Experiment 11

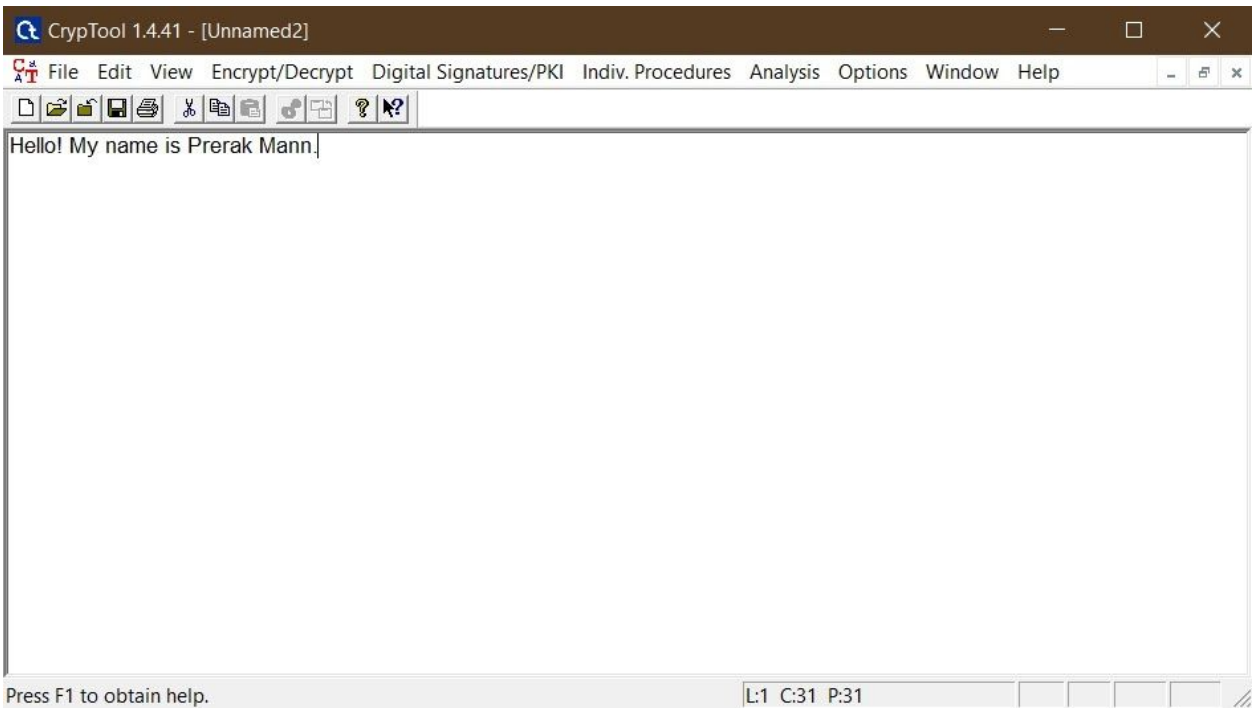
Aim: Perform various encryption-decryption techniques with cryptool.

Theory: CrypTool is an open-source windows program that focuses on the free e-learning software CrypTool 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 their 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.

Output:

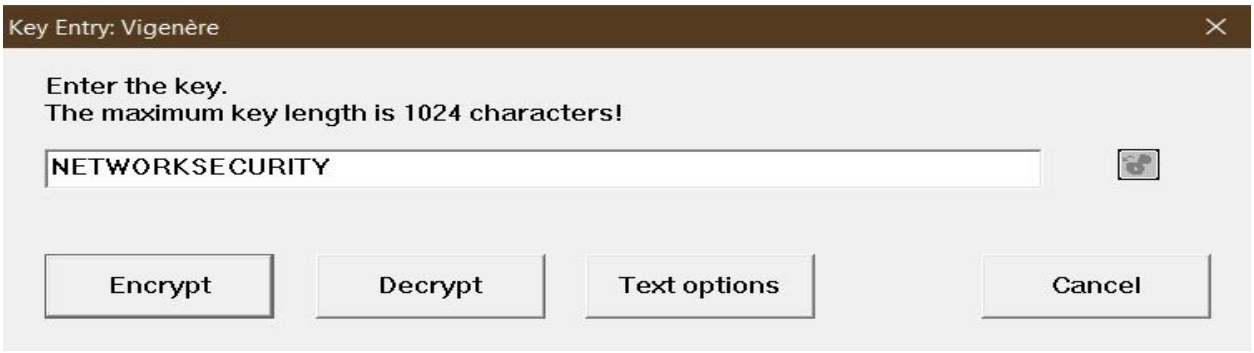
Plain Text



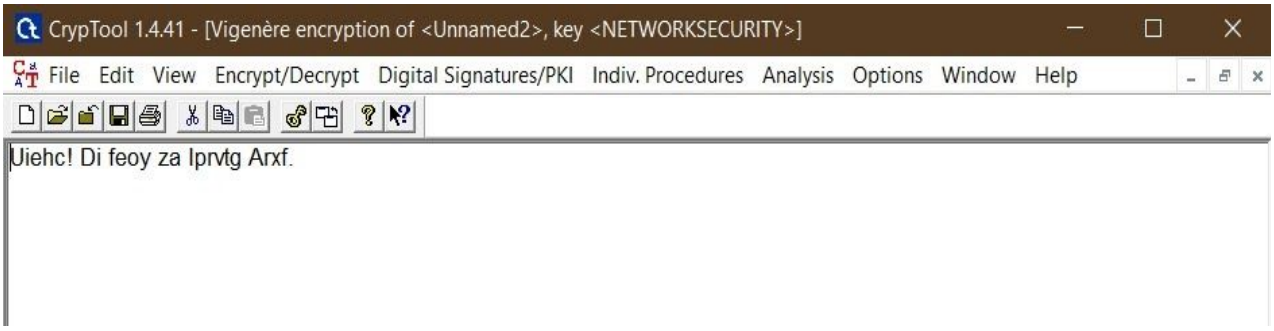
Vigenere Cipher

To facilitate encryption, all the alphabets are usually written out in a large table, traditionally called a tableau. Usually the tableau is 26 × 26, so that 26 full ciphertext alphabets are available. The method of filling the tableau, and of choosing which alphabet to use next, defines the particular polyalphabetic cipher. All such ciphers are easier to break than were believed since the substitution alphabets are repeated for sufficiently large plaintexts.

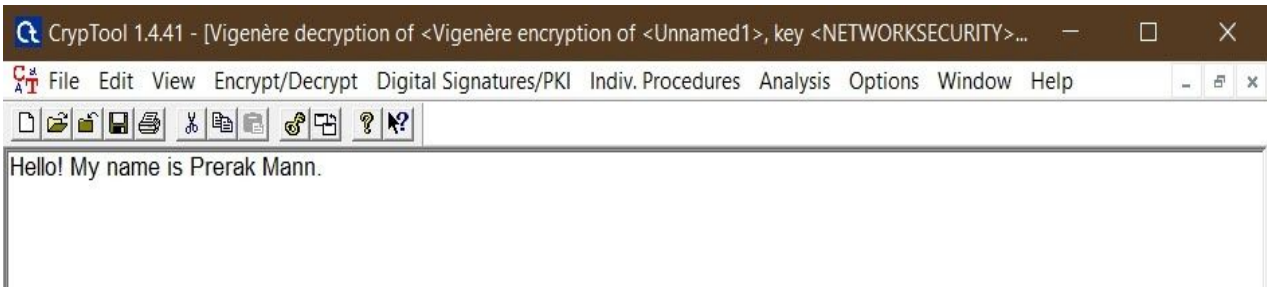
Key



Encryption



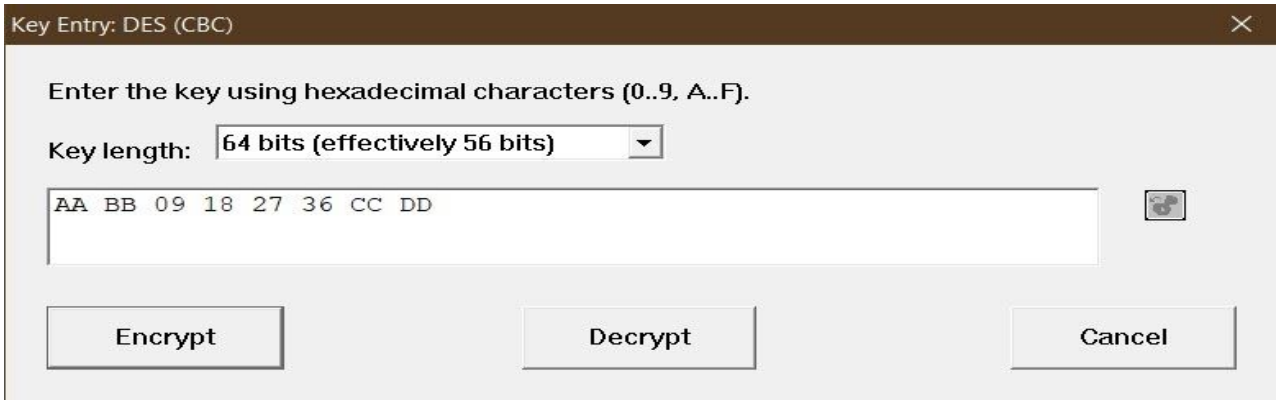
Decryption



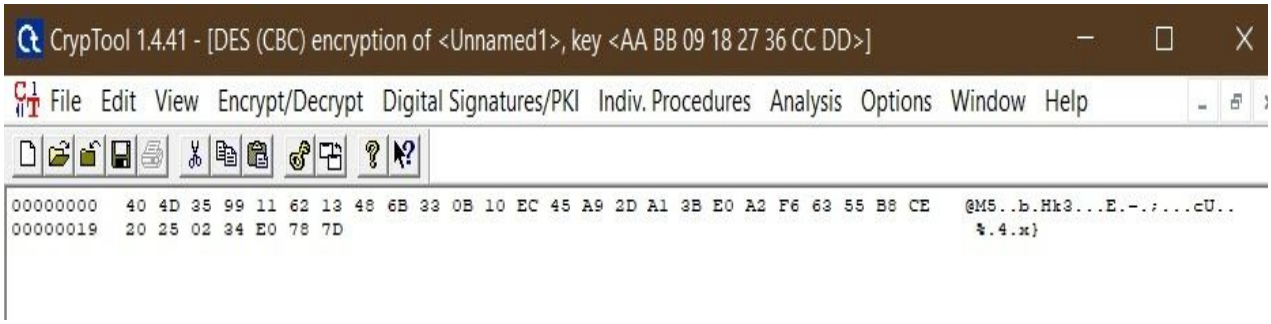
DES

Simplified-DES The S-DES encryption algorithm takes an 8-bit block of plaintext (example: 10111101) and a 10-bit key as input and produces an 8-bit block of ciphertext as output. The S-DES decryption algorithm takes an 8-bit block of ciphertext and the same 10-bit key used to produce that ciphertext as input and produces the original 8-bit block of plaintext.

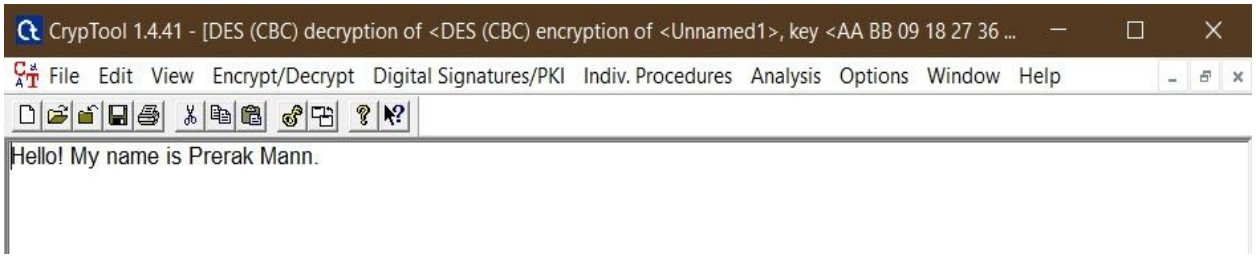
Key



Encryption



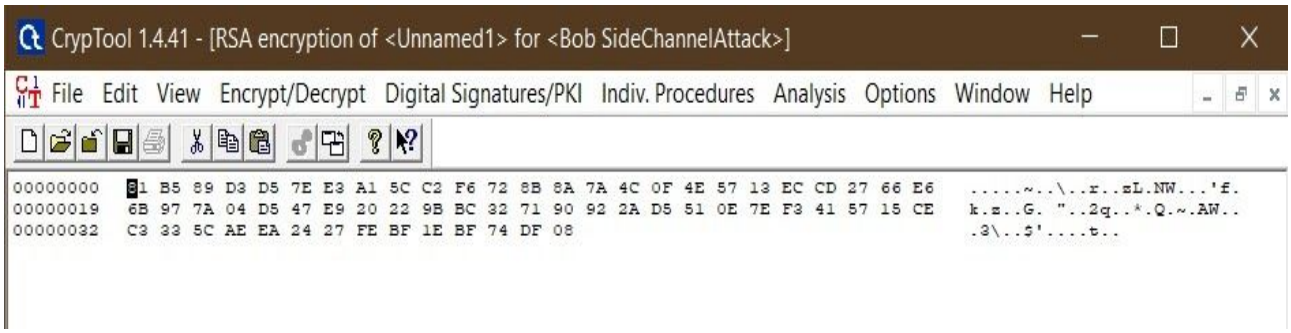
Decryption



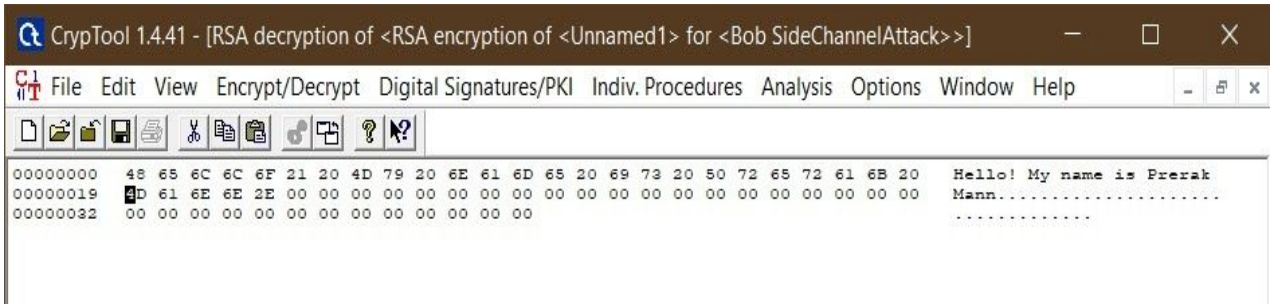
RSA

RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret.

Encryption



Decryption



Learning Outcomes:

Here we have used CrypTool Online to implement 5 different encryption/decryption algorithms - Hill Cipher, Caeser Cipher, AutoKey Cipher, Beaufort Cipher, Rotation Cipher.