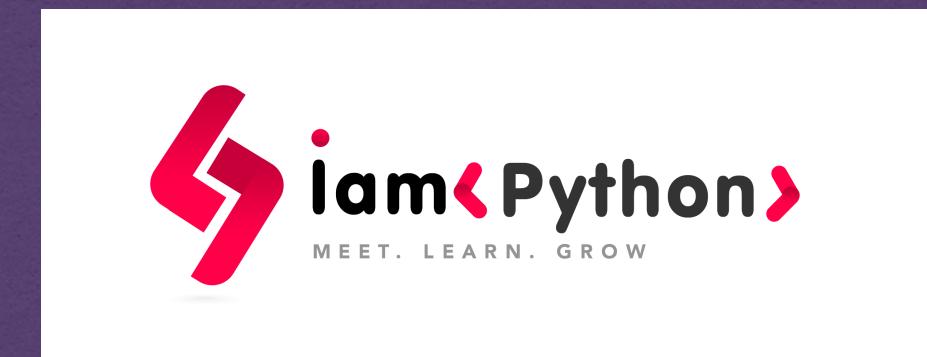
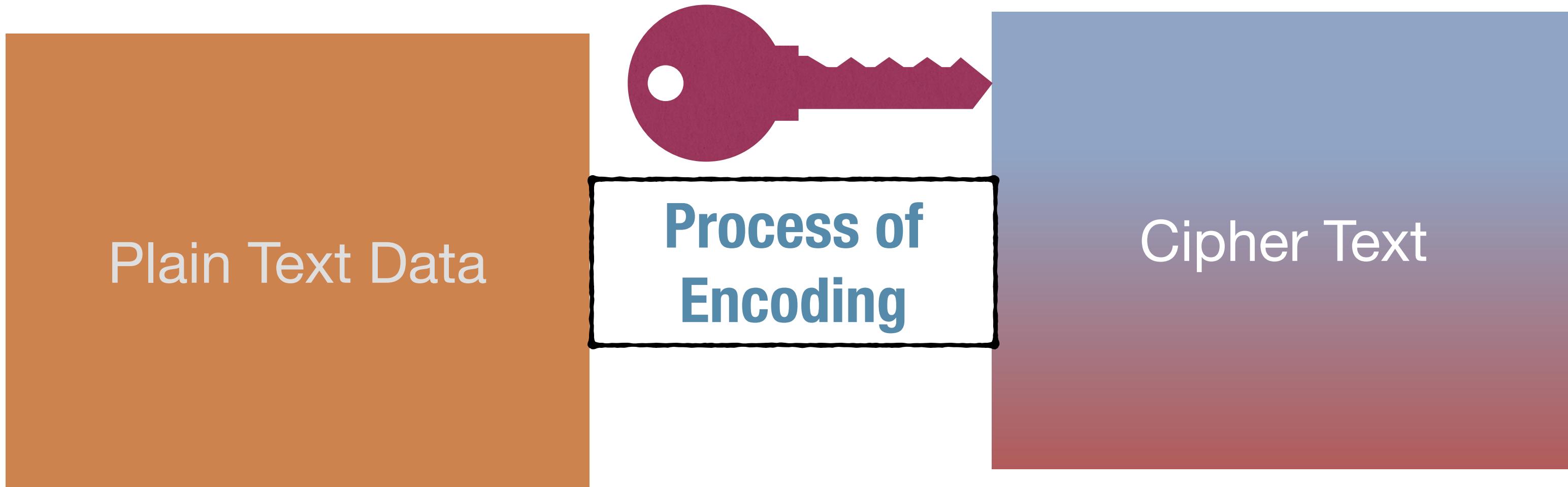


# ENCRYPTION DECRYPTION IN PYTHON



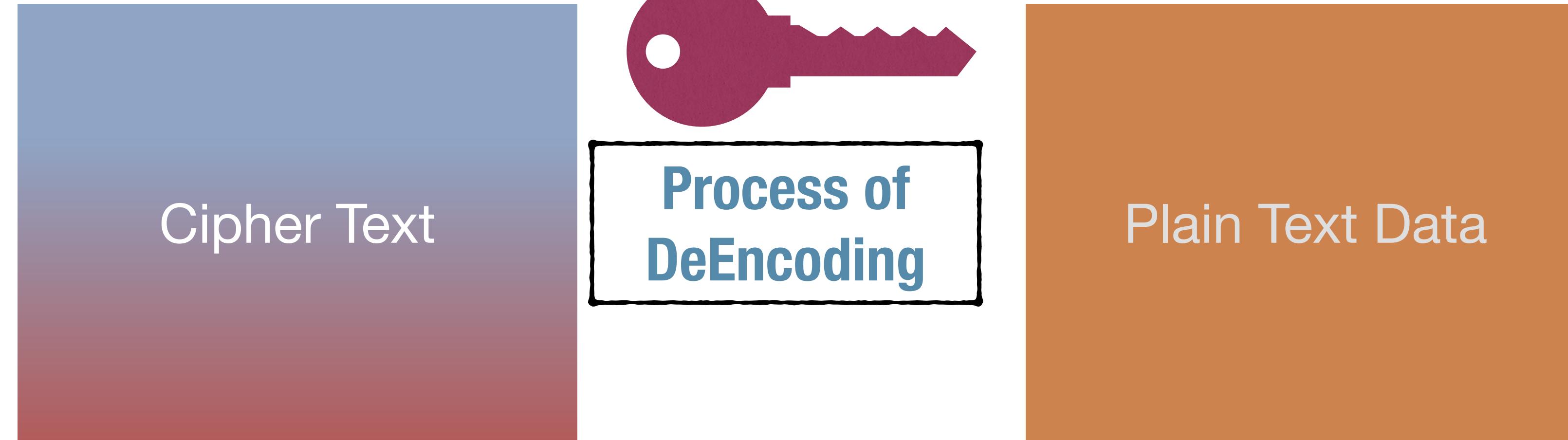
# What is Encryption?



**Encryption is the process of encoding the data.  
i.e converting plain text into ciphertext.**

**This conversion is done with a key called an  
encryption key.**

# What is Decryption?



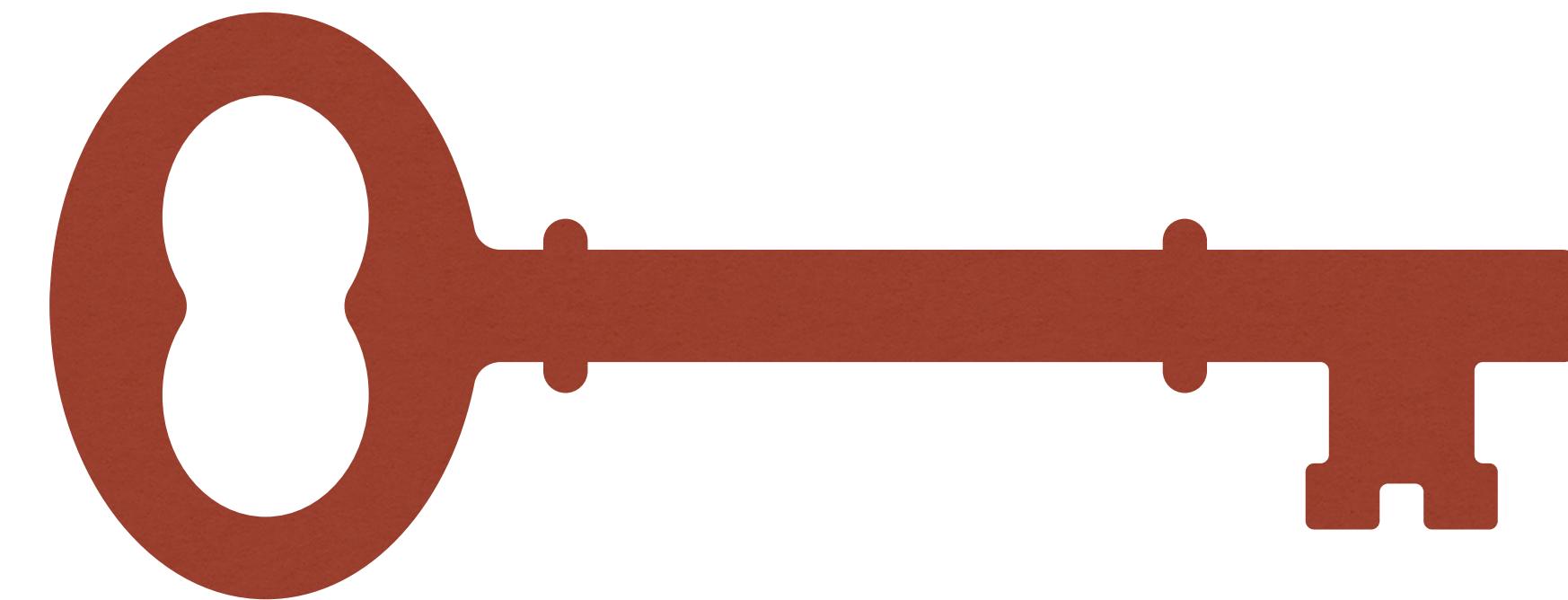
**Decryption is a process of decoding the encoded data. Converting the ciphertext into plain text.**

**This process requires a key that we used for encryption.**

# Two Important Keys Used.



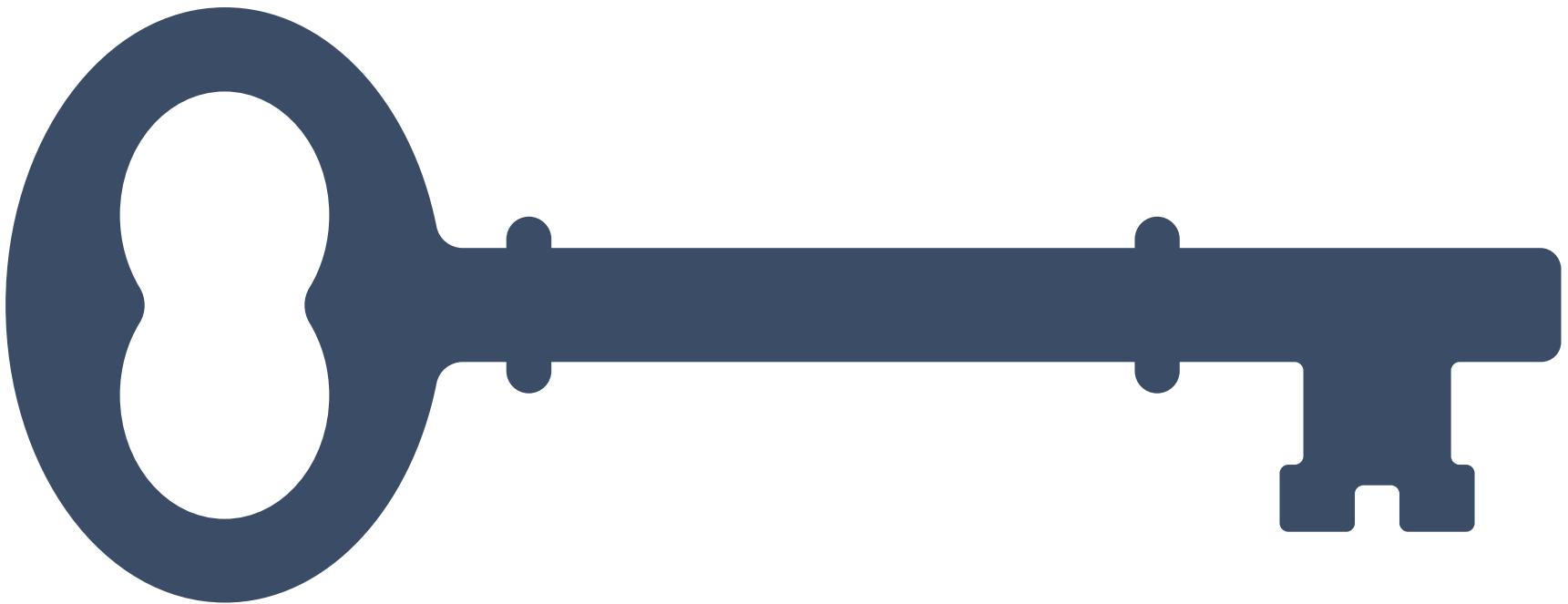
**SYMMETRIC-KEY**



**ASYMMETRIC-KEY.**

# What is Symmetric-key?

The data is encoded  
and decoded with  
the same key.

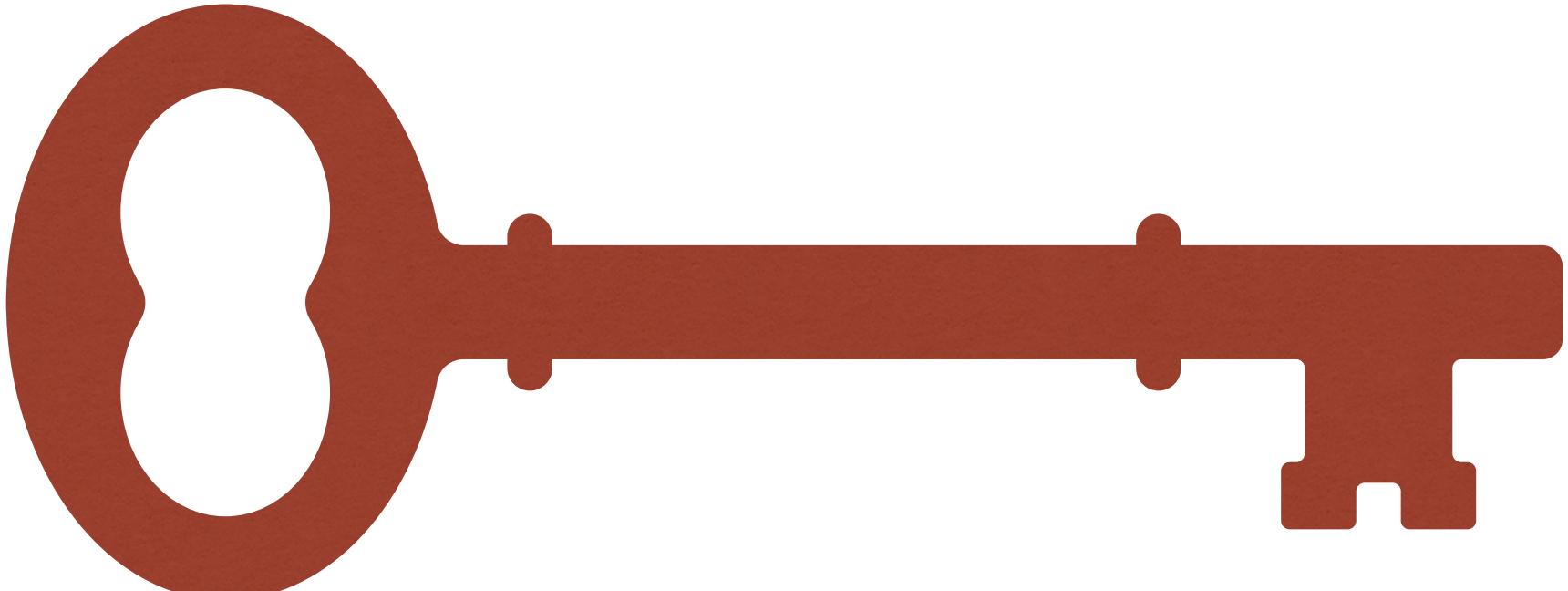


**SYMMETRIC-KEY**

This is the easiest way of  
encryption, but also less  
secure.

# What is Asymmetric-key?

We use two keys a  
public key and  
private key



**ASYMMETRIC-KEY.**

The public key is used to  
encrypt the data and the  
private key is used to  
decrypt the data.

# Python Libraries

MODULE NAME	DESCRIPTION	INSTALLATION
<b>PYCRYPTO</b>	<p>Secure hash functions such as RIPEMD160, SHA256, and various <b>encryption</b> algorithms such as AES, DES, RSA, ElGamal</p> 	<pre>pip install pycrypto</pre>
<b>CRYPTOGRAPHY</b>	<p>Cryptographic algorithms such as symmetric ciphers, message digests, and key derivation functions.</p> <p>( <b>Fernet - symmetric encryption</b>)</p>	<pre>pip install cryptography</pre>
<b>RSA</b>	<p>It supports encryption and decryption, signing and verifying signatures, and key generation according to PKCS#1 version 1.5.</p> <p>( <b>rsa.newkeys() - asymmetric encryption</b>)</p>	<pre>pip install rsa</pre>

**CODE NOW....**

```
from cryptography.fernet import Fernet

message = "Hello, iampython"

key = Fernet.generate_key()
fernet = Fernet(key)

encrypted_message = fernet.encrypt(message.encode())
decrypted_message = fernet.decrypt(encrypted_message).decode()

print("Original String Value: ", message)
print("Encrypted String Value: ", encrypted_message)
print("decrypted string: ", decrypted_message)

with open('test.txt', 'wb') as file:
    file.write(encrypted_message)
```

```
import rsa

publicKey, privateKey = rsa.newkeys(512)
print(publicKey, privateKey)
message = "hello iampythoner"
encrypted_message = rsa.encrypt(message.encode(),
                                 publicKey)
print("my string: ", message)
print("encrypted string: ", encrypted_message)
decrypted_message = rsa.decrypt(encrypted_message, privateKey).decode()
print("decrypted string: ", decrypted_message)
```