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

Laboratory work 4: Cryptography and Security

Elaborated:
st. gr. FAF-211 Echim Mihail

Verified:
asist. univ. Aureliu ZGUREANU

Chişinău - 2023

CRYPTOGRAPHY AND SECURITY

Subject: Block cipher. DES Algorithm

Tasks: Given the key of the DES algorithm (8 symbols), determine K+

Introduction:
The following report provides an implementation of a Python script that converts an 8-symbol DES key to its respective 64-bit key representation, including the necessary parity bits. Additionally, the report provides an overview of the Data Encryption Standard (DES) algorithm and an explanation of why keys in DES work the way they do.

About DES:
The Data Encryption Standard (DES) is a symmetric-key block cipher that was widely used for secure data transmission and encryption. It operates on 64-bit blocks using a 56-bit key. The algorithm involves multiple rounds of permutation, substitution, and transposition to provide encryption and decryption functionality. Although DES has been largely replaced by more secure algorithms, it played a significant role in the history of cryptography and encryption.

DES Key Structure:
The DES key structure comprises 64 bits, where 56 bits are used for encryption and 8 bits are used for parity checking. The parity bits ensure that each 7-bit segment of the key contains an odd or even number of '1' bits. This structure aids in the detection of errors and helps maintain the integrity of the key during the encryption and decryption processes.

Implementation:
For the implementation, a Python script was developed to convert an 8-symbol DES key into a 64-bit key. The script first converts each symbol of the key into its binary representation and then calculates the parity bit for each 7-bit segment. The resulting 64-bit key includes the necessary parity bits, ensuring the correctness and integrity of the key.

Conclusion
The provided Python script serves as a practical implementation of the conversion of an 8-symbol DES key to its corresponding 64-bit key representation, including the necessary parity bits. Understanding the structure of DES keys and the rationale behind their design is essential in comprehending the inner workings of the DES encryption algorithm and its key management.

Appendix:
The full code can be found here