Ministerul Educaţiei și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică

Laboratory work 3:
Cryptography and Security

Elaborated:
st. gr. FAF-211 Echim Mihail

Verified:
asist. univ. Aureliu ZGUREANU

Chişinău - 2023

CRYPTOGRAPHY AND SECURITY

Subject: Cryptanalysis of monoalphabetic ciphers

Tasks: De implementat algoritmul Vigenere în unul din limbajele de programare pentru mesaje în limba română (31 de litere), acestea fiind codificate cu numerele 0, 1, ... 30. Valorile caracterelor textului sunt cuprinse între 'A' și 'Z', 'a' și 'z' și nu sunt premise alte valori. În cazul în care utilizatorul introduce alte valori - i se va sugera diapazonul corect al caracterelor. Lungimea cheii nu trebuie să fie mai mică de 7. Criptarea și decriptarea se va realiza în conformitate cu formulele din modelul matematic prezentat mai sus. În mesaj mai întâi trebuie eliminate spațiile, apoi toate literele se vor transforma în majuscule. Utilizatorul va putea alege operația - criptare sau decriptare, va putea introduce cheia, mesajul sau criptograma și va obține criptograma sau mesajul decriptat.

Introduction:
Cryptography is a fundamental aspect of information security, and historical ciphers such as the Vigenère cipher and the Playfair cipher have played significant roles in the development of modern encryption techniques. In this project, we implemented the Vigenère cipher in Python for the Romanian alphabet, providing a user-friendly script for encryption and decryption purposes. Additionally, we included a section that introduces the Playfair cipher, highlighting its unique characteristics and application in cryptography.

Vigenère Cipher:
The Vigenère cipher, developed by Giovan Battista Bellaso in the 16th century and later popularized by Blaise de Vigenère, is a polyalphabetic substitution cipher that improves upon the Caesar cipher's security. It involves using a keyword to encrypt and decrypt messages, with each letter of the plaintext being shifted differently based on the letters of the keyword. This variation in shifting provides a higher level of security compared to simple substitution ciphers.

Playfair Cipher:
The Playfair cipher, invented by Charles Wheatstone in 1854, is a digraph substitution cipher that encrypts pairs of letters rather than single letters. It operates by creating a 5x5 grid containing a key that determines the placement of letters. The key excludes repeating letters and typically omits the letter "J." During encryption, each pair of letters is mapped to specific rules based on their positions within the grid. The Playfair cipher is known for its simplicity and effectiveness in encrypting large volumes of text.

Implementation Details:
The Python script was developed to specifically handle the Vigenère cipher for the Romanian alphabet. It includes various functions to support the encryption and decryption processes, ensuring the security and integrity of the encrypted messages. The script's user-friendly interface and input validation mechanism contribute to a seamless and secure user experience.

Usage:
The script's interface allows users to choose between encryption and decryption, input plaintext or ciphertext, and specify the encryption or decryption key. Users are guided to input valid characters from the Romanian alphabet, thus ensuring the accuracy and security of the encryption and decryption processes.

Results and Discussion:
Through the implementation of the Vigenère cipher for the Romanian alphabet, the script successfully encrypts and decrypts messages while maintaining user-friendliness and security. The explanation of the Playfair cipher provides a broader context for understanding classical encryption techniques, highlighting its unique features compared to the Vigenère cipher. The script's adaptability to both uppercase and lowercase characters further enhances its practicality and usability.

Conclusion:
The implementation of the Vigenère cipher for the Romanian alphabet in Python, along with the introduction to the Playfair cipher, underscores the importance of classical encryption techniques in modern cryptography. The script's robustness, security features, and user-friendly design make it a valuable tool for individuals and organizations seeking to secure their communications and data.

References:
1. The Vigenère Cipher - Wikipedia. Available at: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher.
2. The Playfair Cipher - Wikipedia. Available at: https://en.wikipedia.org/wiki/Playfair_cipher.

Appendix:
The full code can be found here