PRACTICAL: 9

AIM:

Study of various cryptographic algorithms using CrypTool.

THEORY:

CrypTool is an open-source project that is a free e-learning software for illustrating cryptographic and cryptanalytic concepts. According to "Hakin9", CrypTool is worldwide the most widespread e-learning software in the field of cryptology. CrypTool implements more than 400 algorithms.Users can adjust these with own parameters. To introduce users to the field of cryptography, the organization created multiple graphical interface software containing an online documentation, analytic tools and algorithms. They contain most classical ciphers, as well as modern symmetric and asymmetric cryptography including RSA, ECC, digital signatures, hybrid encryption, homomorphic encryption, and Diffie–Hellman key exchange. Methods from the area of quantum cryptography (like BB84 key exchange protocol) and the area of post-quantum cryptography (like McEliece, WOTS, Merkle-Signature-Scheme, XMSS, XMSS_MT, and SPHINCS) are implemented. In addition to the algorithms, solvers (analyzers) are included, especially for classical ciphers. Other methods (for instance Huffman code, AES, Keccak, MSS) are visualized.

Algorithms analyzed in this practical:

Caesar cipher: A Caesar cipher is a simple method of encoding messages. Caesar ciphers use a substitution method where letters in the alphabet are shifted by some fixed number of spaces to yield an encoding alphabet. A Caesar cipher with a shift of 1 would encode an A as a B, an M as an N, and a Z as an A, and so on.

AES: Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

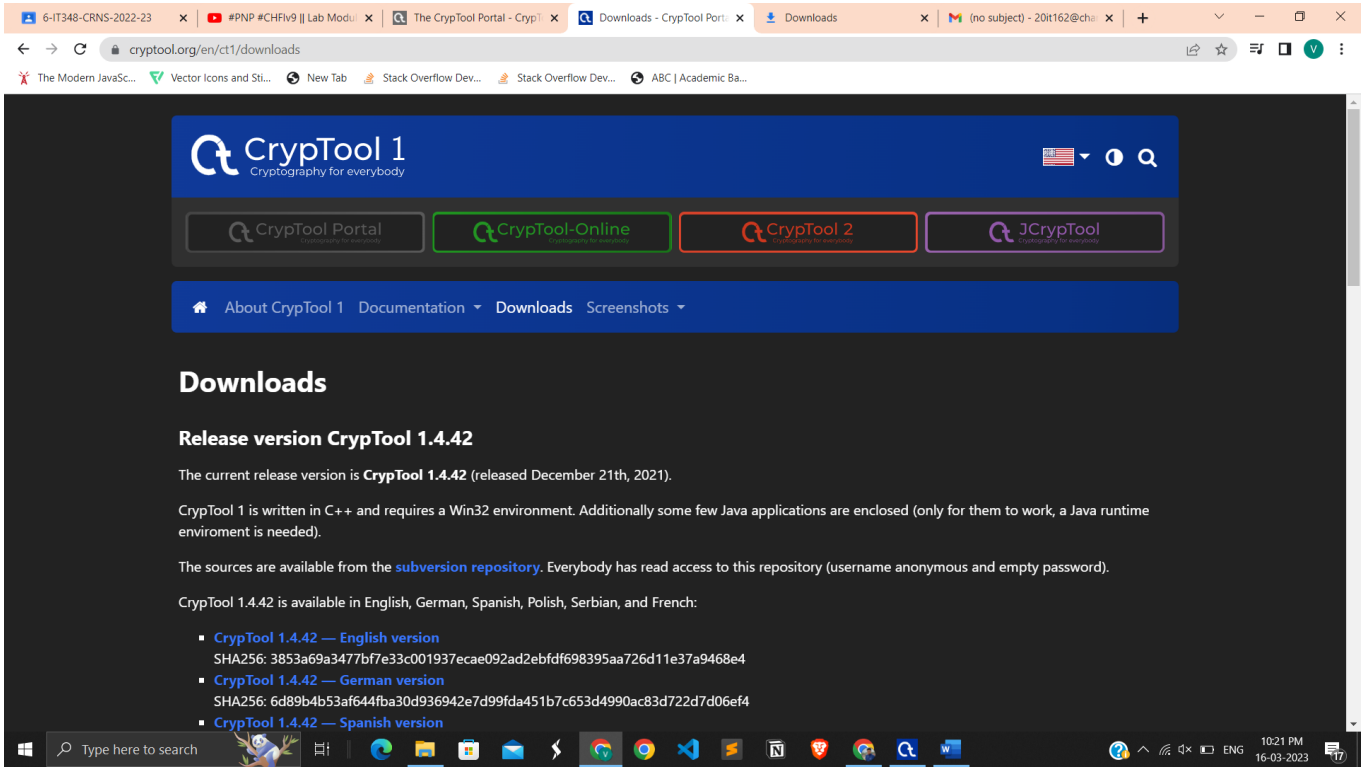
Points to remember

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each

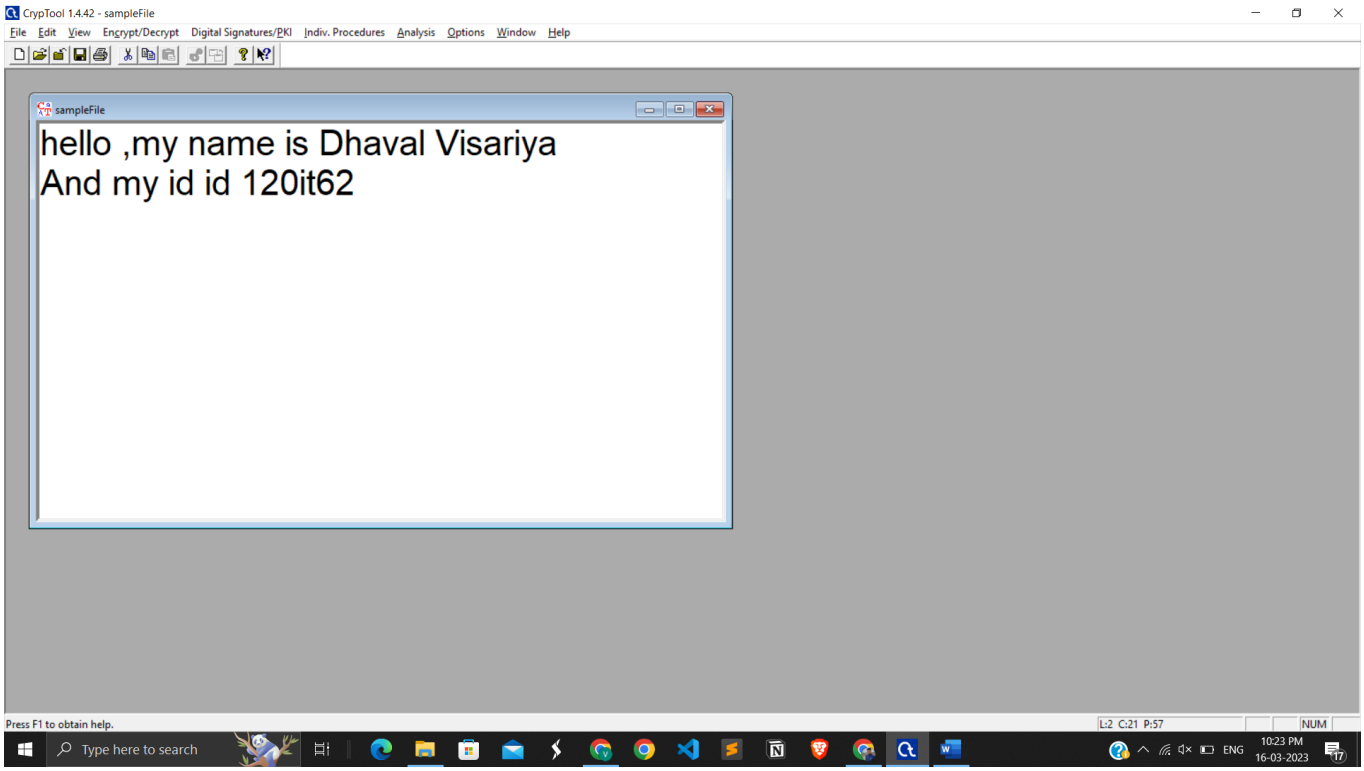
DES: DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

RSA: RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private.

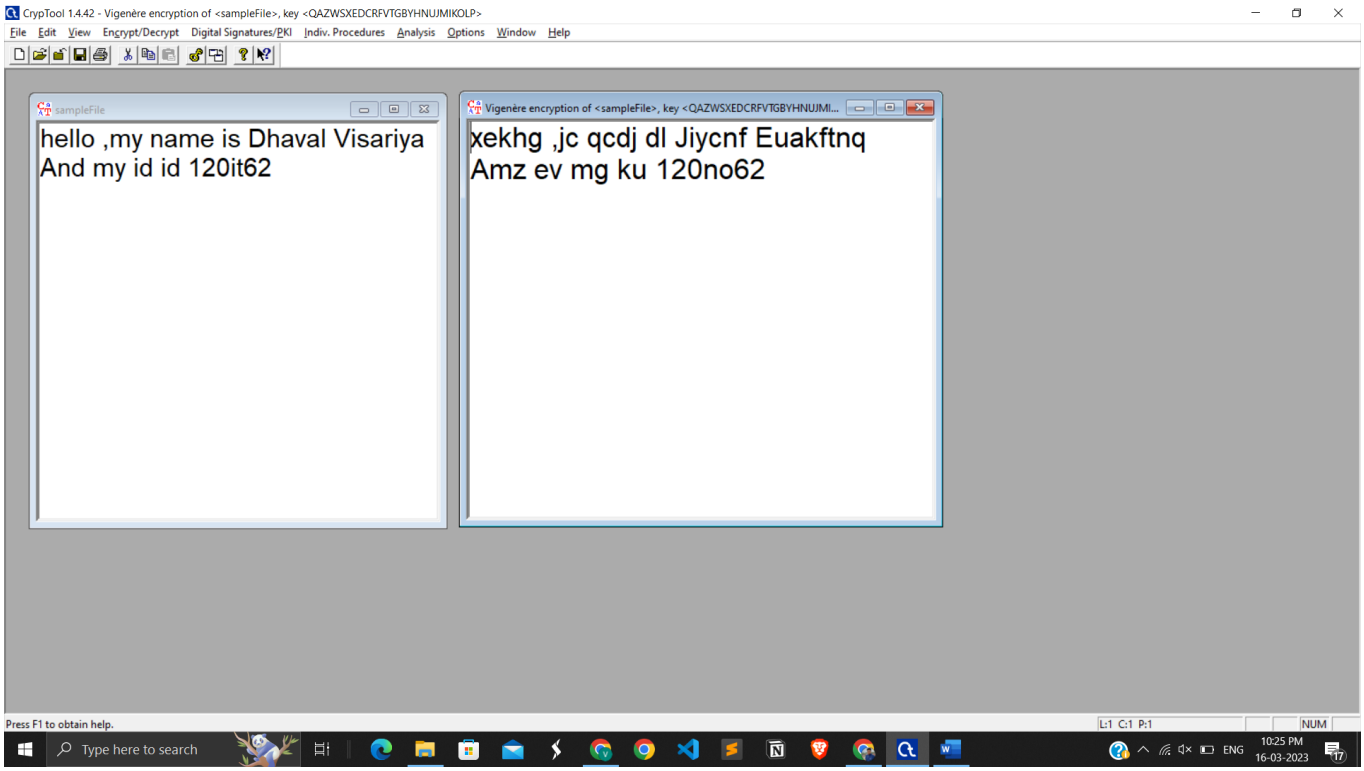
OUTPUT:



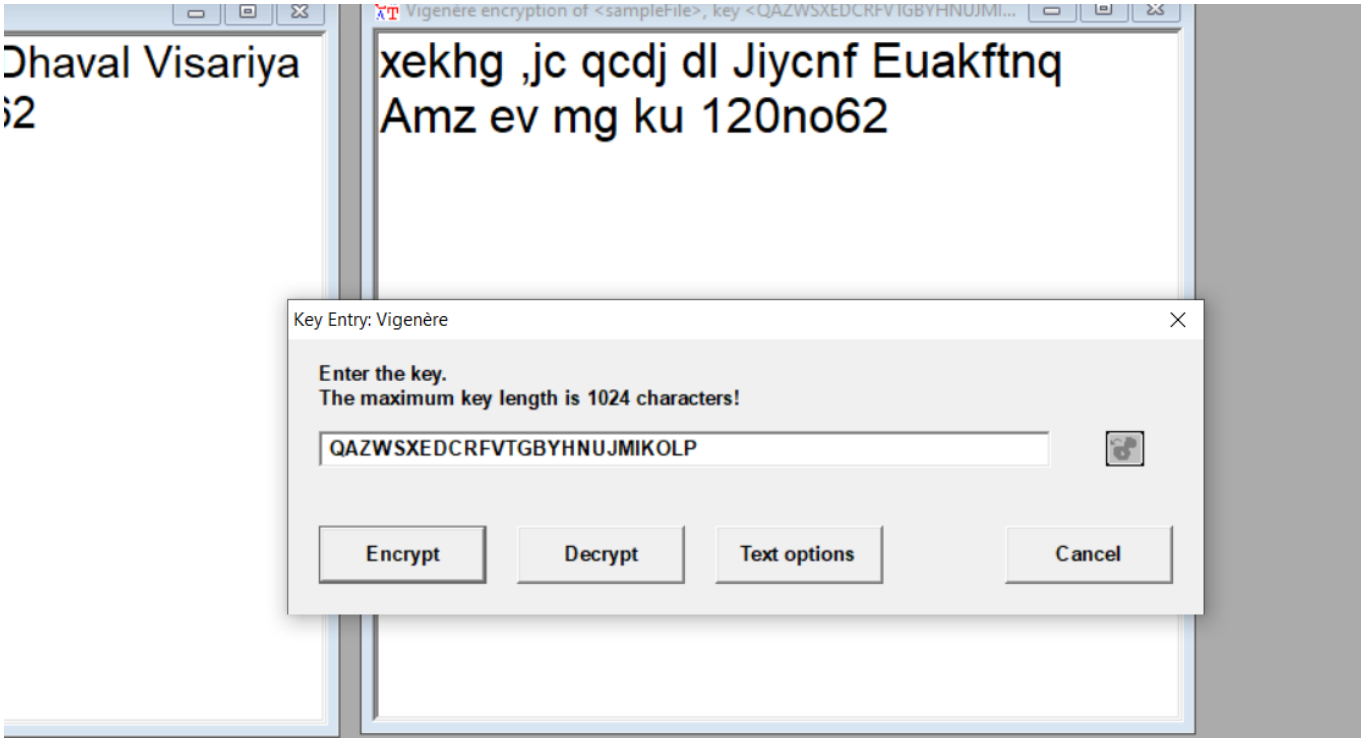
We can download CrypTool from this site



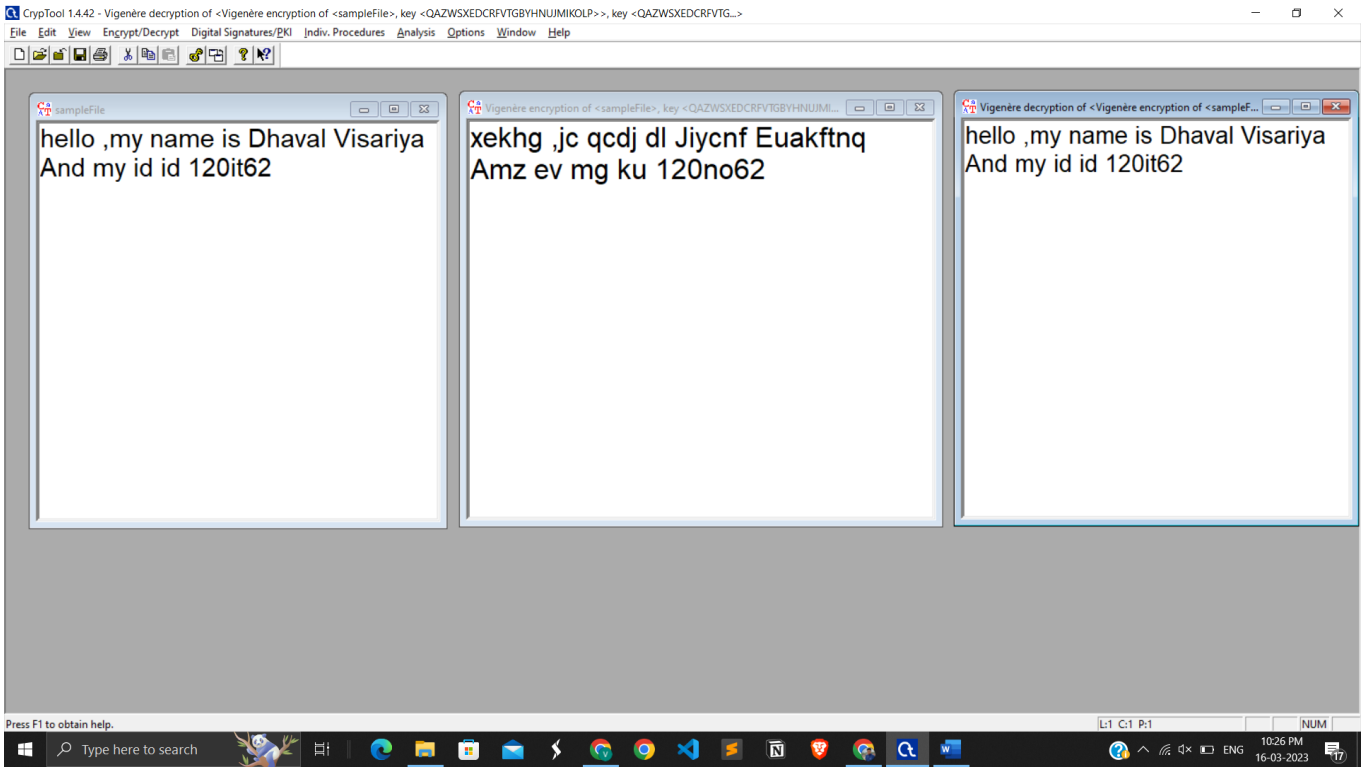
Created a file for encryption and decryption



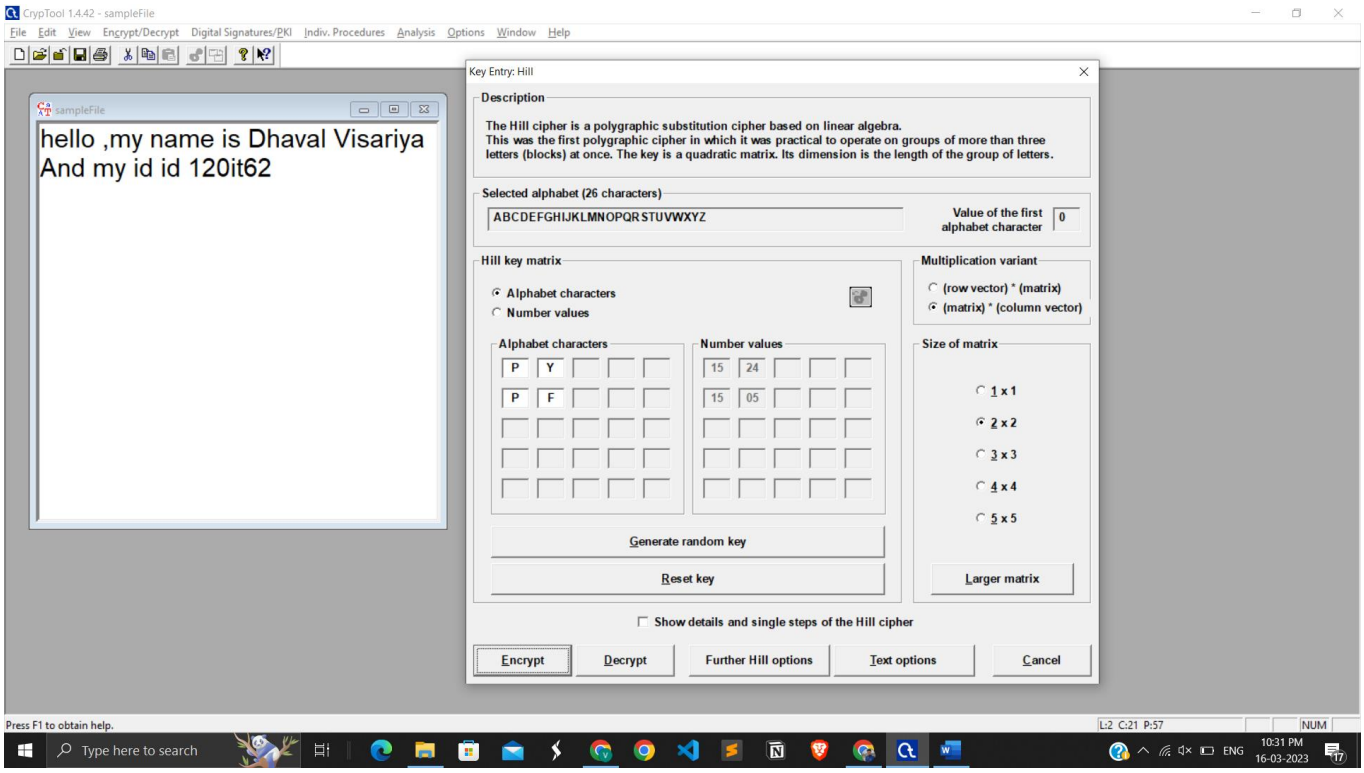
Encrypt a file using Vigenere



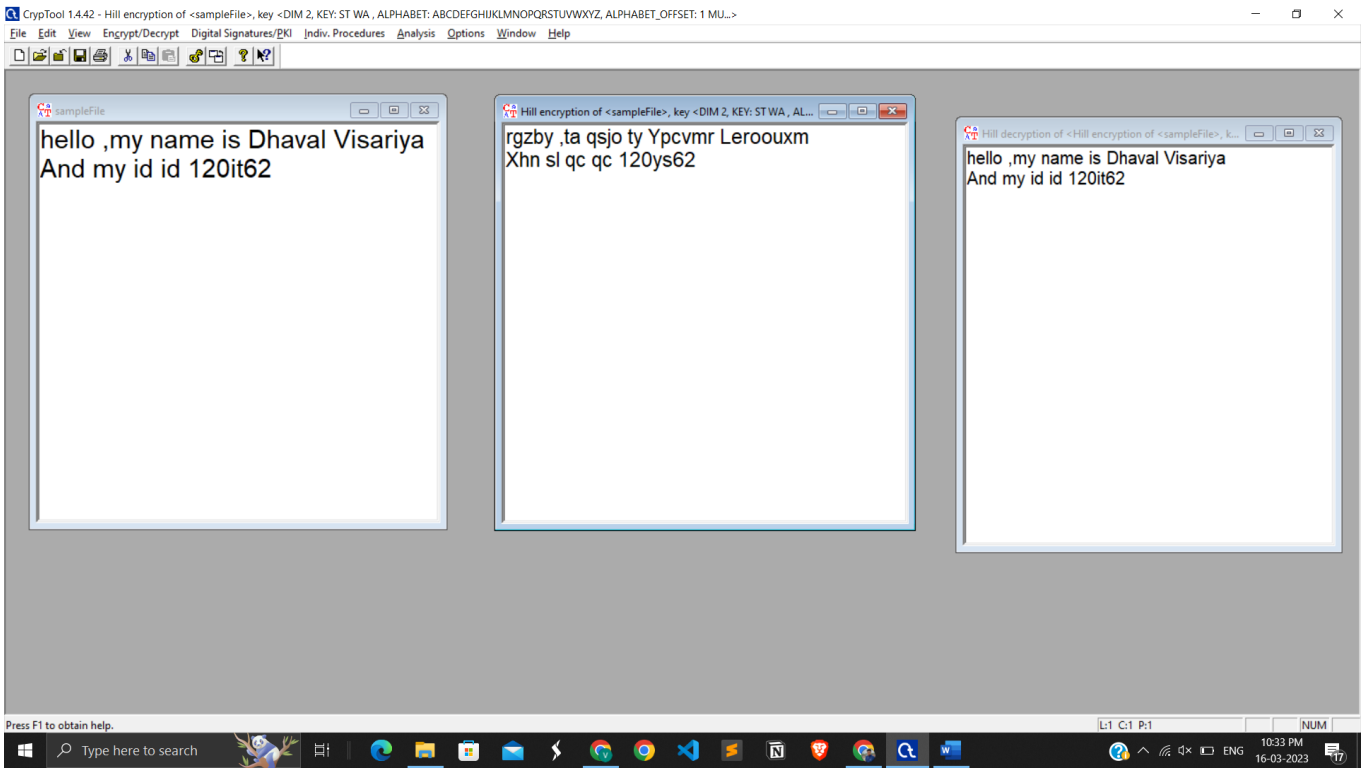
Entered a key for Vigenere



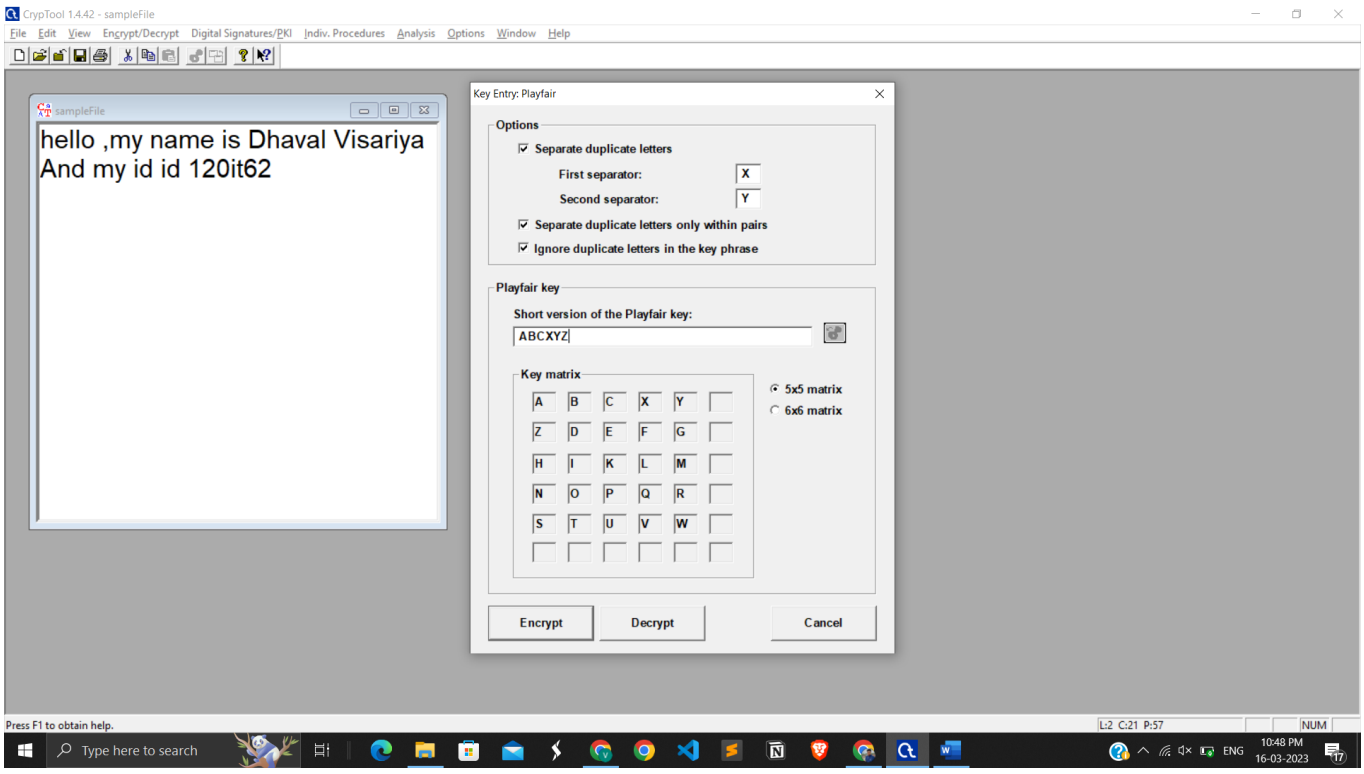
Encryption and Description of Vigenere



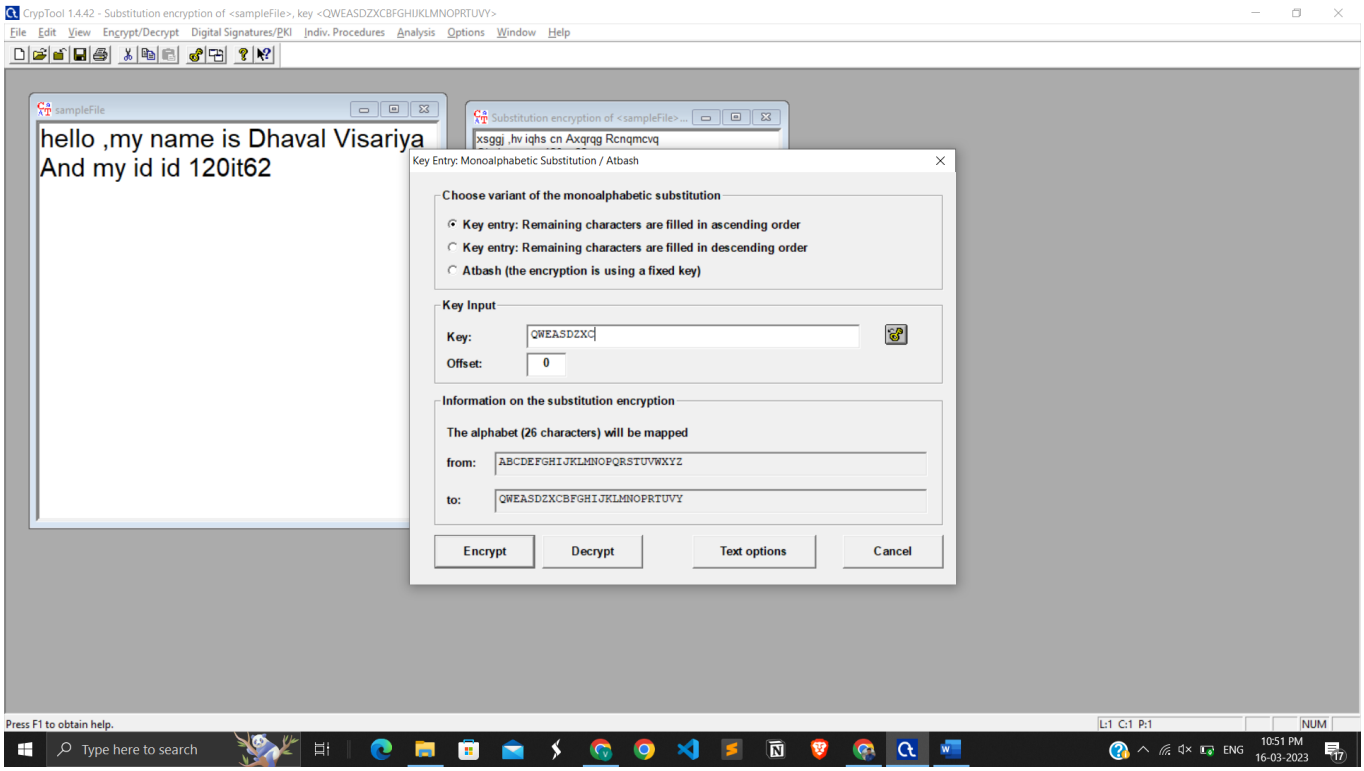
Encrypt a hill cipher using this key



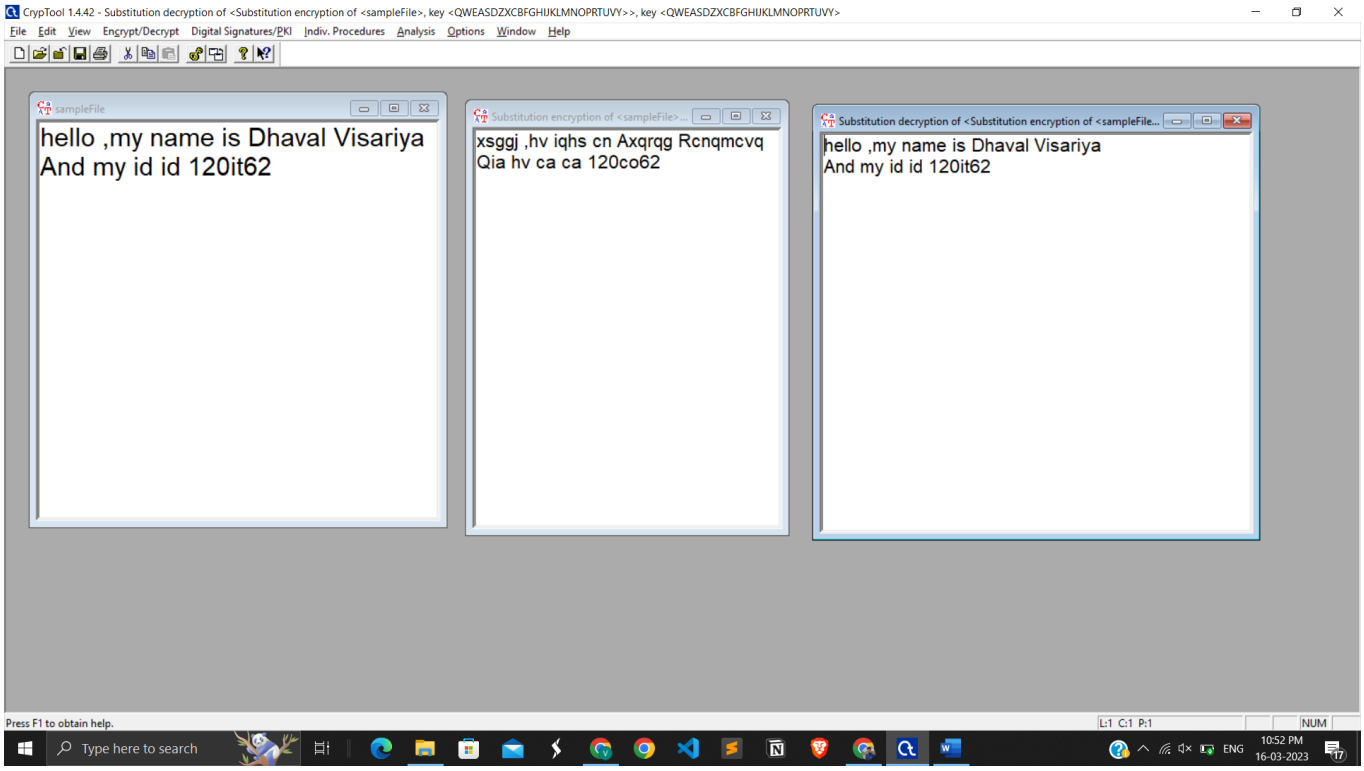
Encryption and decryption using Hill cipher.



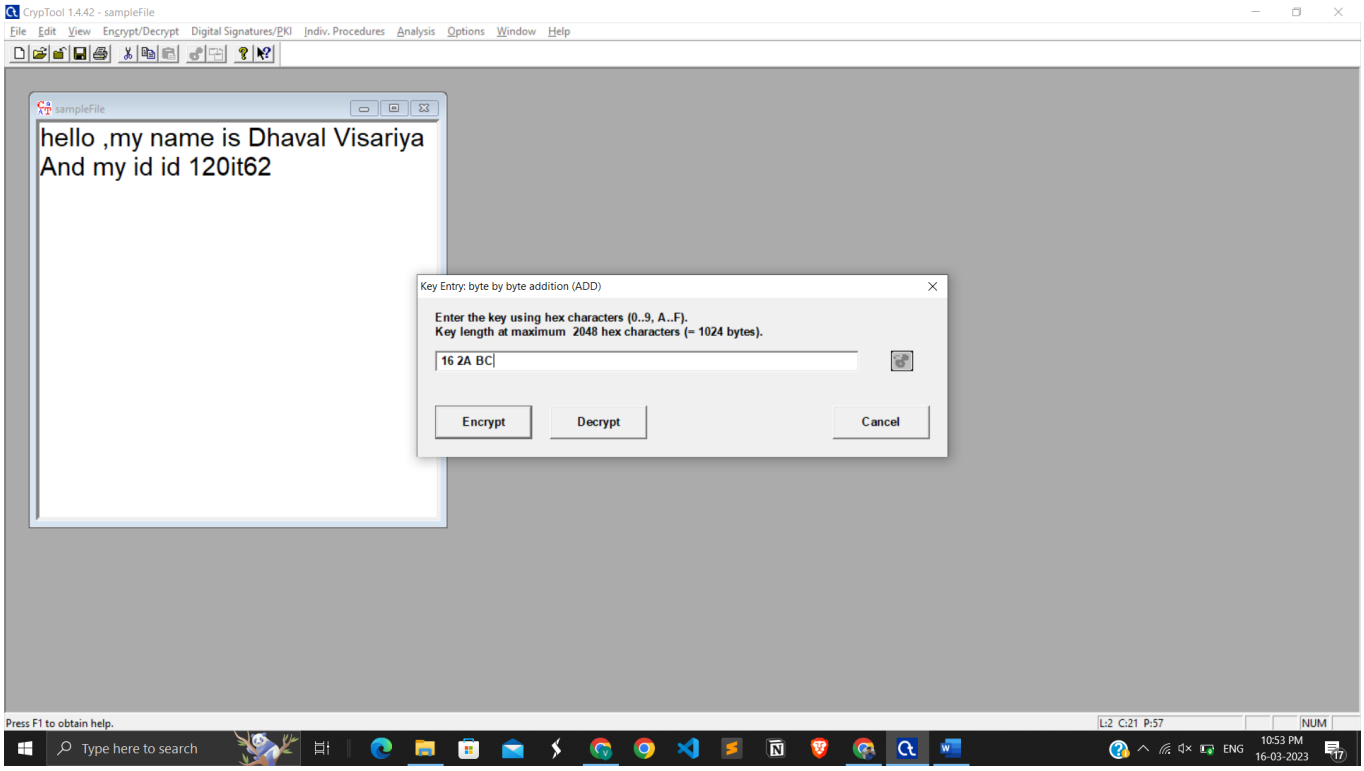
Encrypt using Playfair and entered a key also



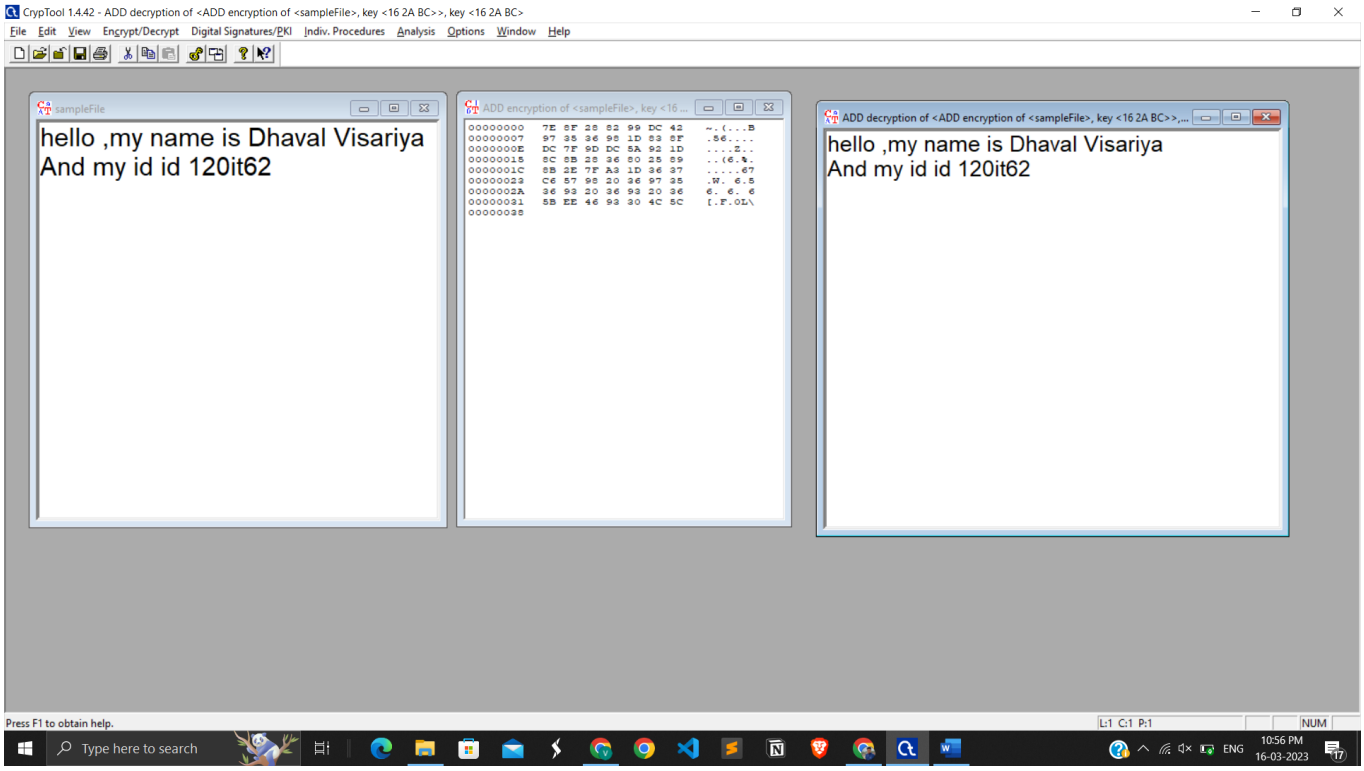
Encrypt using Substitution and entered a key



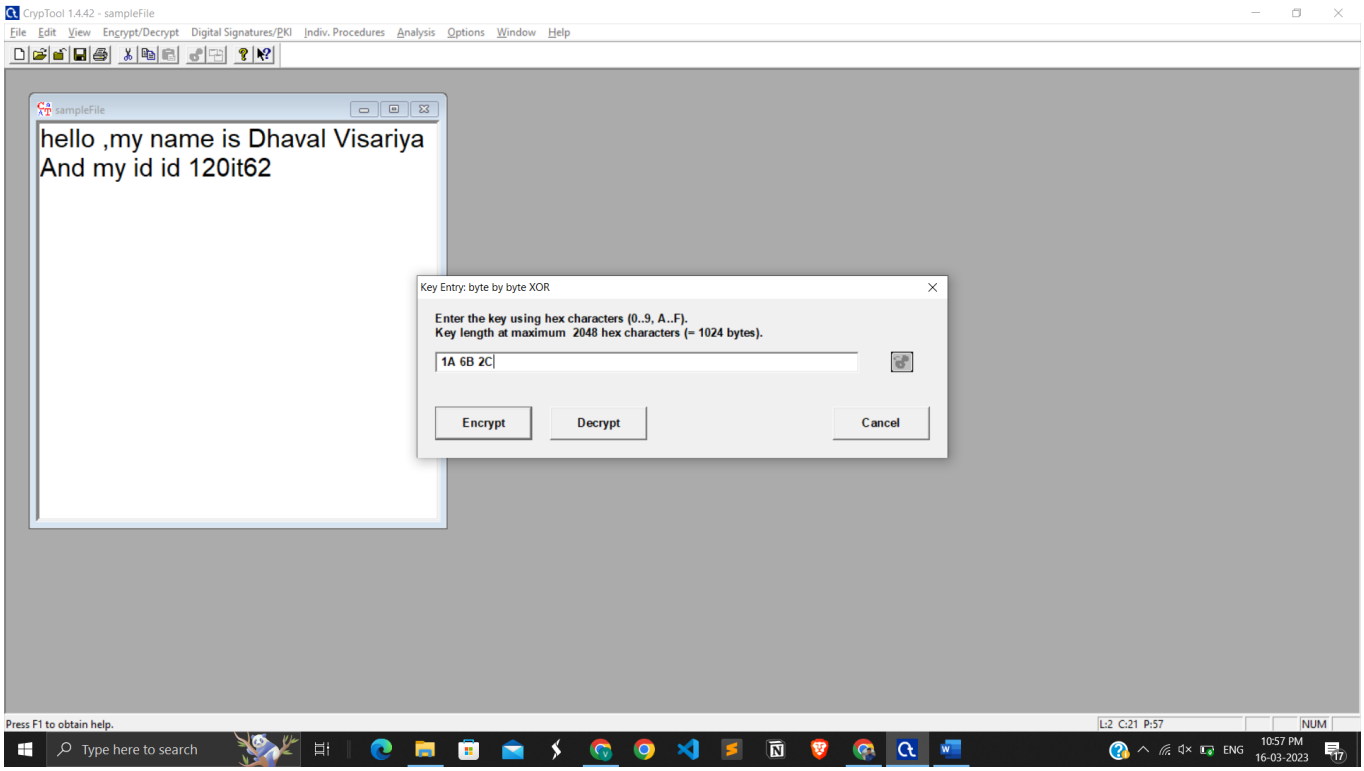
Encrypted and decrypted a file using Substitution method



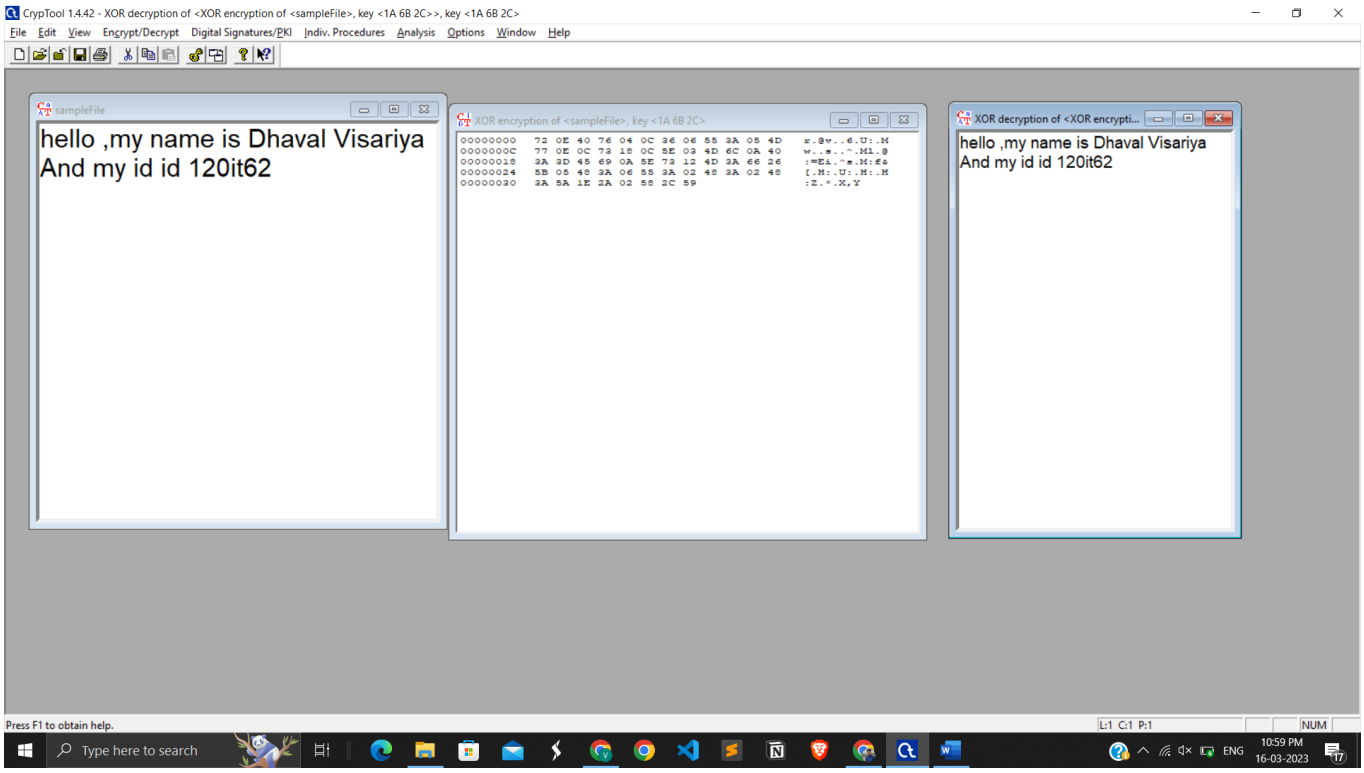
Encrypt using byte addition and key



Encrypted and Decrypted



Encrypt using byte by byte XOR



Message is properly generating

LATEST APPLICATIONS:

- CrypTool is used in schools, universities, companies and agencies for education and awareness training
- Worldwide, the CrypTool packages are downloaded more than 10,000 times per month from the CrypTool website. Just over 50% of the downloads are for the English version.
- The CrypTool project also includes the website CrypTool-Online, launched in 2009. This website allows users to try cryptographic methods directly within a browser on a PC or on a smartphone (using JavaScript), without the need to download and install software. This site aims to present the topic in an easy and attractive way for new users and young people.Advanced tasks still require the offline versions of CrypTool.

LEARNING OUTCOME:

Through this practical I learnt about a highly useful yet simple to use tool to analyze different algorithms available for encryption and decryption. Through this practical I could visualize the difference in the cipher texts produced by different algorithms even when same input is given.

REFERENCES:

1. CrypTool: https://en.wikipedia.org/wiki/CrypTool
2. CrypTool download: https://www.cryptool.org/en/ct2/downloads
3. Caesar cipher: https://www.google.com/search?q=caesar+cipher&rlz=1C1UEAD_en
4. CrypTool latest applications: https://en.wikipedia.org/wiki/CrypTool