MINISTRY OF EDUCATION, CULTURE AND RESEARCH OF REPUBLIC OF MOLDOVA
TECHNICAL UNIVERSITY OF MOLDOVA
FACULTY OF COMPUTERS, INFORMATICS AND MICROELECTRONICS
DEPARTMENT OF SOFTWARE ENGINEERING AND AUTOMATICS

Criptography and Security

Laboratory work 3: Polialphabetical Chiper

Elaborated:
st.gr. FAF-211 Nistor Stefan
Verified:
asist.univ. Cătălin Mîțu

Chișinău, 2023

Playfair cipher

Historical Context

The Playfair cipher, invented in 1854 by British scientist Sir Charles Wheatstone, was notably popularized by Lord Lyon Playfair, lending the cipher its name. Distinct from simple substitution ciphers, Playfair employs a 5x5 grid of letters to encrypt digraphs (pairs of letters) in the plaintext, making it significantly harder to decrypt without knowledge of the key. This encryption method was revolutionary for its time and was adopted by the British military during the 19th and early 20th centuries, particularly in World War I, due to its efficacy and relative simplicity in manual encryption and decryption.

Mechanism of the Playfair Cipher

The Playfair cipher operates using a 5x5 grid, filled with letters of the alphabet (with the letter 'J' typically omitted and replaced by 'I'). To create this grid, a keyword or phrase (with duplicates removed) is chosen and entered into the grid first, with remaining spaces filled by the other letters of the alphabet in order. During encryption, the plaintext is divided into digraphs (pairs of letters). If both letters of a digraph are in the same row, each is replaced by the letter to its immediate right (or left for decryption). If in the same column, they are replaced by the letter immediately below (or above for decryption). If they form the corners of a rectangle, they are replaced by the letters on the same row but at the opposite corner. If a pair has the same letter, a filler like 'X' is inserted. This method of pairing and substituting letters provides the cipher its robustness against frequency analysis.

Encryption Process

Grid Creation:

1. Choose a keyword or phrase (without any repeating letters).
2. Write it into a 5×5 grid.
3. Fill the remaining spaces with the rest of the alphabet in order. Combine the letters 'I' and 'J' to fit into one cell.

Preparation of Plaintext:

1. Divide the plaintext message into digraphs (pairs of letters).
2. If a pair has the same letter, insert a filler like 'X' between them and consider the repeated letter in the next digraph.
3. If the plaintext has an odd number of letters, add a filler at the end.

Encryption of Digraphs:

1. If both letters of a digraph are in the same row:
    - Replace each letter with the one immediately to its right. Wrap around to the start of the row if

necessary.

2. If both letters are in the same column:
    - Replace each letter with the one immediately below it. Wrap around to the top of the column if necessary.
3. If the letters form the corners of a rectangle:
    - Replace each letter with the one in the same row but at the opposite horizontal corner of the rectangle.

Implementation

Task 3.2

Implement the Playfair algorithm in Python for messages in the Romanian language (31 letters). The character values of the text are between 'A' and 'Z', 'a' and 'z', and no other values are allowed. If the user enters other values, they will be suggested the correct range of characters. The length of the key must not be less than 7. The user will be able to choose the operation - encryption or decryption, can enter the key, the message or the cryptogram, and will get the cryptogram or the decrypted message. The final phase of adding new spaces, depending on the language used and the logic of the message, will be done manually.

Section 1: Definitions and Initializations

The create matrix function begins by initializing a modified Romanian alphabet, containing 30 unique characters after replacing 'J' with 'I'. This predefined set of characters is utilized throughout the program, especially during the construction of the Playfair matrix and subsequent encryption and decryption processes.

Section 2: Matrix Construction

The function create matrix takes a keyword and constructs the Playfair matrix. It starts with the given keyword, ensuring no repeated characters and that 'J' is replaced with 'I'. Then, the matrix is populated with the remaining characters from the modified Romanian alphabet. The resulting matrix contains rows of 6 characters each, with the total number of rows depending on the length of the combined set of characters.

Section 3: Character Positioning

The find position function is introduced to locate the row and column index of a specific character within the Playfair matrix. This function is instrumental in the encryption and decryption stages to determine how pairs of characters are transformed.

Section 4: Playfair Encryption

The encrypt pair function processes pairs of characters, determining their encrypted counterparts. It examines the relative positions of the characters in the matrix and applies the Playfair rules for characters in the same row, the same column, or in different rows and columns.

Section 5: Playfair Decryption

Similarly, the decrypt pair function takes pairs of encrypted characters and deciphers them using the Playfair rules. It reverses the transformations made during the encryption process to retrieve the original character pairs.

Section 6: Cipher Implementation

The playfair cipher function serves as the main gateway for executing the Playfair encryption or decryption. It prepares the input text, breaking it into character pairs and applying either the encryption or decryption process depending on the mode specified. For encryption, it also ensures that the input text has an even number of characters, appending an ’X’ if necessary.

Section 7: User Interaction

The main execution segment of the program invites users to choose between encryption and decryption. Depending on the user’s choice, they are prompted to provide a key and either a plaintext (for encryption) or a ciphertext (for decryption). The corresponding function is then invoked, and the result is displayed to the user. If an unrecognized option is chosen, an error message is displayed.

[https://github.com/StefanNistor69/Criptography/tree/main/lab3]

Below is a screenshot displaying the output generated by the implemented Playfair cipher code.

```
Choose the operation (encryption/decryption): decryption
Enter the key (at least 7 characters long): criptography
Enter the cryptogram to decrypt: GKMMDÂ
Decrypted message: HELLOX

Process finished with exit code 0
```

Task 3.2

```
Choose the operation (encryption/decryption): encryption
Enter the key (at least 7 characters long): criptography
Enter the message to encrypt: hello
[['C', 'R', 'I', 'P', 'T', 'O'], ['G', 'A', 'H', 'Y', 'B', 'D'], ['E', 'F', 'K', 'L', 'M', 'N'], ['Q', 'S', 'U', 'V', 'W', 'X'], ['Z', 'Ș', 'Ț', 'Ă', 'Î', 'Â']]
[['C', 'R', 'I', 'P', 'T', 'O'], ['G', 'A', 'H', 'Y', 'B', 'D'], ['E', 'F', 'K', 'L', 'M', 'N'], ['Q', 'S', 'U', 'V', 'W', 'X'], ['Z', 'Ș', 'Ț', 'Ă', 'Î', 'Â']]
[['C', 'R', 'I', 'P', 'T', 'O'], ['G', 'A', 'H', 'Y', 'B', 'D'], ['E', 'F', 'K', 'L', 'M', 'N'], ['Q', 'S', 'U', 'V', 'W', 'X'], ['Z', 'Ș', 'Ț', 'Ă', 'Î', 'Â']]
Encrypted message: GKMMDÂ
```

Task 3.2

Conclusion

The Playfair cipher, a classical method of encryption, has been adeptly implemented in the presented code to accommodate the nuances of the Romanian alphabet. By constructing a matrix-based framework, this implementation ensures that the encryption and decryption processes are both intricate and systematic, offering a more robust security measure than simple monoalphabetic ciphers. With its matrix foundation and the Playfair rules for character transformation, the cipher exhibits unique properties: pairs of characters undergo specific transformations depending on their relative positions within the matrix.

The presented code stands out not only for its core encryption functionality but also for the importance it places on input validation, matrix construction, and user interaction. The seamless integration of these components offers users a comprehensive tool for encrypting and decrypting messages while preserving the integrity of the original text and ensuring its confidentiality.

In an age where digital security has never been more paramount, revisiting and understanding classical encryption methods like the Playfair cipher provides valuable insights. These methods, though antiquated, form the foundational knowledge upon which modern cryptographic algorithms are built. The presented implementation is a testament to the versatility and timeless appeal of the Playfair cipher, masterfully adapted to the Romanian context.