Data Encryption Standard

- Implement DES with Rust and Linear Analysis -

Ji Yong-Hyeon

Department of Information Security, Cryptology, and Mathematics
College of Science and Technology
Kookmin University

March 7, 2024

Acknowledgements

Contents

Chapter 1

Data Encryption Standard

- Symmetric Block Cipher.
- A.k.a Data Encryption Algorithm.
- Adopted by NIST in 1977.
- Advanced Encryption Standard (AES) in 2001.

Table 1.1: Parameters of the Block Cipher DES

Input	Output	Master Key	Sub-key	Round Key	No. of rounds
64-bit	64-bit	64-bit	56-bit	48-bit	16 rounds

1.1 Key Schedule