

# CIPHER GUARD

"SECURE EVERY WORD, PROTECT  
EVERY THOUGHT."

SEARCH [WWW.CIPHERGUARD.COM](http://WWW.CIPHERGUARD.COM) SPEECH



# OUTLINE

1. INTRODUCTION

2. WHAT IS CIPHERGUARD?

3. HOW THIS WORKS?

4. ADDED-VALUE?



# 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.



# 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?

Encrypt Text

Enter text to encrypt

Choose Algorithm

Encrypt Text

Enter text to encrypt

Choose Algorithm

Choose Algorithm

- AES
- RSA
- ECC

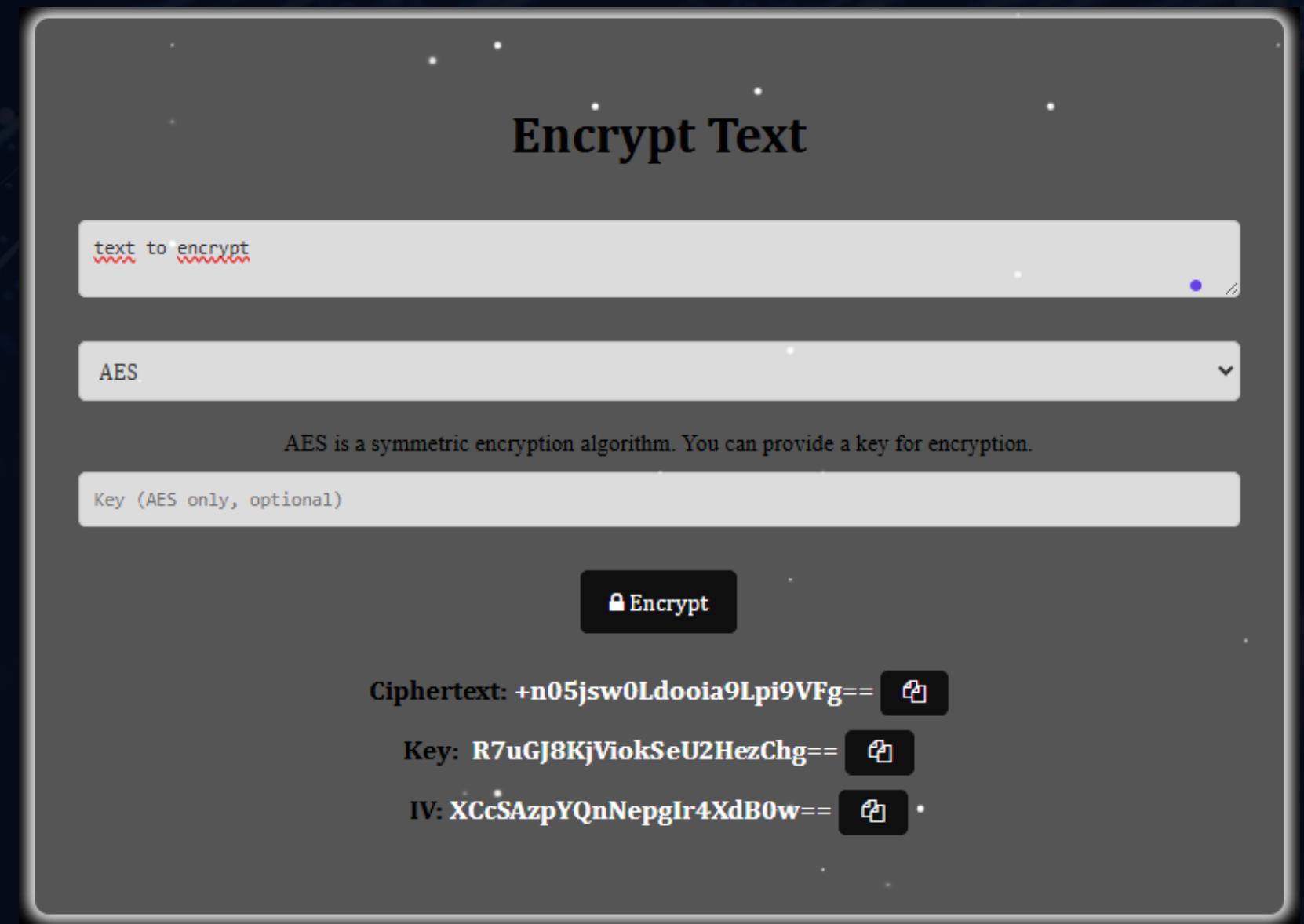
## ENCRYPTION PHASE

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.



task to encrypt

**RSA**

RSA is an asymmetric encryption algorithm. The system will generate the key pairs for you.

**Encrypt**

**Ciphertext:**

```
534884539904400ba3e565532b0574339ab7c3fc2e5f56771ab9b7946fb051a2c43c18e7
113bd4ca4f21ce1abadd51ae91150ea63ac9c7734526430039eacc7b6050906d170e4577
ba2fb219d16e54900733369b0f50d6f62adcc7907fb9747eabca1abdc4f5d71433d40bc3aa4
9e8011e2e0530379a158ba3b43ee726d20437dd3c1le82e2505e790095732h1e5a8cb64c
a65c87d8701120b2549fe0d731544de80921076041f7ec72dd4198e0ba477e88f1f1b6b03d2
cb53feefbd8e9ab2ba25103e16bed724772aee8a1cb1a825a837odd7b25fb0d72c5e5e4ff9
79bfba7d81a071e071fc162db98880c5104479e0210424791eacc4ed4e1570976abf66d17fc9f
d5080ab4708023c97c2e23cc2a231a54899b763e9e8a575a1be81bf505c7fa525e05a5111793cf
7d55500e092a8591ccdf7736e73d6b980e54211b331dd1b1f8ecc1a07104716790ff4ad8790
fa8431chd198a2e5ec37ba61aa26claccabed30cc630d9162eaccalle7b77fc9c1d5cabf78
d7a779ac814ad872fd7af9210ad
```

**Receiver's Public Key: -----BEGIN PUBLIC KEY-----**

```
MIGfMA0GCSqGSIb3DQEAYAAQJQDPAHQACAYBAMHIBigKCAYEApNospfHljqAxI0SwiPMODf
zN/gpDdJLx0DjJnCNlypmkZ22hr4GyjdV)ja5x7hx0nCG+NReTahtU5O6b0lly4lyb6pV
7e714yUpjHx+KDKuEwlpMPqRDIgjUTYnkaP3SueabJlg16XkhOsOmYv/SxTlira7BS/K
PKpwpvxFQKyp2800er41zN4k9w25163JKrvaBaM8Gaujp0DQyuwAa/OJcy28ernVn
k3y3ICQ4e0KxDr9UGnaaVLLBIWWfCSDXrFayqQaZeD62rANjbQng0E+LJ3TfKfr803E
DUNVY2UrdePrKEJElleSmcaqyngdrLcraPsbr2+eY+hhwRirerWlhewUmkrksZ
s08001ConeNgFcYcPP22WqoLkm577linuXPHfjkn448jgjT03cqZASRgpaNgla/0z
www;|Pc9TzR08MwAMdULGp/tnm/jba7Ar7IT/1Pphfam7a5WQwthDqJrbwWjxhid]w
x4Cb0krMKaoLafrcrc2bja001kpaDP3cDb6B2yICW)pvAgMBAAE=
```

**-----END PUBLIC KEY-----**

**Receiver's Private Key: -----BEGIN RSA PRIVATE KEY-----**

```
MIGfMA0GCSqGSIb3DQEAYAAQJQDp9pHljqAxI0SwiPMODf2284r4Cy
jdV)ja5x7hx0nCG+NReTahtU5O6b0lly4lyUpjHx7e714yUpjHx+KDKuEwlpMPqRDIgj
P7mkaP35wabJlg16XkhOsOmYv/SxTlira7BS/KPKpwpvxFQKyp2800er41zN4k9w25
M3JKrvaBaM8Gaujp0DQyuwAa/OJcy28ernVn
k3y3ICQ4e0KxDr9UGnaaVLLBIWWfCSDXrFayqQaZeD62rANjbQng0E+LJ3TfKfr803E
XrFayqQaZeIX62rANjbQng0E+LJ3TfKfr803Q0LVNY2UrdePrKEJElleSmcaqyngdr
rQlcrtaPsbr2+eY+hhwRirerWlhewUmkrksZs08001ConeNgFcYcPP22WqoLkm5771
nfDUxPHfjkn448jgjT03cqZASRgpaNgla/0zwww;|Pc9TzR08MwAMdULGp/tnm/jba
7Ar7IT/1Pphfam7a5WQwthDqJrbwWjxhid]w4Cb0krMKaoLafrcrc2bja001kpaDP3cDb6B2yICW)pvAgMBAAE=
```

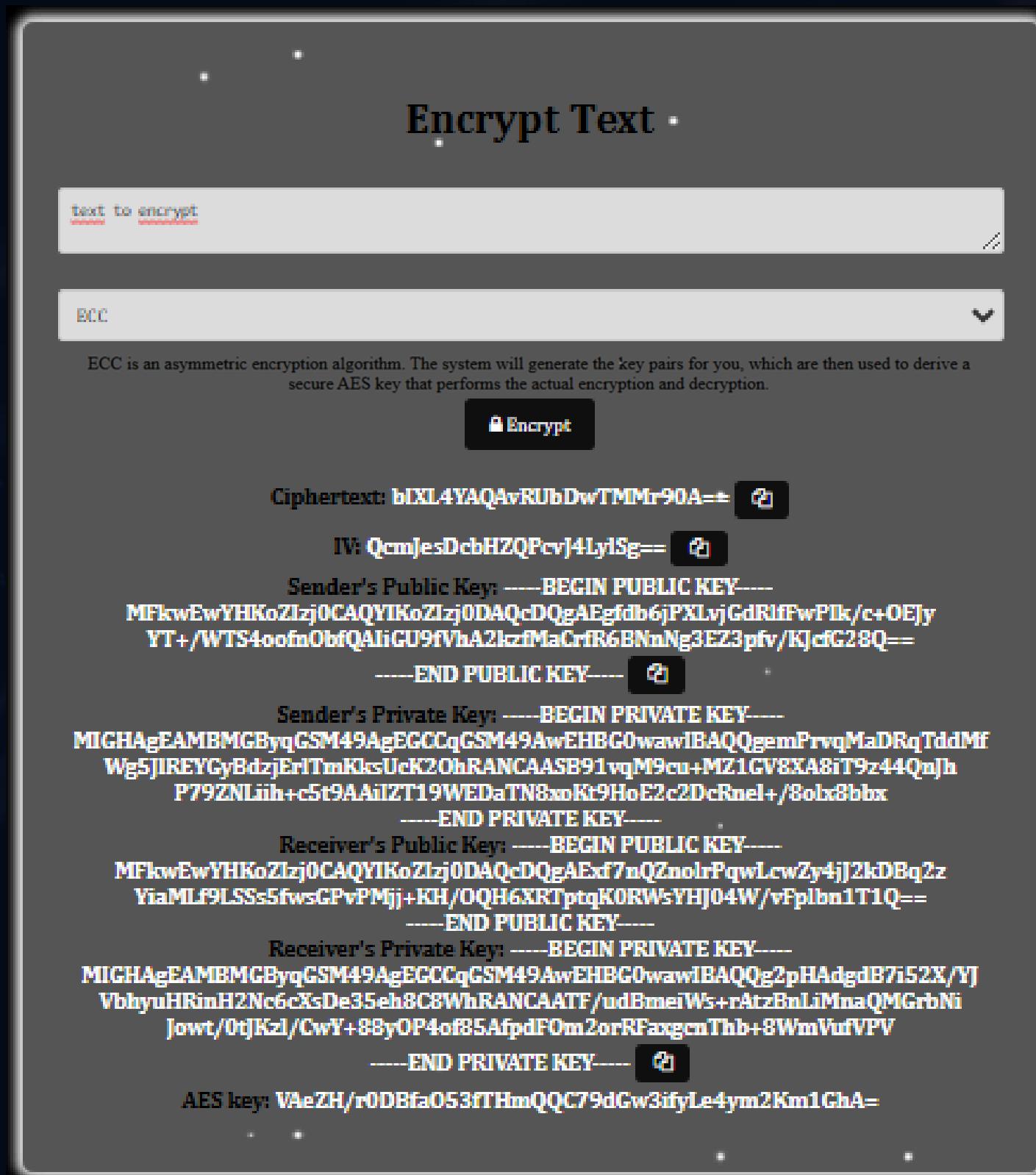
**-----END RSA PRIVATE KEY-----**

# 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.



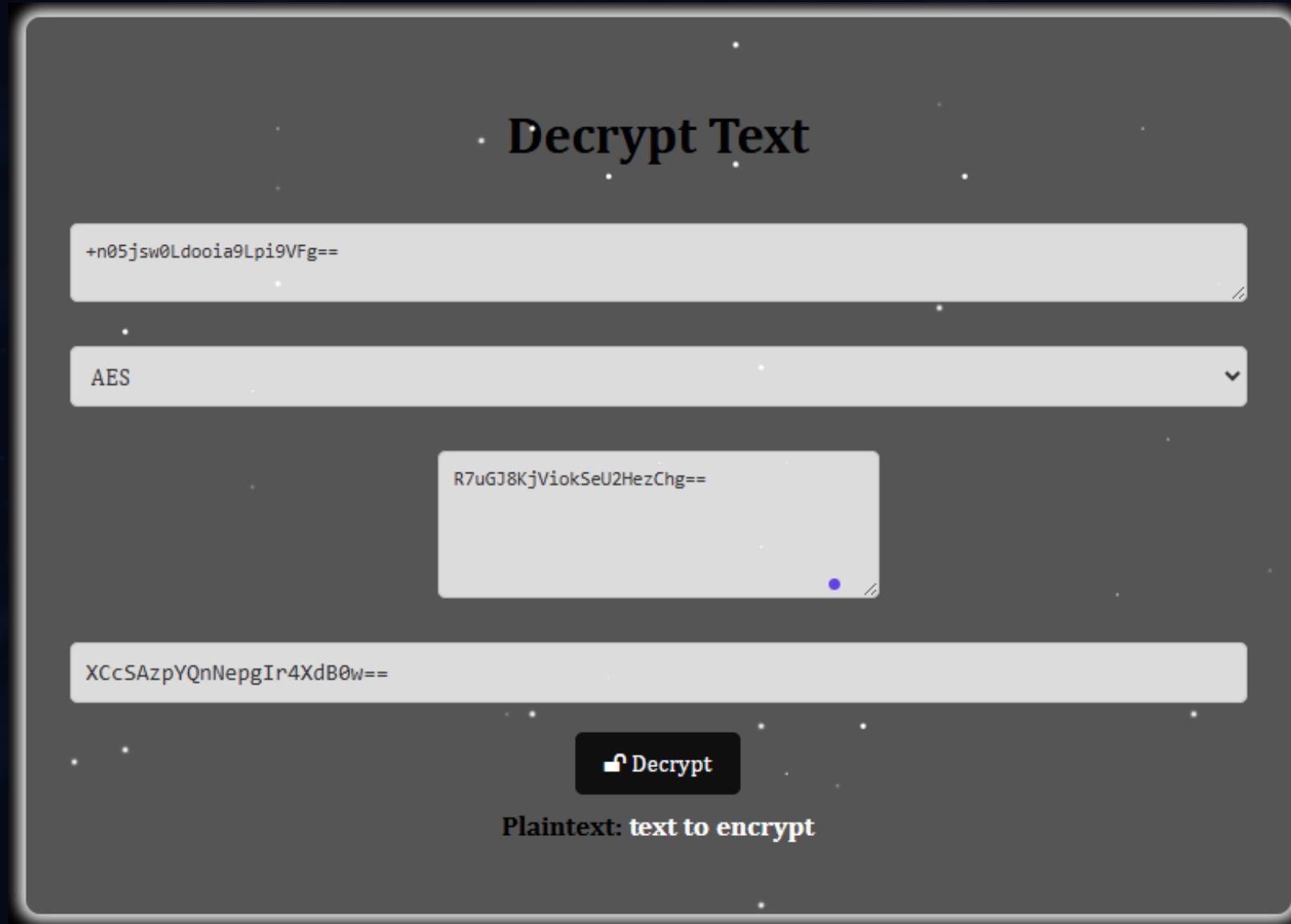
# HOW THIS WORKS?



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?

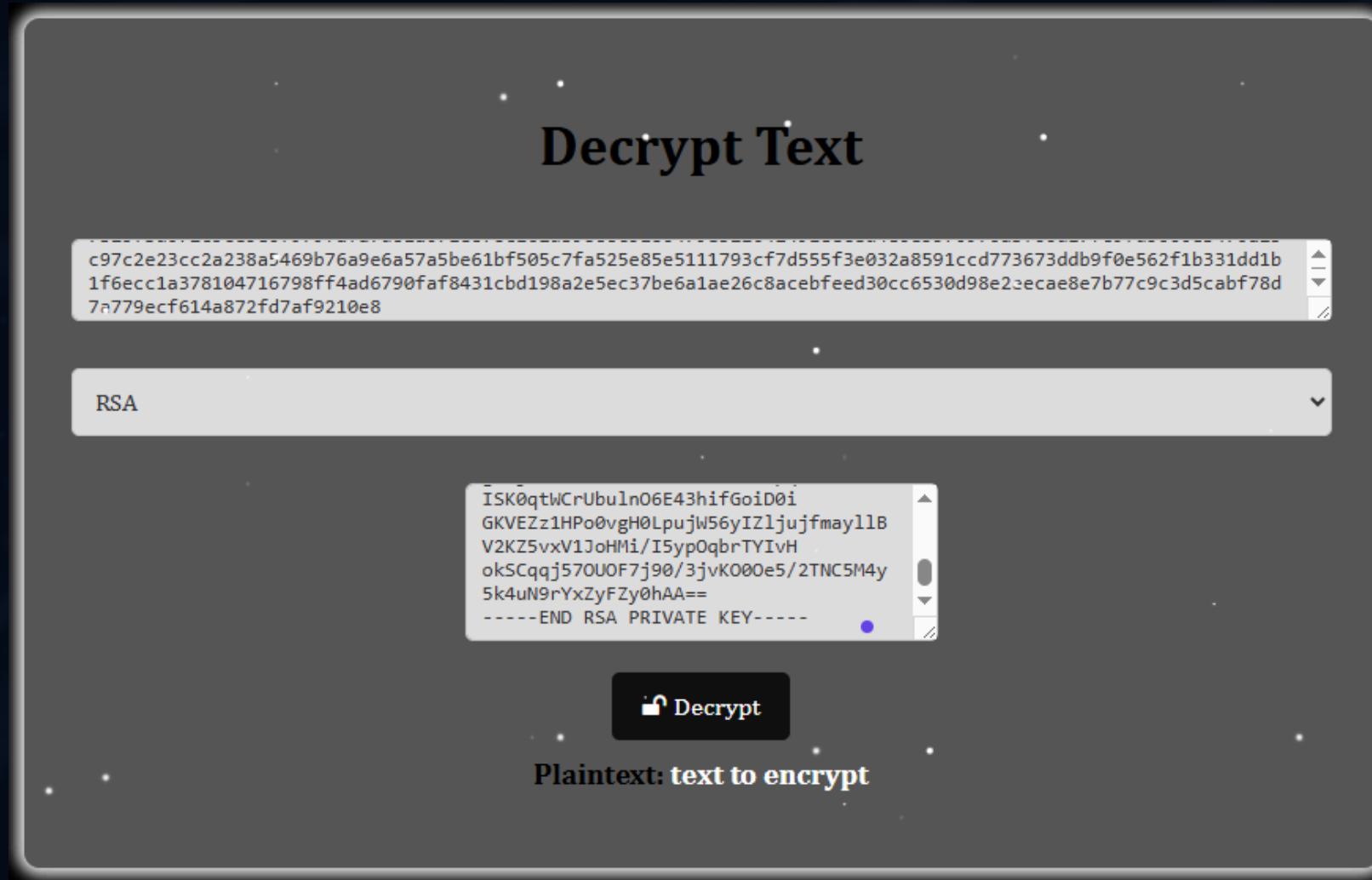
## DECRYPTION PHASE



**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.

# HOW THIS WORKS?

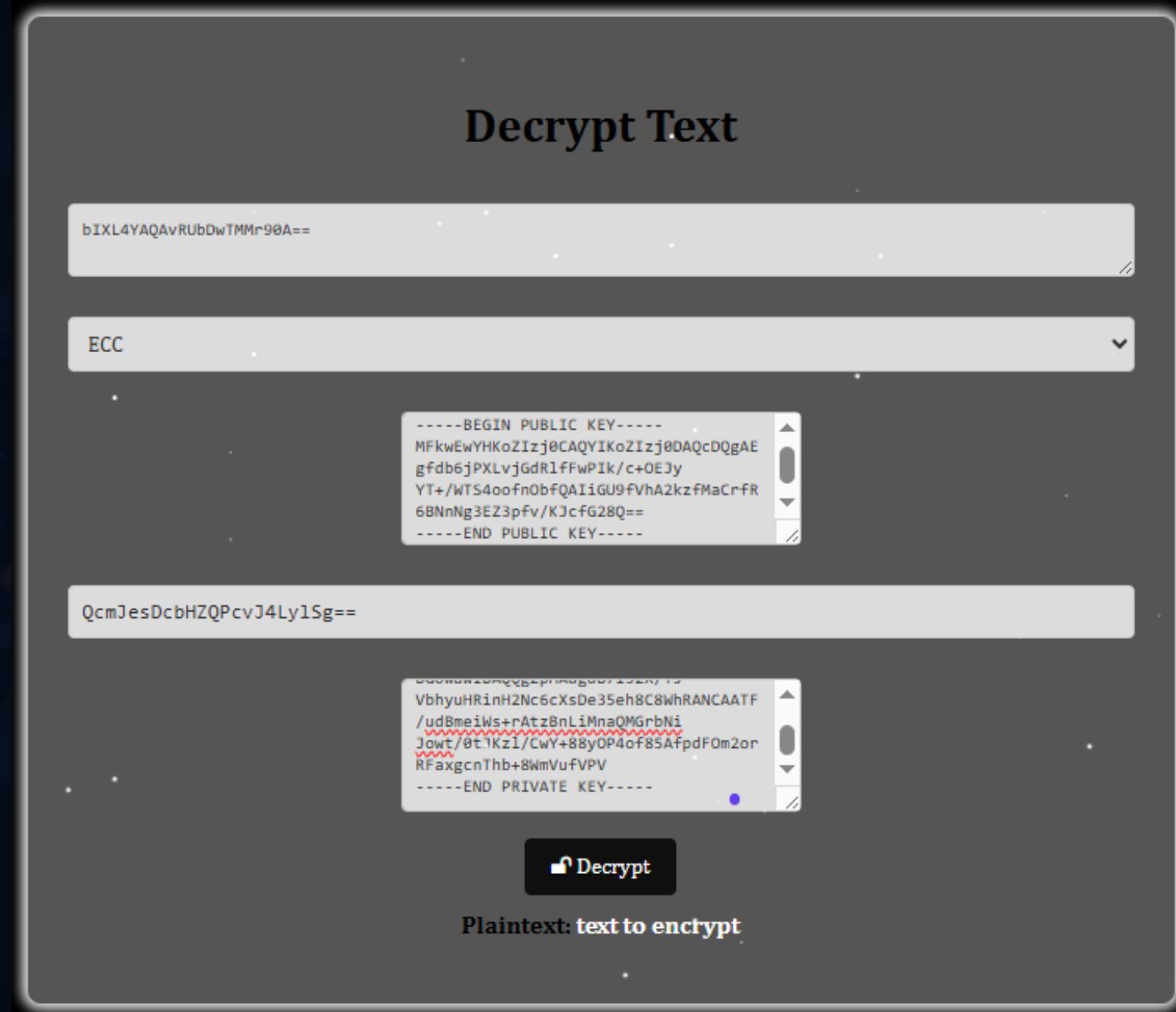
## DECRYPTION PHASE



**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.

# 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](http://WWW.CIPHERGUARD.COM)



# MEET THE TEAM



AHMED MNAOUER



ROUA ABASSI

WWW.CIPHERGUARD.COM



# THANK YOU !

WWW.CIPHERGUARD.COM