The DES-like encryption (over all possible
substitutions, secure data communications, and the protection of passwords or PINs 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 ⊕. Many symmetric block ciphers such as DES are based on Luby Rackoff (Feistel) networks. In [3] was shown that 4-round Luby Rackoff cipher gives "strong" security if the round function f is a cryptographically secure pseudorandom function.

**Theoretical Results**

**Definition**

DES is a function \( D : G^{2k} \rightarrow G^{2k} \) with \( m \) Feistel rounds and left-right swaps between each Feistel round.

**Theorem**

Let \( G \) be a finite group, and fix \( g \in G \). Consider DES 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 \( \text{lcm}(2, |g|) \).

**Definition**

A Feistel round is a function \( f_f : G^{2k} \rightarrow G^{2k} \) where \( f_f(x, y) = (x \oplus f(y), y) \).

**Theorem**

\( n \)-round DES over a group of order \( \geq 2 \) does not form a group provided that no round functions \( f_i \) is the constant function returning the identity.

**Theorem**

Let \( G \) be a group with odd order where \( |G|^k \equiv 3 \) mod 4. Then, the group of permutations generated by \( n \)-round DES over \( G \) contains odd permutations.

**Conclusions**

Questions such as "Is DES 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).

**Future Work**

- Investigate which group is generated by E-DES and construct more secure S-boxes.
- Determine the order of the group generated by DES over a finite group \( G \).
- Consider the following problem: If \( n \)-round DES permutations generate a group \( H \), what is the smallest set of DES permutations that generates \( H \)?

**References**


**Acknowledgments**

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