CIPHERGUARD

"SECURE EVERY WORD, PROTECT EVERY THOUGHT."

WWW.CIPHERGUARD.COM

TUNIS BUSINESS SCHOOL

OUTLINE

1. INTRODUCTION
2. WHAT IS CIPHERGUARD?
3. HOW THIS WORKS?
4. ADDED-VALUE?

WWW.CIPHERGUARD.COM

INTRODUCTION

80% & more of data breaches involve compromised credentials or plaintext data. That’s why, encryption is crucial for transforming sensitive information into secure, unreadable formats. Algorithms like AES, RSA, and ECC ensure this by implementing robust encryption methods. This is essential for maintaining data security in today’s interconnected world.

WHAT IS CIPHERGUARD?

A web-app that allows users to encrypt and decrypt text messages using well-known and very secure cryptographic algorithms like **AES**, **RSA**, and **ECC**.

The system takes user input, applies the selected encryption algorithm, and return the encrypted output. It will also allow decryption using the appropriate key.

WWW.CIPHERGUARD.COM

SECURE & STATE-OF-ART ALGORITHMS WE RELY ON!

AES

Symmetric encryption algorithm. It encrypts data in blocks.

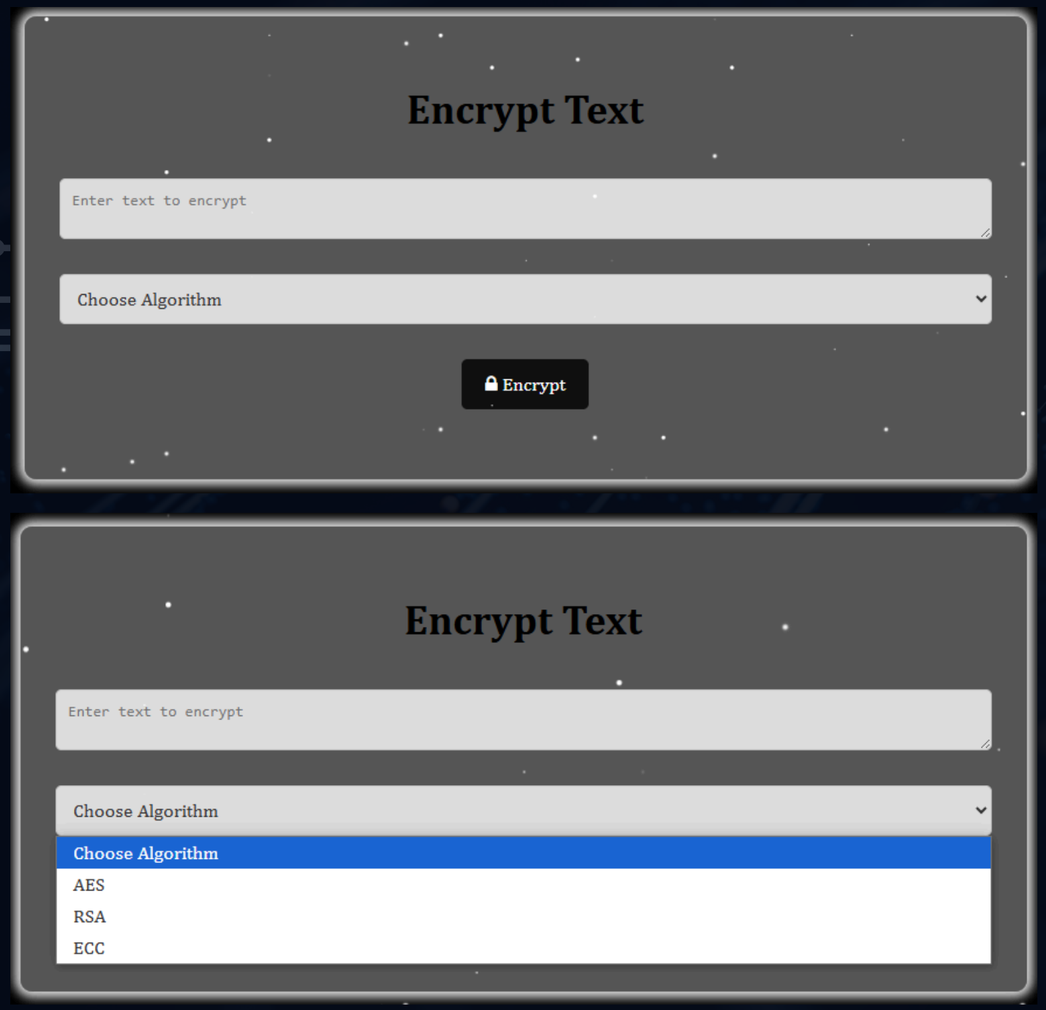
RSA

Asymmetric encryption algorithm. It uses two keys (public & private).

ECC

Asymmetric encryption algorithm. It uses two keys (public & private) for key exchange.

HOW THIS WORKS?

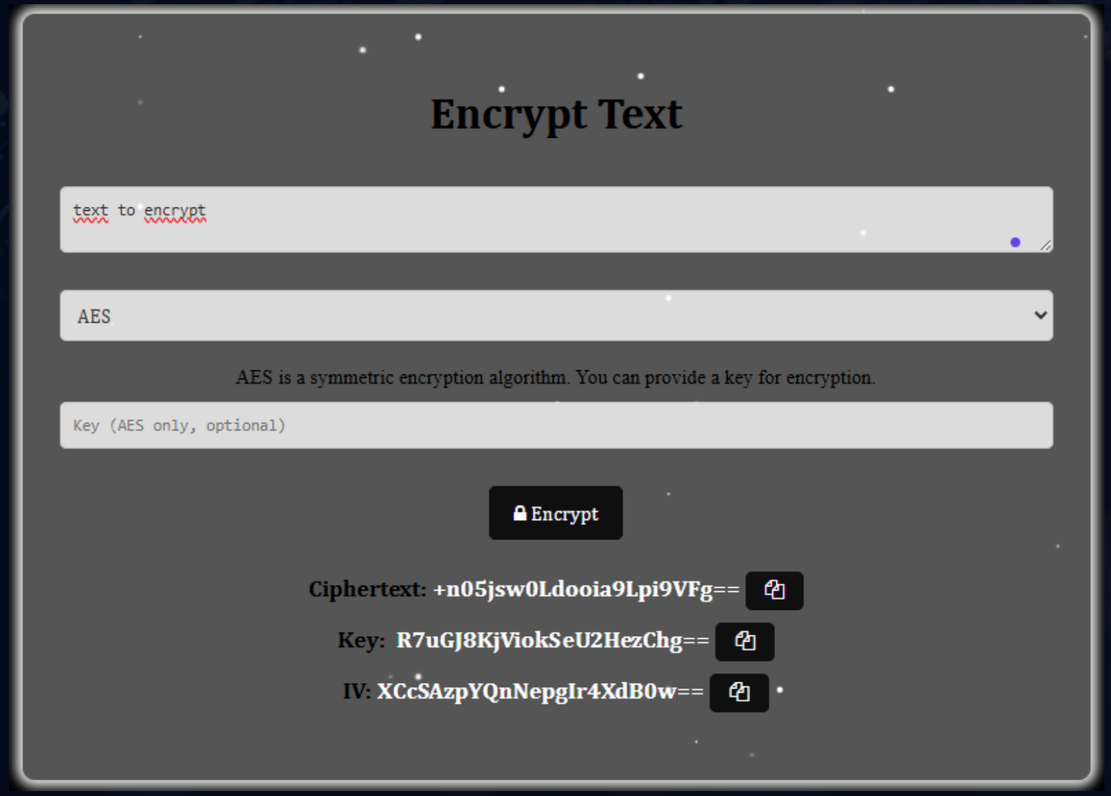


ENCRYPTION PHASE

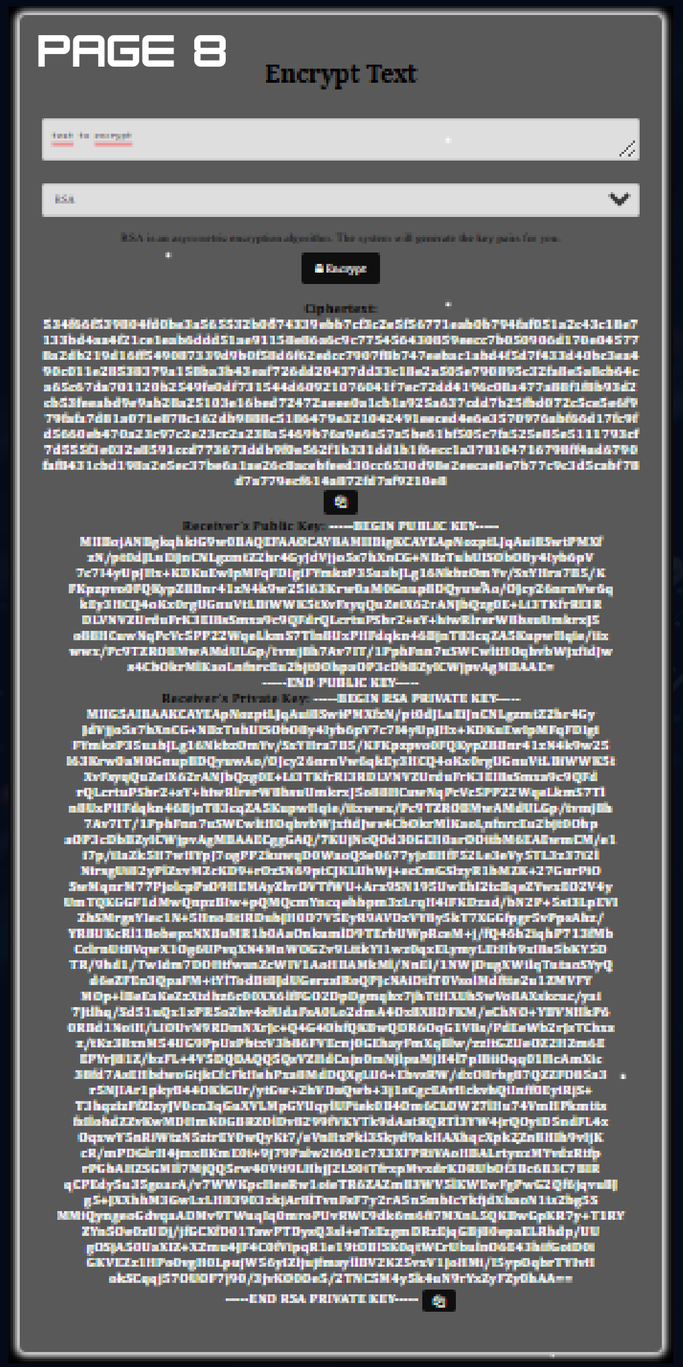
The user enters a text message to encrypt.
Then he selects a cryptographic algorithm between **AES, RSA** and **ECC**.

HOW THIS WORKS?

If he chooses the **AES** algorithm: The user has the option to input himself the key or to let the system generate it for him automatically.



WWW.CIPHERGUARD.COM



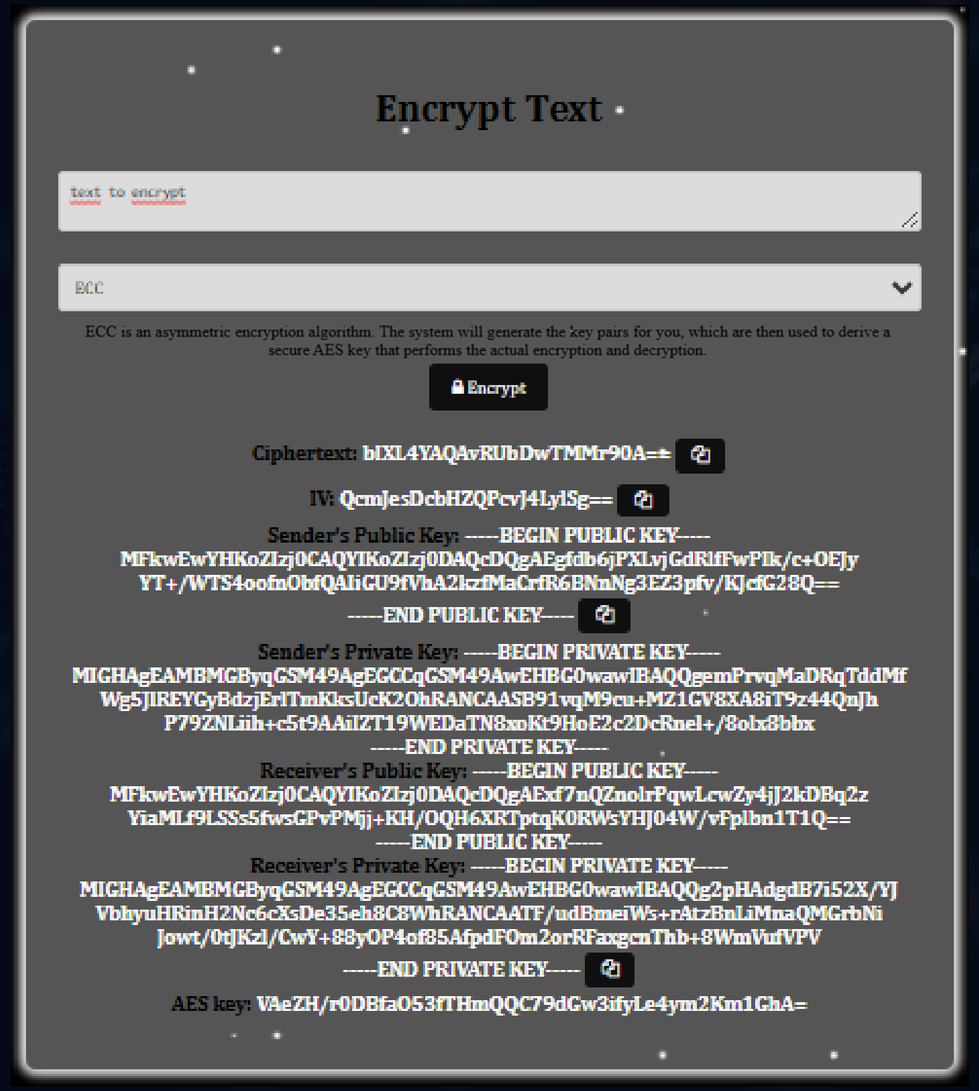
HOW THIS WORKS?

If he chooses the **RSA** algorithm:
The system will automatically generate all the public & private key pairs for the user.
The encryption is done using the autogenerated Receiver's public key.

WWW.CIPHERGUARD.COM

TUNIS BUSINESS SCHOOL

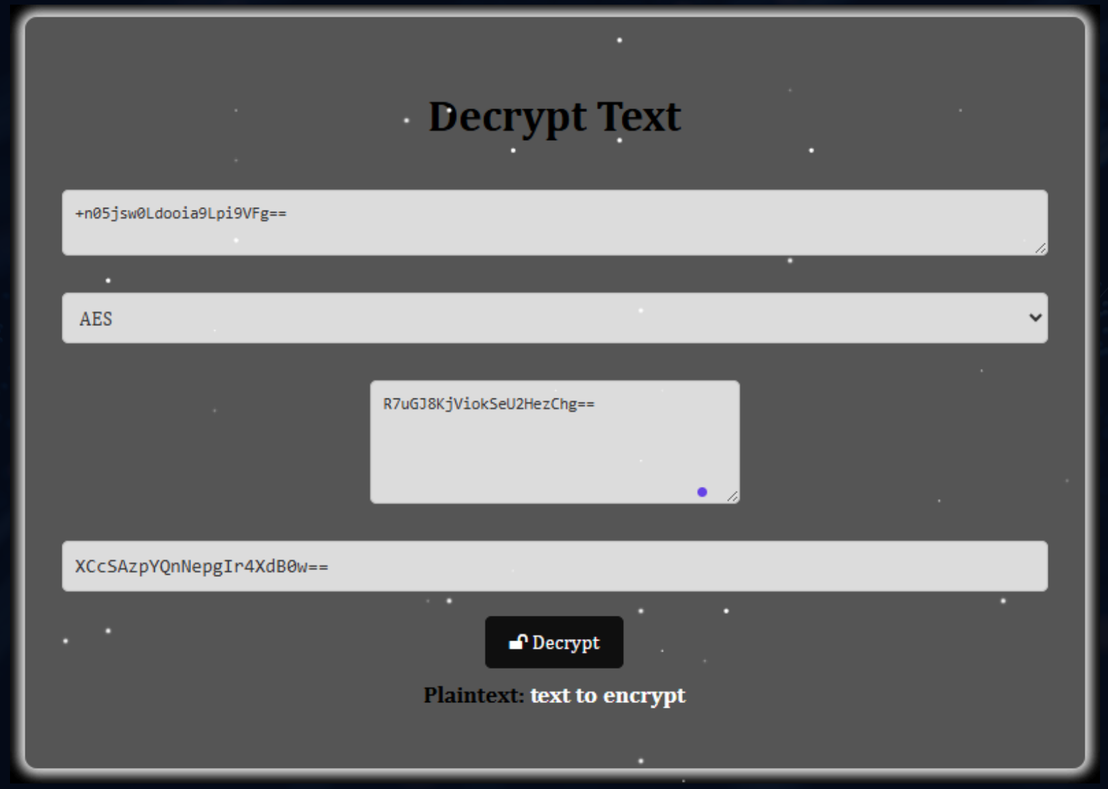
HOW THIS WORKS?



If he chooses the **ECC** algorithm: The system will automatically generate all the public & private key pairs. It will also display for the user the generated IV and derived AES key.

HOW THIS WORKS?

DECRYPTION PHASE

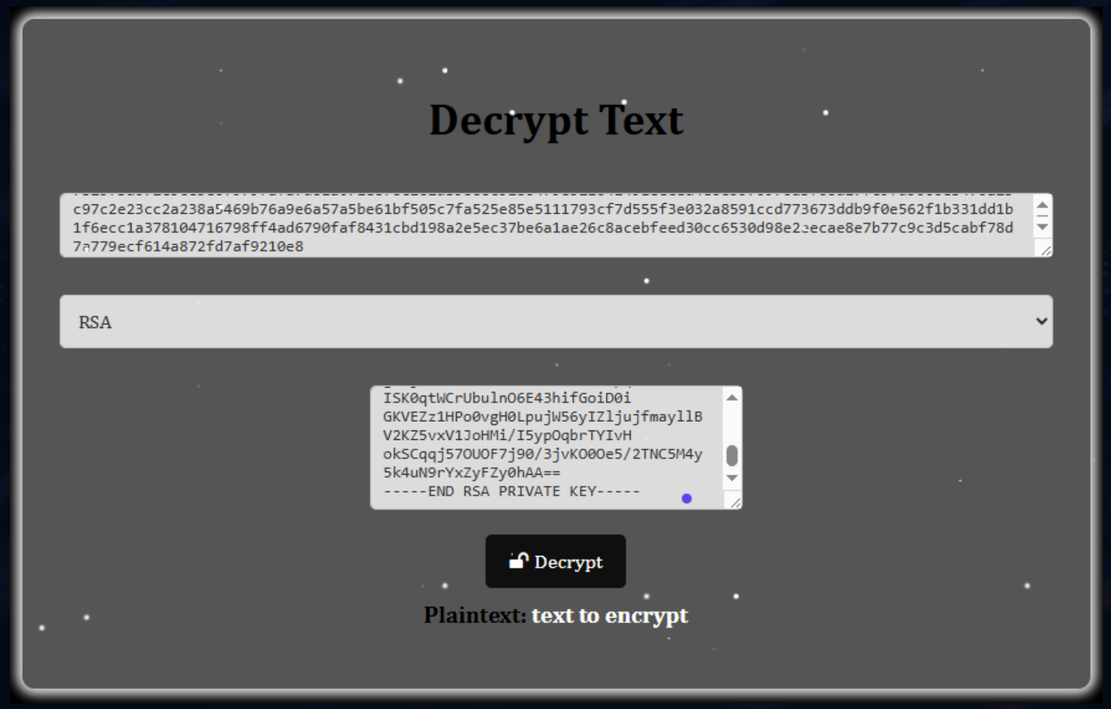


AES: The user receives a ciphertext, enters the inputted or autogenerated symmetric key along with the IV generated by the system to decrypt the cipher.

WWW.CIPHERGUARD.COM

HOW THIS WORKS?

DECRYPTION PHASE

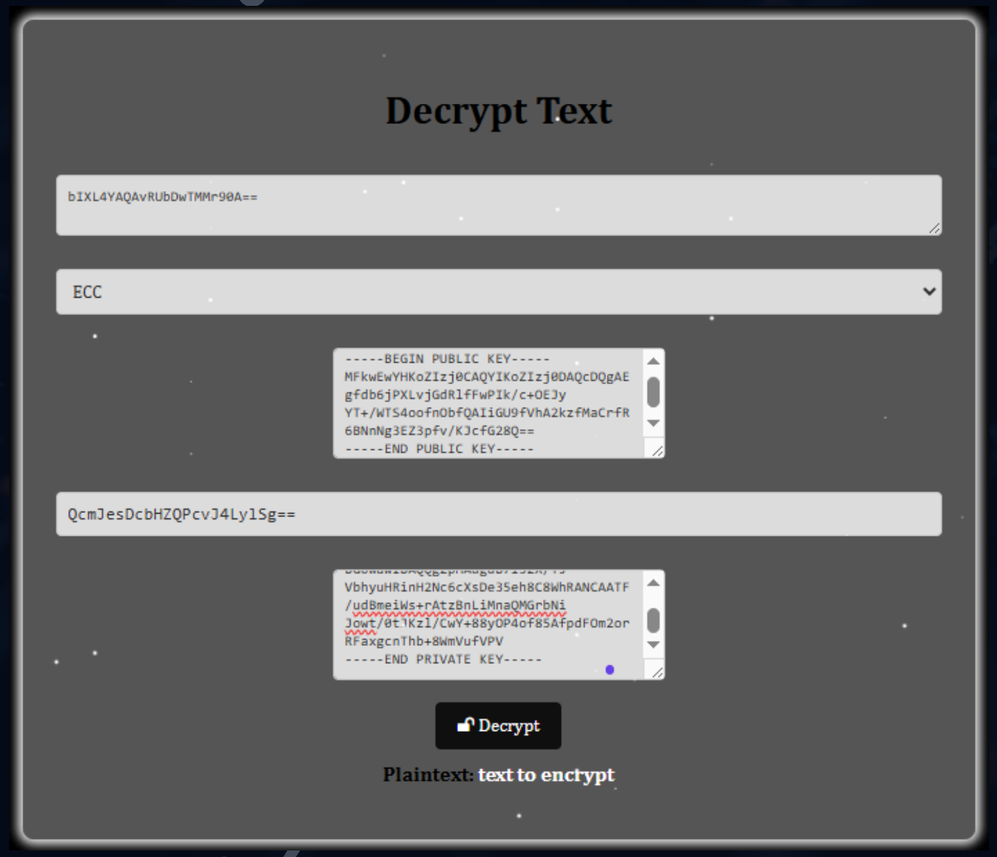


RSA: Upon receiving the ciphertext, the user enters it along with the autogenerated Receiver's private key to be able to decrypt it and get the original plaintext.

WWW.CIPHERGUARD.COM

HOW THIS WORKS?

DECRYPTION PHASE



ECC: The user will have to enter the obtained ciphertext, along with the autogenerated sender's public key + Receiver's private key (which will be used to retrieve the AES key in the backend), as well as the autogenerated IV so as to decrypt the text

CIPHERTEXT ADDED-VALUE?

MULTI-ALGORITHM SUPPORT

USER-FRIENDLY INTERFACE

WWW.CIPHERGUARD.COM

MEET THE TEAM

AHMED MNAOUER

ROUA ABASSI

WWW.CIPHERGUARD.COM

THANK YOU !

WWW.CIPHERGUARD.COM