Full-Time-Pad
Symmetric Stream Cipher

Improved One-Time-Pad Encryption Scheme

Taha Canturk
`kibnakanoto@protonmail.com`

2024-05-20

`Version 1.0`

License to copy this document is granted provided it is identified as ”Full-Time-Pad”,
in all material mentioning or referencing it.

Abstract

Abstract

Contents

1 Introduction **2**

1.1 Pre-requisite Terminology . . . 2

1.2 Applications . . . 2

1.3 Key Generation . . . 2

1.4 Prerequisite Mathematics . . . 2

1.5 Vector Permutation . . . 2

2 Security Vulnerabilities **2**

2.1 Brute-Force . . . 2

2.1.1 Birthday Attack . . . 2

2.1.2 Denial of Service (DoS) . . . 2

2.2 Reverse Engineering the Transformation . . . 2

2.3 Collision-Resistance . . . 2

2.3.1 Different Permutation Matrices . . . 2

2.3.2 Number of Rounds . . . 2

2.3.3 Constant - F_p - Prime Galois Field Size . . . 2

2.3.4 Constant - r - Dynamic Rotation Constant . . . 2

3 Hashing **2**

3.1 Diffusion - Permutation . . . 2

3.1.1 Vector Permutation . . . 2

3.1.2 Dynamic vs. Static . . . 2

3.2 Dynamic Matrix Permutation . . . 2

3.2.1 Deravation . . . 2

3.2.2 Other Options . . . 2

3.3 Confusion - ARX . . . 2

3.3.1 A - Modular Addition . . . 2

3.3.2 R - Bitwise Rotation . . . 2

3.3.3 X - XOR . . . 2

3.4 Key Transformation . . . 2

4 Cipher **2**

4.1 Transformation . . . 2

4.2 Avalanche Effect - Plaintext . . . 2

4.2.1 Encryption Index . . . 2

4.3 Long Plaintexts . . . 2

1 Introduction

1.1 Pre-requisite Terminology

1.2 Applications

1.3 Key Generation

1.4 Prerequisite Mathematics

1.5 Vector Permutation

2 Security Vulnerabilities

2.1 Brute-Force

2.1.1 Birthday Attack

2.1.2 Denial of Service (DoS)

2.2 Reverse Engineering the Transformation

2.3 Collision-Resistance

2.3.1 Different Permutation Matrices

2.3.2 Number of Rounds

2.3.3 Constant - F_p - Prime Galois Field Size

2.3.4 Constant - r - Dynamic Rotation Constant

3 Hashing

3.1 Diffusion - Permutation

3.1.1 Vector Permutation

3.1.2 Dynamic vs. Static

3.2 Dynamic Matrix Permutation

3.2.1 Deravation

3.2.2 Other Options

3.3 Confusion - ARX

3.3.1 A - Modular Addition

3.3.2 R - Bitwise Rotation

3.3.3 X - XOR

3.4 Key Transformation

4 Cipher

4.1 Transformation