Introduction

The Data Encryption Standard (DES) is a symmetric key encryption system that was published by the National Bureau of Standards in 1975. Symmetric key encryption algorithms transform blocks of plaintext into blocks of ciphertext of the same length, which requires a user-provided secret key. Decryption is performed by reversing the transformation using the same key. DES and its variants are commonly used in electronic financial transactions, secure data communications, and the protection of passwords or PIN’s against unauthorized access. DES performs encryption through permutations and targeted substitutions using S-boxes as shown in Figure 1. Substitutions are targeted using a secret key whose use is scheduled over several rounds as shown in Figure 2. This targeting employs a group operation ⊕. All commercial versions of DES have been implemented only over the group $\mathbb{Z}_2$.

Objectives

- Investigate well-publicized problems related to the algebraic structure of DES-like algorithms. This is useful because there is a strong relationship between a cryptosystem’s algebraic properties and its security.
- Implement DES over groups other than $\mathbb{Z}_2$.

Computational Results

We developed a program in Maple to implement S-DES (a simplified version of DES) over $\mathbb{Z}_n$. Then, using Coppersmith’s method and known mathematical results, we proved that S-DES over $\mathbb{Z}_n$ and over $\mathbb{Z}_n \times G$ does not form a group when $G$ is finite and $n$ is divisible by 2, 3, 5, 7, or 11.

Theoretical Results

**Definition**

A DES-like encryption is a function $D : G^{2k} \rightarrow G^{2k}$ with $m$ Feistel rounds.

**Theorem**

Let $G$ be a finite group, and fix $g \in G$. Consider a DES-like encryption over $G$, where each entry in all of the S-boxes is $g$. Then the following are true:

1. The DES-like encryption (over all possible keys) does not form a group under composition.
2. The group generated by the DES-like encryption is a cyclic group of order $\text{lcm}(2, |g|)$.

**Theorem**

Let $G$ be a group such that $|G|$ is odd and $|G|^k \equiv 3 \pmod{4}$, where $k$ is an odd integer. Then the group of substitutions generated by DES is either $S_{G^{2k}}$ or a subgroup $H$ of $S_{G^{2k}}$ such that half of the elements in $H$ are even permutations.

Conclusions

Questions such as “Is DES is a group?” and “What is the group generated by DES?” are crucial for the security of DES [1], but they had previously been solved only for DES over $\mathbb{Z}_2$ [2]. We proved that DES does not form a group over any finite group, which solves the first open problem in general. We also showed that DES over a finite group can generate the alternating group or a subgroup of the symmetric group containing odd permutations, which gives an answer to the second question in general. For educational purposes we designed the first simplified version of DES that encrypts over an elliptic curve group (E-DES).

References


Acknowledgements

Funding for this project was provided by the National Science Foundation under Award DMS 1062857 and by Boise State University.