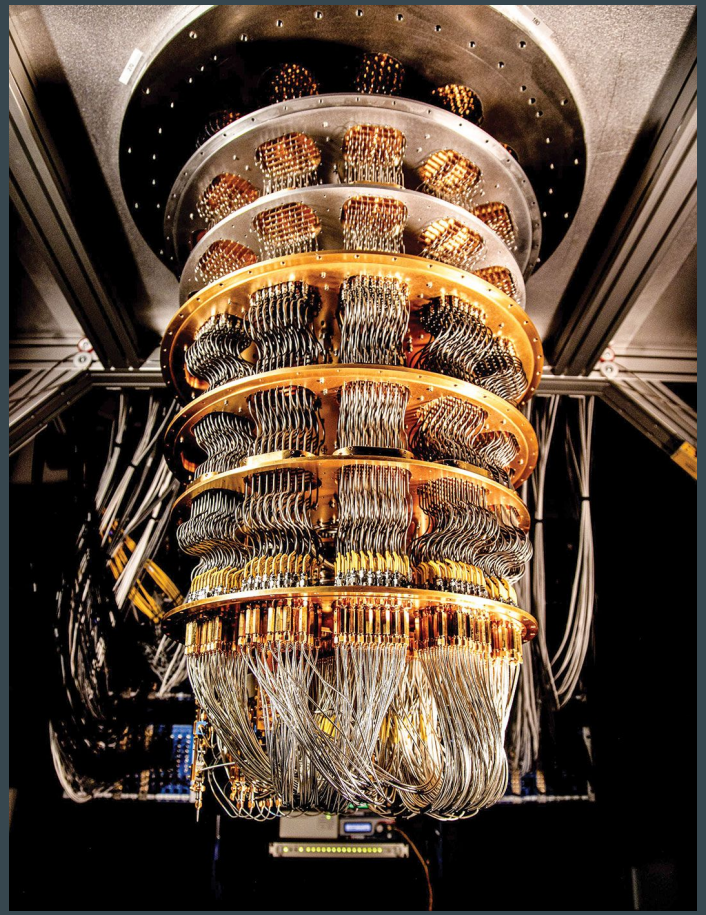
DATA PROTECTIONS

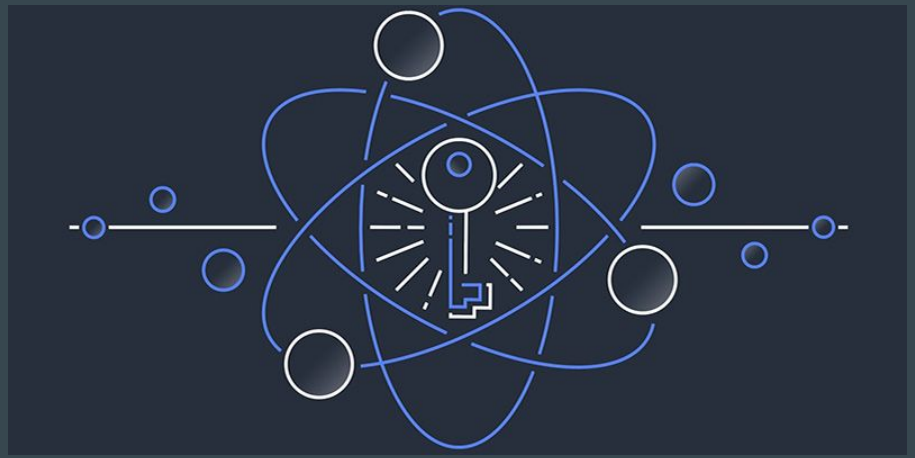


TEAM QUANTUM MANIAC •••

TEAM MEMBERS:-

- NAMAN KAUSHIK
- MD SAJIDULLAH ANSARI

TIMELINE:-



DES ENCRYPTION

AES ENCRYPTION

Quantum cryptography

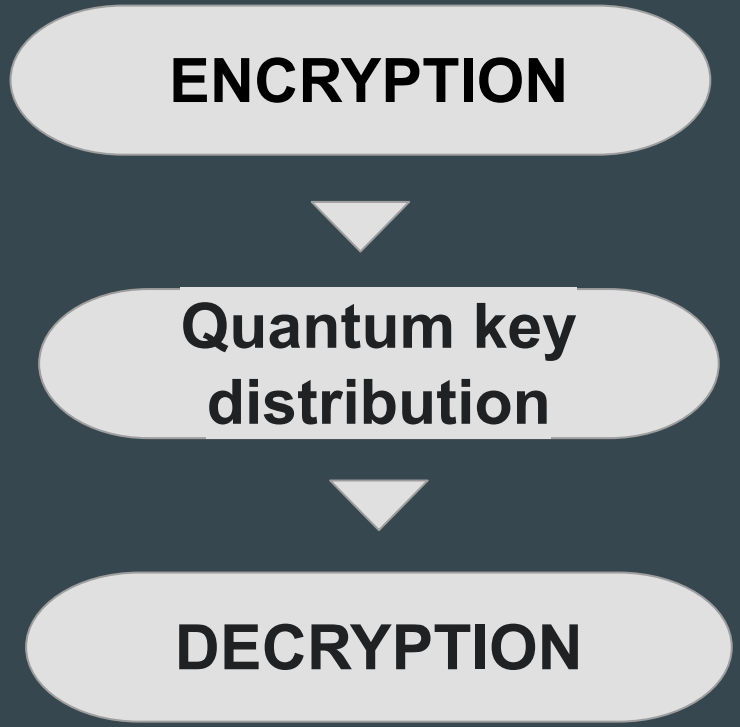
PROBLEM STATEMENT

As a Banking Firm, You always need to be data proof because these are sensitive data to deal with and with the advent of quantum computing, traditional encryption methods are becoming increasingly vulnerable to attacks. Therefore, there is a growing need for developing quantum-safe encryption algorithms to protect sensitive data from potential breaches. The challenge is to find efficient and reliable methods of implementing quantum-safe encryption techniques that can secure the transfer and storage of sensitive data. The objective is to explore the potential of quantum cryptography and related technologies to provide a secure platform for data protection in the face of quantum computing threats.

SOLUTION

QKD can provide unconditional security against any computational attack, including quantum attacks, making it a promising solution for secure communication.QKD is a method of generating and sharing secret keys between two parties based on the principles of quantum mechanics. Unlike classical key exchange protocols, QKD uses the fundamental laws of physics to protect data transmission against eavesdropping.

METHODOLOGY



STEPS:-

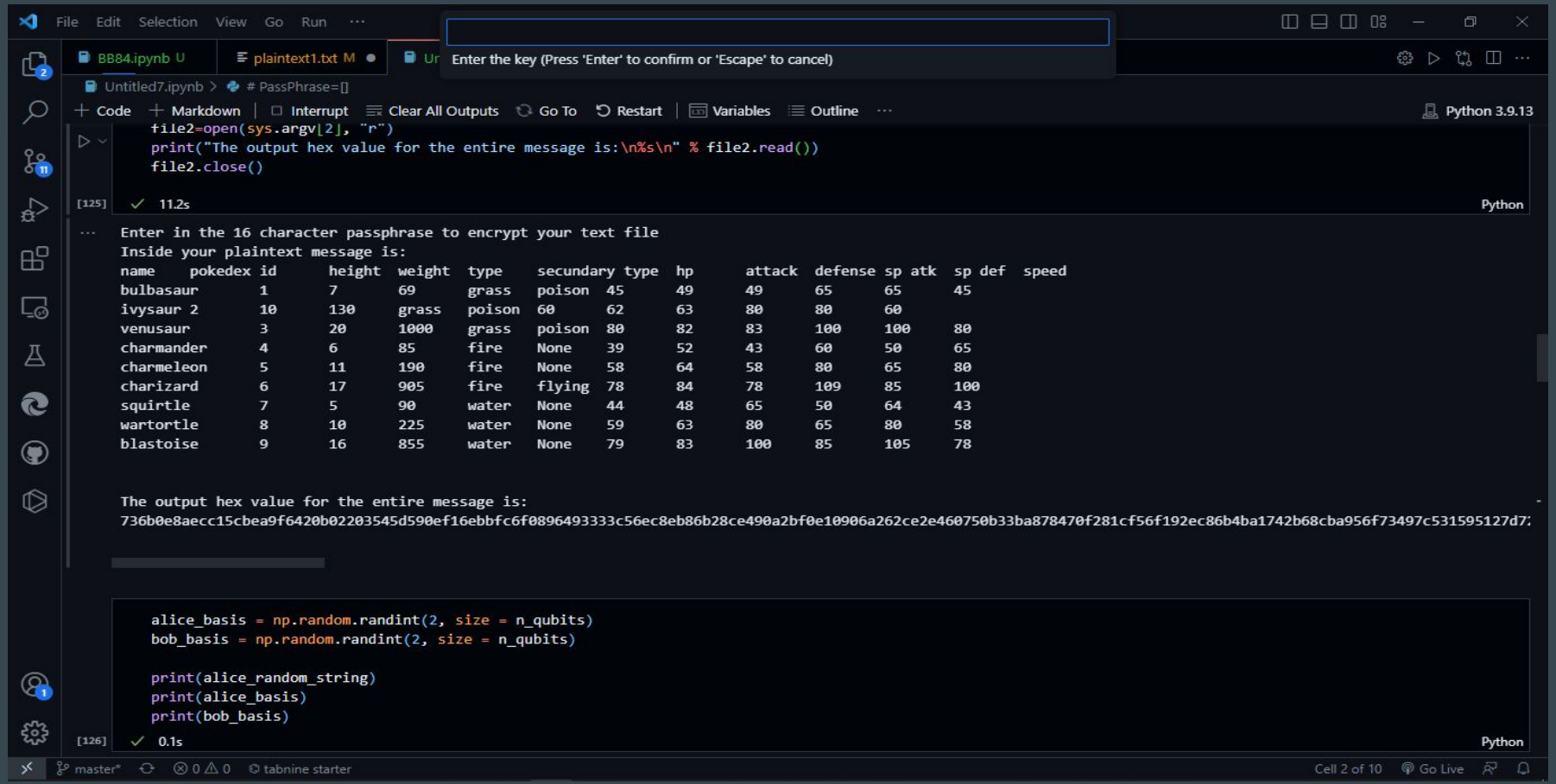
1. We have implemented a secure system for encrypting and decrypting data.
2. The Advanced Encryption Standard (AES) provides strong encryption for sensitive data using a secret key.
3. The BB84 protocol is used for secure key transfer by leveraging the principles of quantum mechanics.
4. By using both AES and BB84, you have created a secure system for transmitting and decrypting data.
5. BB84 is used to detect any attacks or interference during the key transfer process, adding an additional layer of security to the system.

AES algorithm:-

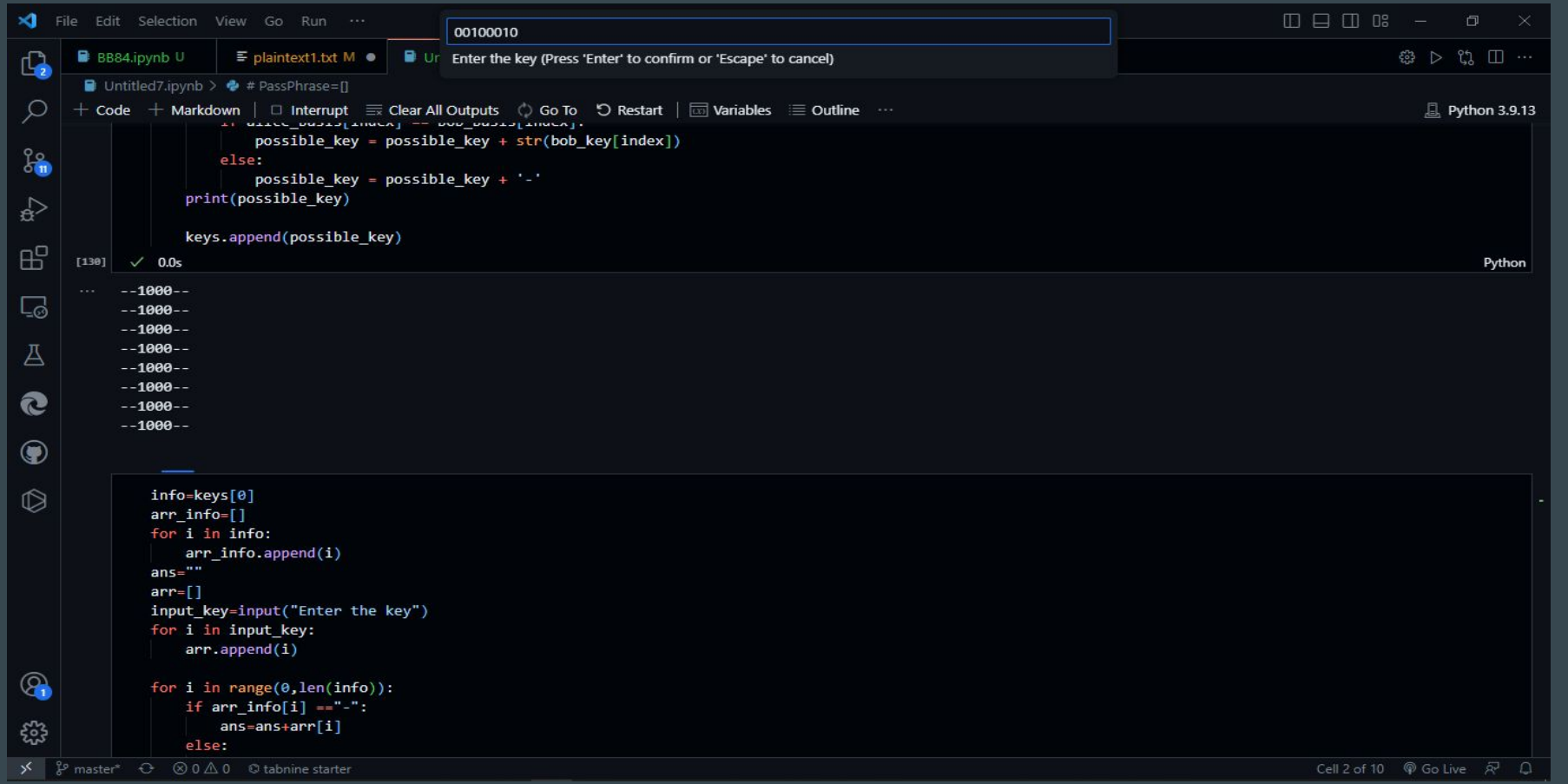
- AES is a symmetric-key encryption algorithm that is widely used for securing data.
- It operates on fixed-length blocks of data and uses a key to transform plaintext into ciphertext and back.
- The key length can be 128, 192, or 256 bits, and the block length is fixed at 128 bits.
- The AES algorithm consists of several rounds of operations, including byte substitution, shift rows, mix columns, and add round key.
- AES is widely accepted and trusted for its strong security properties and efficiency in terms of computation time and memory usage.

WORKING PROTOTYPE

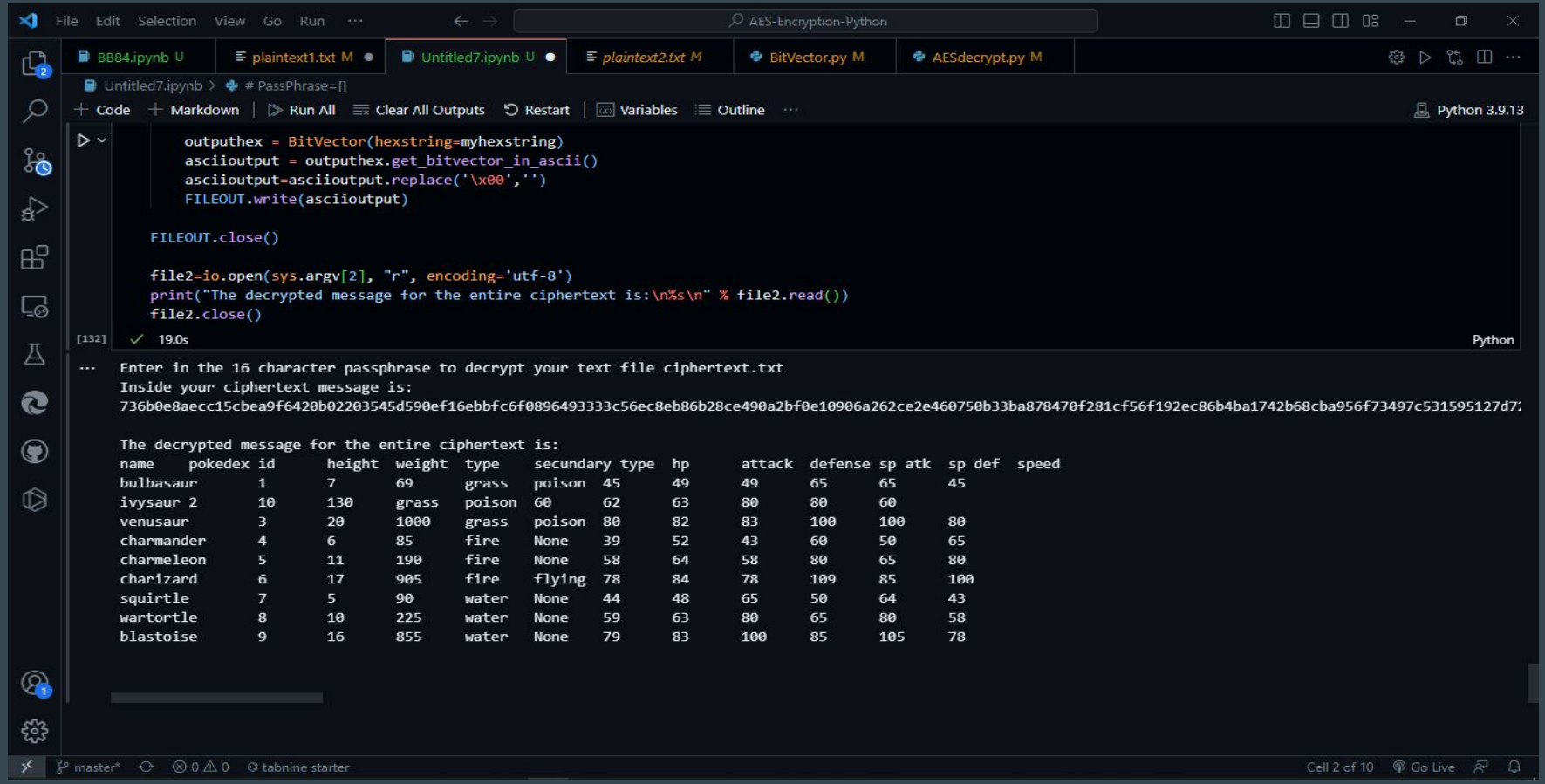
ENCRYPTED DATA



RECEIVER ENTERING THE KEY



DECRYPTED DATA

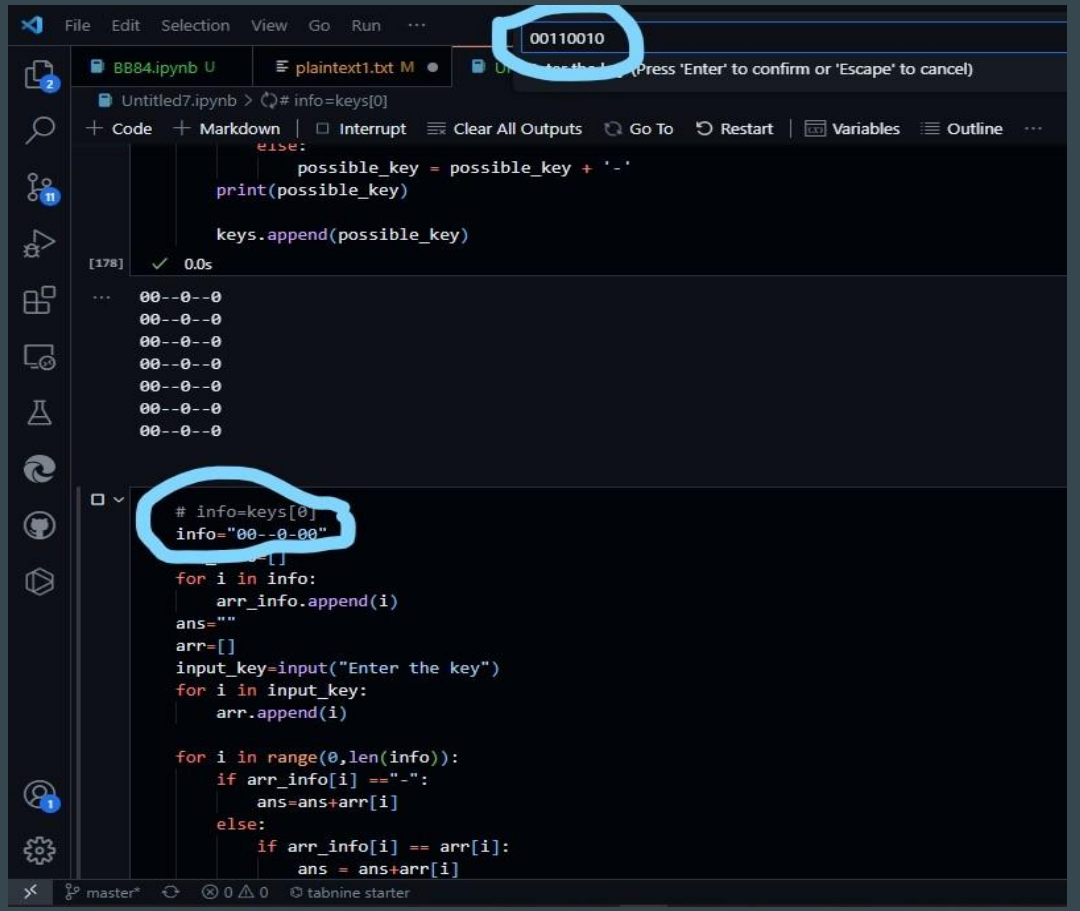


INTERCEPTION DETECTION

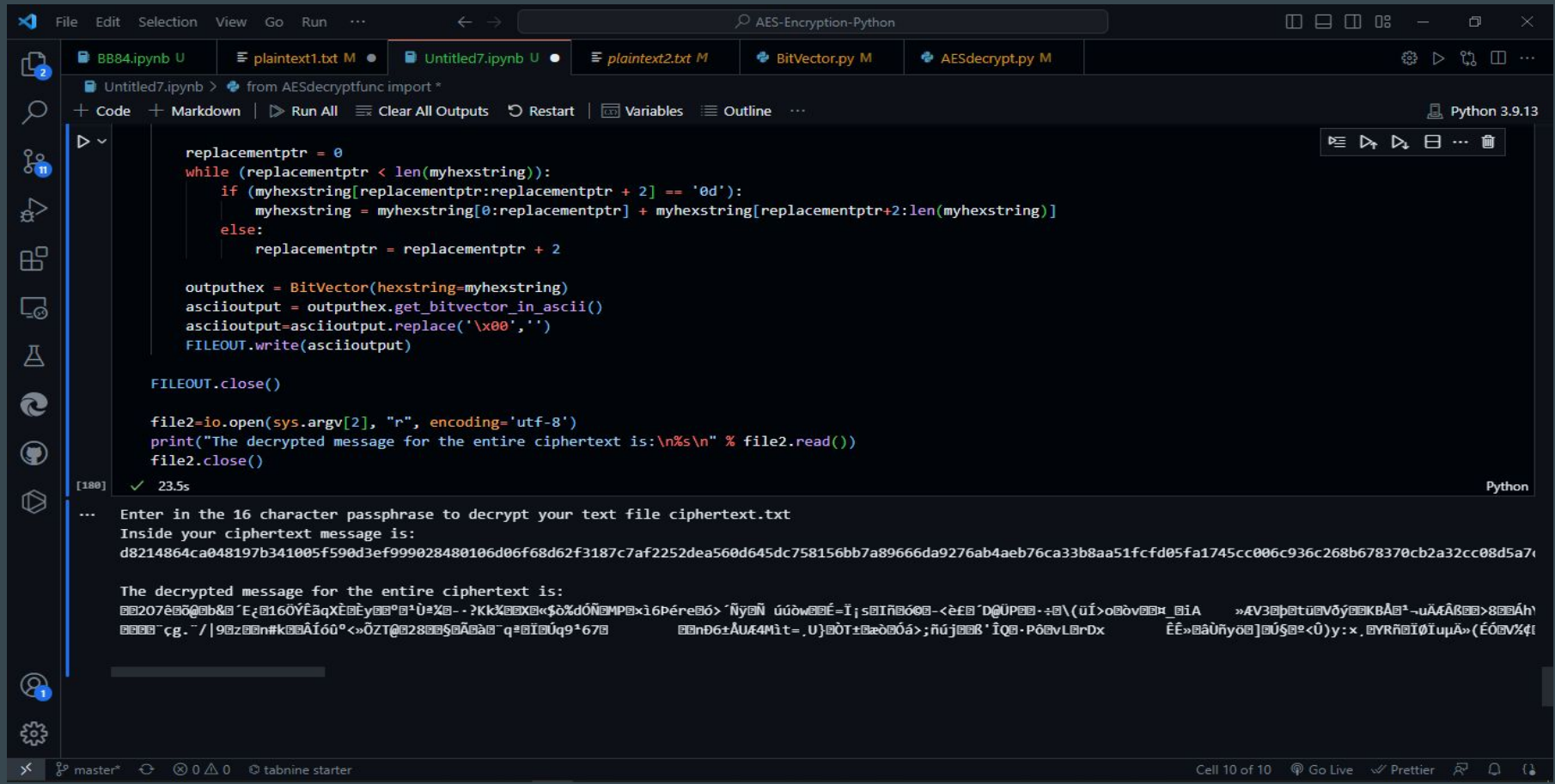
```
# PassPhrase=[]
n_qubits = 8
indx=0
PassPhrase=""
j=""
alice_random_string = np.random.randint(2, size = n_qubits)
for i in alice_random_string:
    j=str(i)
    PassPhrase = PassPhrase + j
print(PassPhrase)
```

[172] ✓ 0.0s

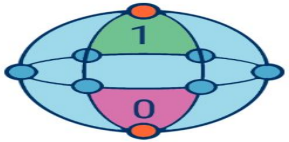
```
00110010
```



DECRYPTED DATA AFTER INTERCEPTION

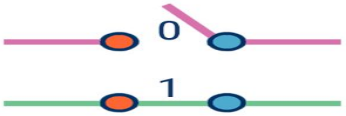


Quantum Computing Vs. Classical Computing



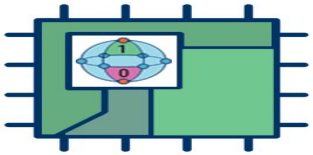
Calculates with qubits, which can represent 0 and 1 at the same time

Calculates with transistors, which can represent either 0 or 1



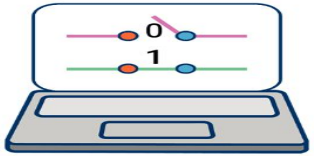
Power increases exponentially in proportion to the number of qubits

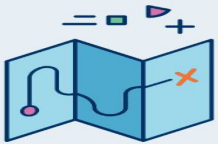
Power increases in a 1:1 relationship with the number of transistors



Quantum computers have high error rates and need to be kept ultracold

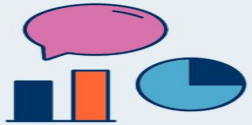
Classical computers have low error rates and can operate at room temp





Well suited for tasks like optimization problems, data analysis, and simulations

Most everyday processing is best handled by classical computers



advantages of quantum computing :-

- **Faster computation:** Quantum computer excels in some specialized tasks over a supercomputer. A currently existing quantum computer developed by Google is 158 million times more powerful than a supercomputer.
- **Lower power consumption:** The power consumption of a quantum computer is less than that of a supercomputer due to quantum tunneling.
- **Simulation:** Quantum computers are more efficient at modeling natural systems at the quantum level and can simulate the dynamics of quantum systems more accurately.

QUANTUM KEY DISTRIBUTION

BB84 ALGORITHM:-

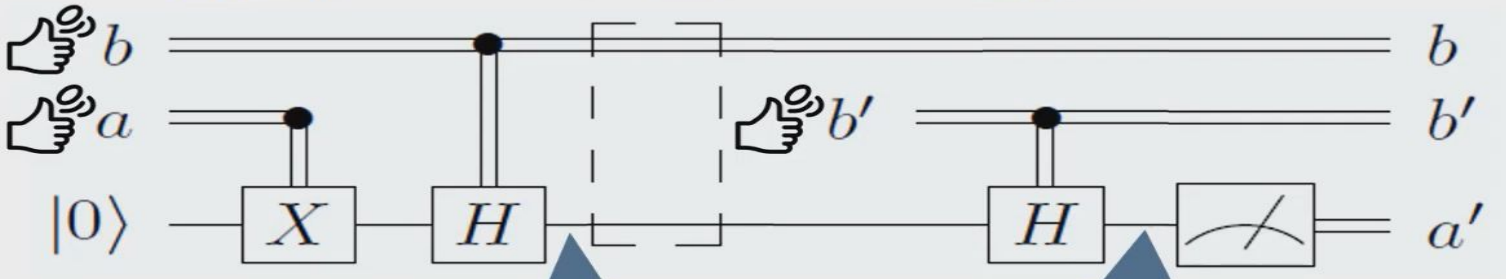
The methodology for implementing the BB84 protocol involves the following steps:

1. Create a random binary key.
2. Encode the key into quantum states using randomly selected bases.
3. Transmit the quantum states over a secure communication channel.
4. Measure the received quantum states using randomly selected bases.
5. Compare a subset of the key bits to detect any errors or eavesdropping attempts.
6. Use privacy amplification techniques to distill a smaller, but more secure key.

BB84 PROTOCOL

measured!

b=b′ / b≠b′



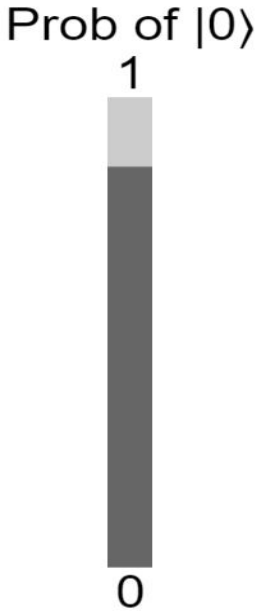
a	b	$\|\psi\rangle$
0	0	$\|0\rangle$
0	1	$\|+\rangle$
1	0	$\|1\rangle$
1	1	$\|-\rangle$

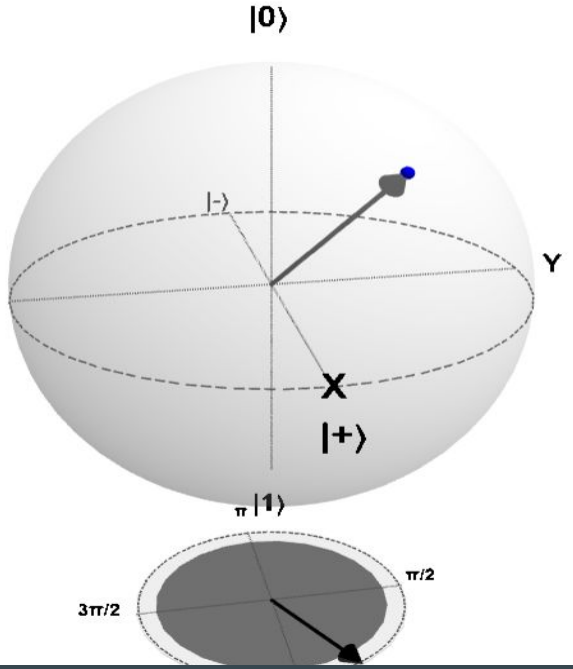
a	b	b'	$\|\psi'\rangle$
0	0	0	$\|0\rangle$
~~0~~	~~0~~	~~1~~	~~$\|+\rangle$~~
~~0~~	~~1~~	~~0~~	~~$\|+\rangle$~~
0	1	1	$\|0\rangle$
1	0	0	$\|1\rangle$
~~1~~	~~0~~	~~1~~	~~$\|-\rangle$~~
~~1~~	~~1~~	~~0~~	~~$\|-\rangle$~~
1	1	1	$\|1\rangle$

QUBIT:-

https://javafxpert.github.io/grok-bloch/

$$|\psi\rangle = \sqrt{0.85}\,|0\rangle + (\sqrt{0.15})e^{i0.15\pi}\,|1\rangle$$





INTERCEPTION-RESEND ATTACK DETECTION TECHNIQUE:-

The Interception-resend attack detection technique is a method used to detect data breaches in the BB84 key exchange protocol

1. The sender and receiver exchange key bits using the BB84 protocol.
2. A subset of the key bits exchanged between the sender and receiver is randomly selected.
3. The sender and receiver compare the selected key bits to a public reference. The public reference is a set of key bits that are publicly known to both parties and are not part of the key exchange.
4. If the selected key bits match the public reference, it is likely that the key exchange was not intercepted and modified by an eavesdropper. If the key bits do not match the public reference, it is likely that an eavesdropper has intercepted and modified the key.

IS IT GREENER AND SUSTAINABLE ALTERNATIVE?

It is a mathematical method that is used to ensure the security and integrity of communication channels. While reducing energy consumption and minimizing waste is essential for a sustainable future.

THANK YOU