Project Report: Cryptography Implementation with CRYPTON, RSA, and Rabin

**Amit Benita 315949594  
Guy Edri 315730374  
Maxim Lazarenko 324314590  
Emanuel Elkobi 212722722**

This project implements a comprehensive cryptographic system combining three different encryption algorithms: CRYPTON, RSA (Rivest-Shamir-Adleman), and Rabin Signature. The system provides secure communication through symmetric and asymmetric encryption, digital signatures, and message verification.

**The project involved studying and implementing the following cryptographic components:**

1) CRYPTON:

* A symmetric block cipher algorithm.
* Implements key scheduling, encryption, and decryption functions.
* Uses substitution-permutation network (SPN) structure.

2) RSA:

* An asymmetric encryption algorithm.
* Implements key generation, encryption, and decryption functions.
* Used for secure key exchange.

3) Rabin:

* Asymmetric cryptosystem.
* Implements key generation, signing, and verification functions.
* Provides an alternative method for digital signatures.

**Project Flow: The project follows these main steps:**

1) CRYPTON Implementation:

* Key setup and generation of S-boxes and round constants.
* Implementation of encryption and decryption functions.
* Conversion between text and block representations.

b) RSA Implementation:

* Generation of prime numbers and key pairs.
* Encryption and decryption functions.

c) Rabin Implementation:

* Key pair generation.
* Signature generation and verification functions.

d) Integration:

* Combining CRYPTON for message encryption.
* Using RSA for key encryption.
* Applying Rabin for message signing and verification.

**Obtained Results:**

The project successfully implemented and integrated the three cryptographic algorithms. The main results include:

* Secure message encryption using CRYPTON.
* Secure key exchange using RSA.
* Message integrity and authentication using Rabin signatures

**Security Considerations: The project implements several security measures:**

* Use of random prime number generation for RSA and Rabin.
* Implementation of modular arithmetic for RSA and Rabin operations.
* Use of S-boxes and round constants in CRYPTON for diffusion and confusion

**Conclusions**

This project successfully demonstrates the implementation and integration of multiple cryptographic algorithms to provide a comprehensive secure communication system.  
The project showcases the practical application of cryptographic principles and provides a foundation for further development and enhancement of secure communication systems.

Some of the conclusions we discovered are:

* The use of both RSA and Rabin Signature algorithms can be used in conjunction to enhance the overall security framework.
* The key management is extremely important to maintain the whole system’s security.
* Even though both algorithms are considered very secure today, they face potential vulnerabilities from quantum computers.
* The design of CRYPTON emphasizes strong security features. The multiple rounds, carefully constructed S-boxes, and robust key schedule provide a high level of resistance to cryptanalytic attacks, including differential and linear cryptanalysis.