 3DES.

In the article it is mentioned that " AES Encryption: Study & Evaluation ", Ahamd-Loay Sousi (2020) AES is the most strong secure protocol and is applied in both hardware and software , it uses key size of greater length for encryption, such as 128,192 and 256 bits so it is more resistant to hacking since around 2^{128} attempts are required for just 128 bits to break and this makes it very difficult to hack it since it is a very secure protocol.

METHODOLOGY

1

2

3

4

5

STEP

STEP

STEP

STEP

STEP

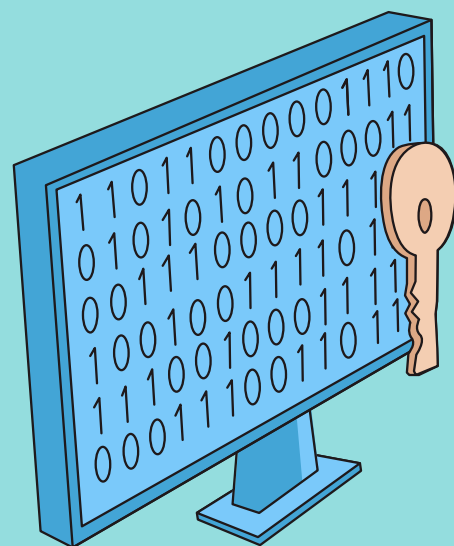
Select the key
standard

Give input and
cipher key

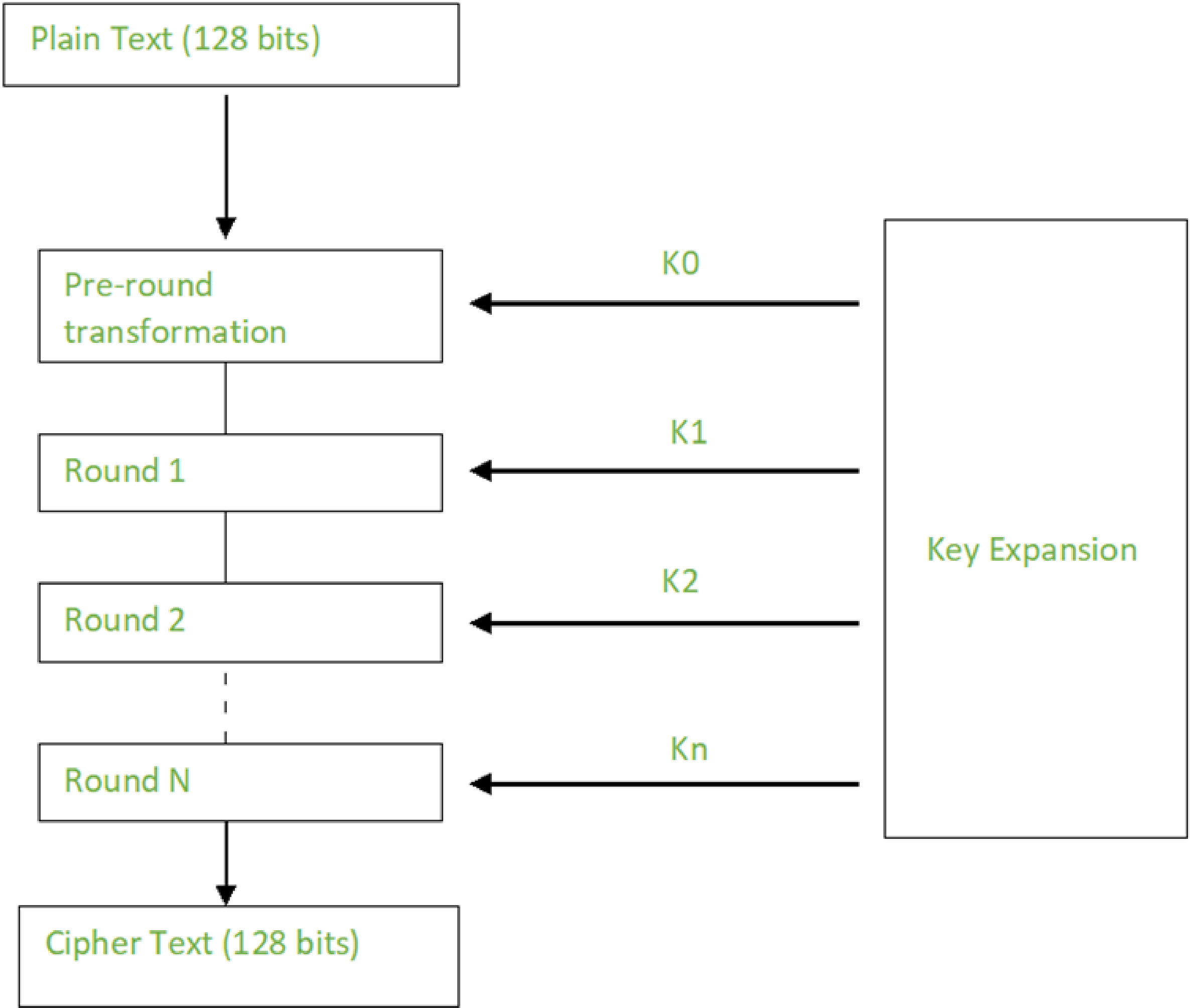
Converting the
text and
cipherkey to
integer array

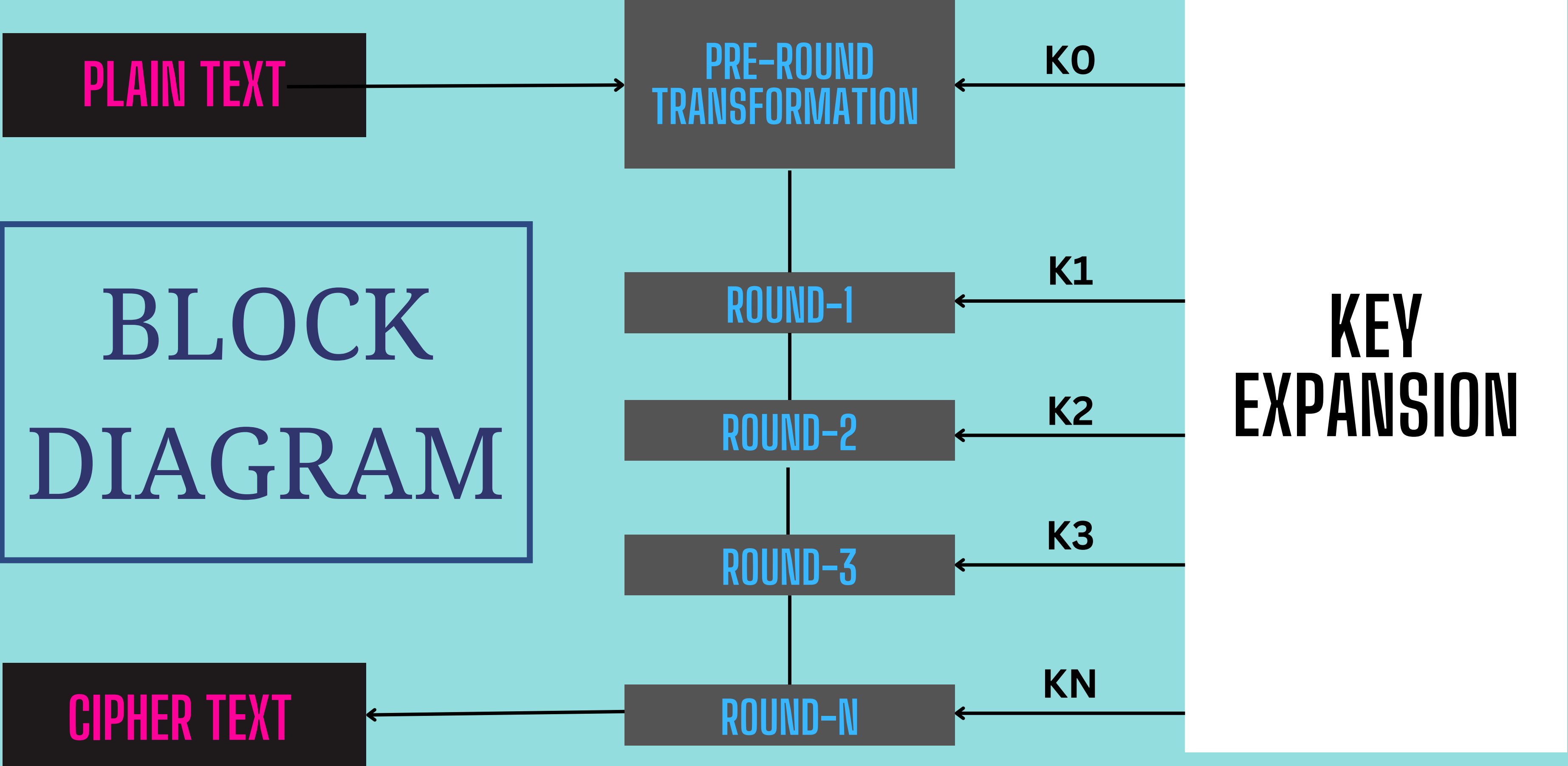
Encrypt the data

Decrypt the
encrypted to get the
complete string and
now generate the
graph



BLOCK DIAGRAM



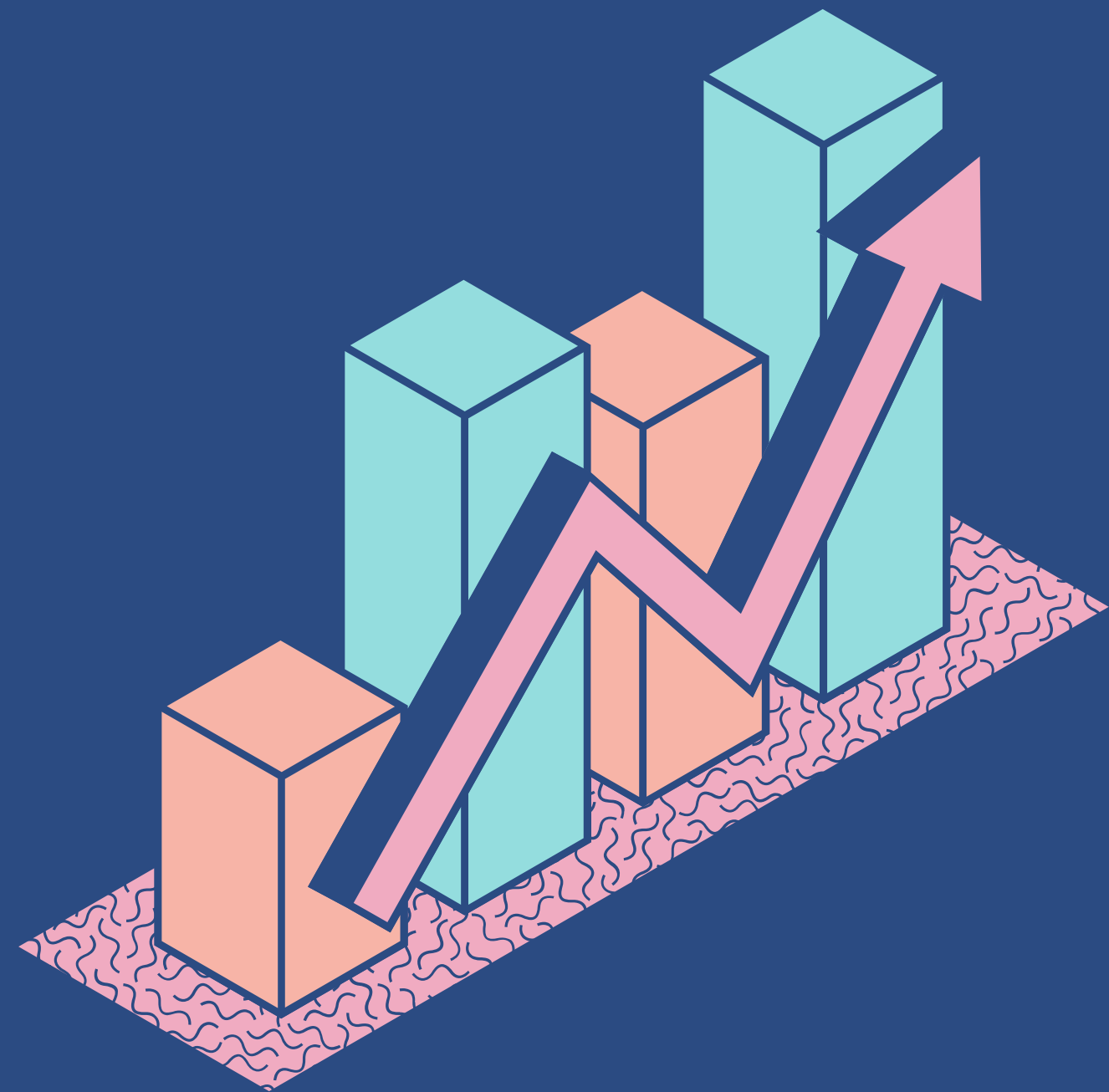


RESULT

```
cipherText = 4x4 int16 matrix
```

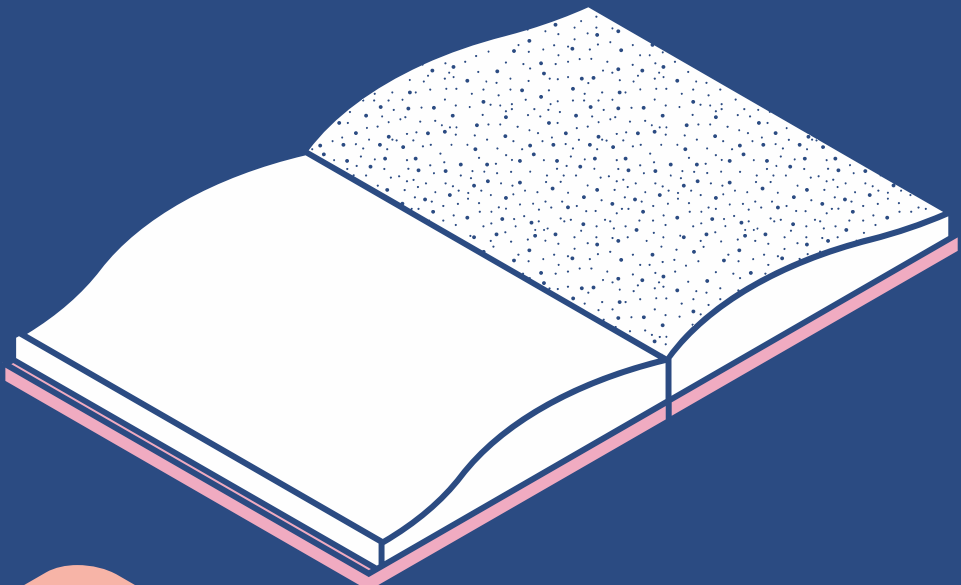
201	47	121	116
172	10	27	58
117	110	180	154
50	231	96	252

```
Decryption successful!  
Plain text: sasank
```

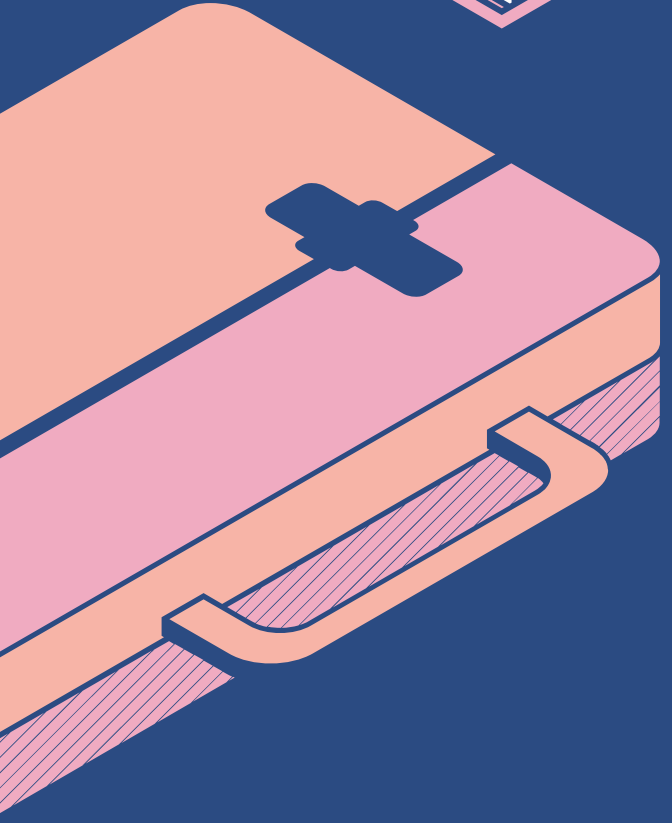




Conclusion



The core of the work is the extended AES algorithm with custom configuration, a novel concept. The method employs AES and includes certain system-customizable phases.



It is common knowledge that the world is shifting more and more toward digital systems, and everywhere has generally good internet accessibility. The AES configuration is widely used to convey classified messages. For such governments as well as other organizations, this technology offers an extra layer of safety that is completely hidden from everyone, including the user. It cannot theoretically be broken without assistance from within.

Reference

Click the Share button on the top right corner of your screen and select 'Present and Record.'

Click 'Go to recording studio,' where you can choose the video and audio source for your video presentation.

Once you're done, download your Canva Presentation in MP4 file format or get a link to your Talking Presentation and share it with others.

You can also record a video inside the editor! Go to 'Uploads' and click on 'Record yourself'.



THANK YOU