DES Over Finite Groups

Liljana Babinkostova[1], Alyssa Bowden[2], Andrew Kimball[3], and Kameryn Williams[1]

[1]Boise State University, [2]Loyola Marymount University, [3]Western Carolina University

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 $\oplus$. 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.

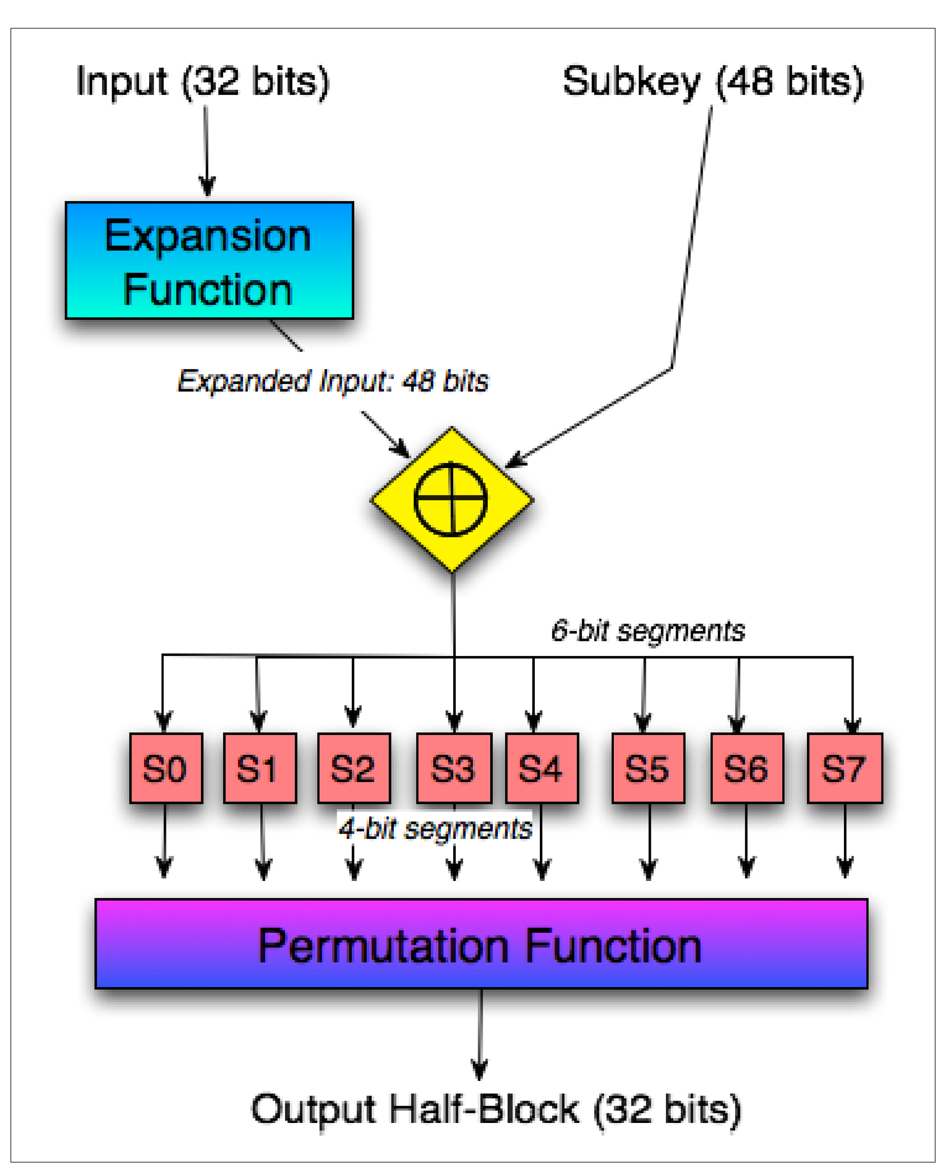

Figure 1: Feistel Round of DES

Objectives

- Investigate well-publicized problems related to the algebraic structure of Feistel-based ciphers such as DES. 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

DES is a function $D : G^{2k} \to G^{2k}$ 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 $\mathrm{lcm}(2, |g|)$.

Definition

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

Theorem

n-round DES over a group of order ≥ 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).

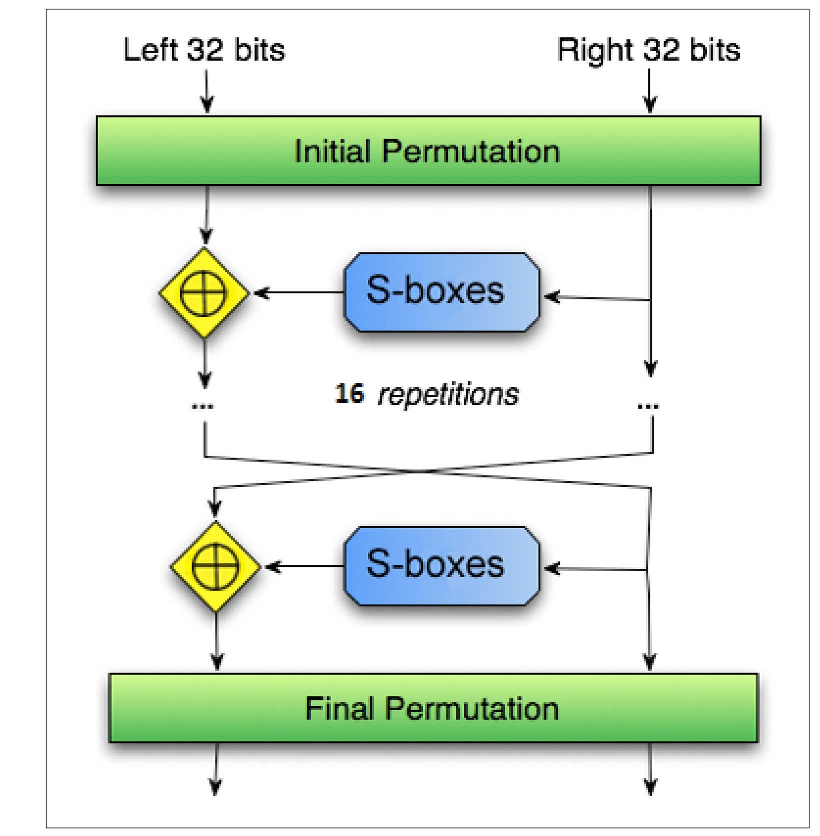

Figure 2: Outline of DES

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

[1] B. S. Kaliski et al., *Is the Data Encryption Standard a Group?*, **J. Cryptology** (1988) 1:3-36.

[2] K. W. Campbell and M.J. Wiener, *DES is not a Group*, **CRYPTO 1992**, 512-520.

[3] M. Luby and C. Rackoff, *How to Construct Pseudorandom Permutations from Pseudorandom Functions*, **SIAM 17** (1988), 373âĂŞ386

Acknowledgments

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