University of Babylon

,College of Information Technology

Department of Information Security

Study: morning

"Implementation of symmetric key cryptography algorithm"

Research submitted to the Council of the University of Babylon

Faculty of Information Technology

As part of the undergraduate degree requirements

In the Information Security Department

student preparation:

Ahmed Aqeel Rashid

Supervisor:

Assistant.Lecturer Farah Alaa Abdul-Hassan

2023-2024

Abstract

Cryptography is a field that deals with the secure communication and protection of information in the presence of adversaries. It involves the use of mathematical algorithms and techniques to transform plaintext into ciphertext, making it unintelligible to unauthorized individuals. Cryptography plays a crucial role in ensuring confidentiality, integrity, authenticity, and non-repudiation of data in various applications, such as online transactions, secure communication networks, and data storage systems.

The abstract nature of cryptography lies in its ability to provide secure communication and data protection without relying on the physical security of the underlying infrastructure. It allows parties to securely exchange information over insecure channels by employing encryption and decryption algorithms. Encryption involves the process of converting plaintext into ciphertext using a cryptographic key, while decryption reverses this process, transforming ciphertext back into its original form. The strength of a cryptographic system lies in the complexity of the algorithms used and the secrecy of the cryptographic keys.

Modern cryptography encompasses several subfields, including symmetric key cryptography, asymmetric key cryptography, and cryptographic protocols. Symmetric key cryptography employs a single shared secret key for both encryption and decryption. It is typically faster and more efficient but requires secure key distribution among communicating parties. Asymmetric key cryptography, on the other hand, uses pairs of public and private keys. The public key is widely distributed and used for encryption, while the private key is keptsecret and used for decryption. This approach overcomes the key distribution challenge but is computationally more expensive.