4-21-2014

The Security of Simplified Data Encryption Standard

Brandon Barker
College of Arts and Sciences, Boise State University

The Security of Simplified Data Encryption Standard

Brandon Barker[1] and Liljana Babinkostova[2], Ph.D

[1]Computer Science Department, [2]Department of Mathematics

BOISE STATE UNIVERSITY

Abstract

The Data Encryption Standard (DES) is the most widely used symmetric key cryptosystem in the commercial world. DES was published in 1975 by the National Bureau of Standards, and since then it and its variants have been commonly used. DES is utilized in many modern industries and products including the Blackberry, electronic financial transactions, and access cards to corporate offices. An efficient but secure cryptosystem is challenging to produce and even after it has been deemed "secure" new attacks and vulnerabilities are often discovered. By investigating the algebraic structure of a simplified version of DES we are able to analyze the structure and security of DES used in the commercial world in an attempt to improve and understand its current security and potential threats.

i^{th} Feistel Round in EDES[1]

A new simplified version of DES was introduced in [1] and its structure is presented in **Figure 1**.

- The message is split in the middle creating L_{i-1} and R_{i-1}
- R_{i-1} is applied to the round function f (**Figure 2**)
- The key k_i is applied in the round function f process
- The output of the function f and L_{i-1} are added in $\mathbb{Z}_3$ The resulting data is the new R_i
- The new Li becomes R_{i-1}
- Process is repeated again with k_{i+1} on $[L_i, R_i]$

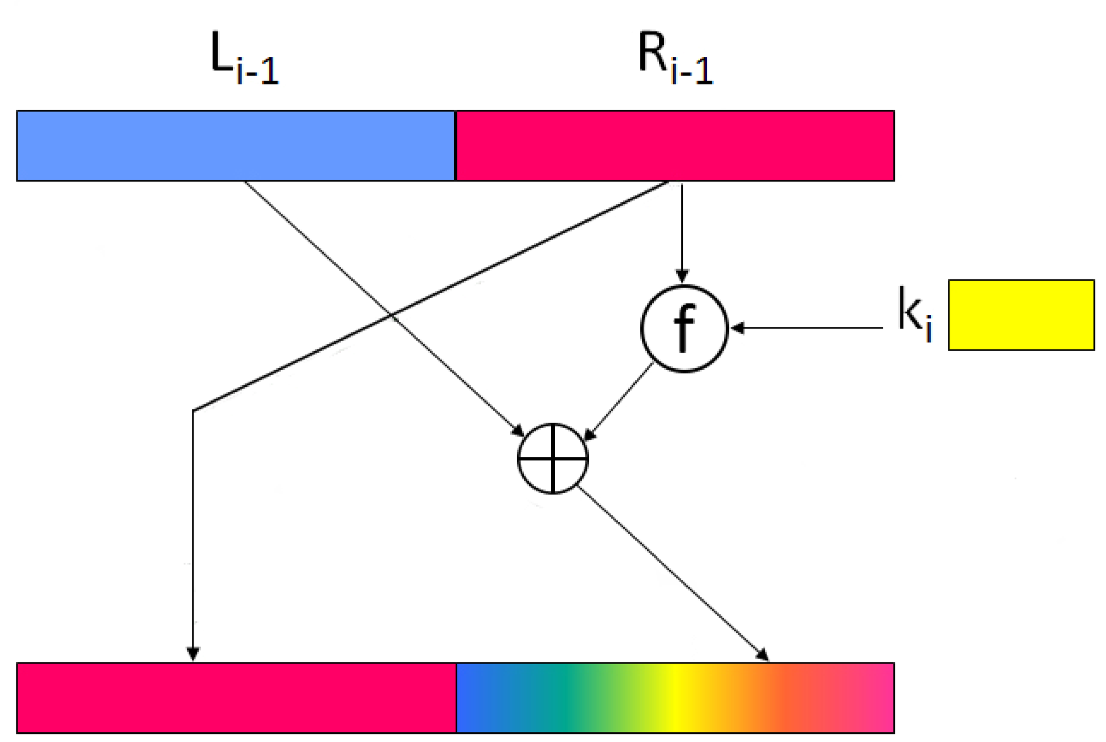

Figure 1. Feistel Round

Mathematical Background

Definition. Let A be a nonempty set. A bijective function f: $A \rightarrow A$ is called a *permutation*.

Definition. The set of all permutations on a set of n elements is called a *symmetric group* and is denoted by S_n.

Theorem. Let A be a finite set with n elements. Then S_n has $n! = (n-1)(n-2) \dots 3 \cdot 2 \cdot 1$ elements.

Example. $\sigma = \begin{pmatrix} 12345678 \\ 34172658 \end{pmatrix} = (13)(2475)(6)(8)$ is a permutation of order LCM(2,4,1)=4.

Definition. Let σ be a permutation written as a product of disjoint cycles of a finite length. The LCM (least common multiple) of the lengths of disjoint cycles is called an *order of the permutation*.

Theorem. The order of a permutation on a set of n elements divides the number of elements in S_n.

Coppersmith Cycling Experiment[2] and New Results

Using Maple and randomly generated messages and keys, we were able to discover various orbit lengths. To find the orbit length, our software would encrypt with the given information repeatedly until it produced the same ciphertext twice. Using these orbit lengths and their least common multiple, we are able to computationally prove the security of the system by increasing the unknown lower bound. The method of finding orbits of encryption permutations defined on randomly chosen messages and keys and the LCD of the lengths of those orbits is called Coppersmith Method[2]. The ideas utilized here are derived from the Coppersmith Method[2].

Original Message	Key 1	Key 2	Orbit Length
[0, 0, 2, 0, 1, 1, 2, 0, 2, 0, 1, 0, 2, 2, 0, 1, 2, 0]	[2, 0, 0, 2, 0, 1, 0, 2, 1, 1, 1, 0, 2, 0, 1, 2, 0, 1, 2, 0]	[0, 2, 1, 1, 2, 0, 2, 0, 1, 2, 2, 0, 1, 2, 2, 1, 0, 0, 0, 2]	132,428,773
[2, 0, 1, 2, 2, 0, 1, 0, 2, 0, 1, 2, 2, 0, 1, 2, 1, 1]	[0, 1, 0, 1, 0, 0, 0, 2, 2, 1, 1, 1, 0, 2, 1, 0, 1, 0, 1, 2]	[1, 2, 2, 1, 1, 0, 1, 1, 2, 1, 0, 2, 2, 1, 2, 1, 2, 1, 2, 0]	14,271,499
[0, 0, 1, 1, 0, 2, 1, 0, 2, 2, 1, 0, 2, 0, 1, 1, 2, 1]	[1, 2, 0, 0, 2, 1, 2, 0, 1, 1, 0, 2, 2, 1, 0, 0, 2, 1, 0, 2]	[2, 0, 0, 0, 1, 0, 1, 1, 2, 0, 1, 0, 1, 0, 2, 0, 1, 1, 1, 0]	14,527,016
[0, 2, 2, 1, 0, 0, 0, 2, 1, 1, 2, 0, 2, 1, 0, 0, 2, 1]	[0, 0, 2, 1, 1, 0, 2, 0, 1, 0, 2, 0, 1, 1, 1, 2, 0, 2, 1, 0]	[1, 2, 2, 1, 1, 0, 2, 1, 0, 2, 0, 1, 0, 2, 2, 2, 2, 1, 2, 0]	146,329,430
[2, 1, 2, 2, 0, 1, 0, 0, 2, 1, 0, 2, 1, 1, 2, 0, 0, 1]	[2, 0, 0, 0, 1, 0, 2, 0, 1, 0, 2, 2, 1, 1, 2, 0, 1, 2, 0, 1]	[0, 2, 0, 1, 0, 1, 0, 2, 0, 1, 0, 1, 1, 0, 2, 0, 1, 0, 2, 0]	147,121,380
[0, 2, 1, 1, 2, 0, 2, 1, 0, 2, 2, 1, 2, 0, 0, 2, 2, 0]	[0, 0, 1, 0, 1, 2, 2, 1, 0, 2, 1, 0, 2, 2, 1, 0, 2, 2, 1, 0]	[2, 0, 1, 1, 0, 2, 0, 1, 0, 2, 0, 1, 1, 1, 2, 0, 0, 2, 1, 0]	262,205,969
[0, 2, 2, 0, 1, 0, 2, 1, 1, 0, 2, 0, 1, 0, 2, 0, 1, 2]	[0, 0, 2, 2, 1, 0, 2, 0, 1, 1, 2, 0, 1, 0, 2, 0, 1, 1, 2, 0]	[2, 1, 0, 0, 2, 1, 0, 2, 2, 0, 1, 0, 2, 0, 1, 1, 2, 0, 0, 1]	316,084,187
[2, 2, 0, 1, 2, 0, 0, 2, 0, 0, 0, 0, 1, 2, 0, 2, 2, 0]	[2, 0, 2, 0, 2, 0, 2, 0, 2, 1, 0, 1, 0, 1, 0, 1, 2, 2, 0, 1]	[2, 1, 0, 2, 2, 1, 0, 1, 1, 2, 2, 0, 1, 1, 2, 0, 2, 1, 2, 0]	355,088,249
[2, 0, 0, 1, 0, 2, 1, 0, 2, 1, 2, 2, 1, 0, 0, 2, 1, 2]	[1, 0, 0, 2, 1, 0, 2, 2, 0, 1, 0, 2, 0, 2, 2, 1, 0, 2, 0, 1]	[0, 0, 1, 0, 2, 1, 1, 2, 0, 1, 0, 2, 0, 2, 1, 2, 2, 0, 1, 2]	376,821,810
[0, 0, 2, 2, 0, 2, 0, 2, 1, 2, 1, 1, 1, 2, 2, 1, 1, 2]	[0, 1, 0, 2, 2, 1, 1, 0, 1, 0, 0, 2, 0, 1, 0, 1, 0, 2, 1, 1]	[0, 1, 2, 1, 0, 2, 0, 1, 0, 2, 0, 0, 2, 0, 1, 0, 0, 1, 2, 1]	52,514,261
[0, 2, 2, 1, 0, 2, 0, 1, 1, 0, 2, 0, 1, 2, 0, 1, 0, 2]	[1, 0, 2, 2, 0, 1, 0, 2, 0, 1, 1, 0, 2, 0, 1, 0, 0, 0, 2, 2]	[2, 0, 1, 0, 2, 0, 1, 0, 1, 1, 0, 2, 0, 2, 0, 1, 0, 1, 0, 1]	52,645,642
[0, 2, 1, 1, 0, 2, 0, 1, 1, 1, 0, 0, 2, 0, 1, 0, 2, 2]	[0, 0, 1, 0, 2, 0, 1, 0, 1, 1, 1, 0, 2, 0, 1, 0, 2, 0, 1, 0]	[2, 2, 2, 1, 1, 2, 0, 1, 0, 2, 0, 0, 0, 1, 2, 2, 0, 1, 2, 1]	8,644,142
[1, 0, 2, 1, 1, 0, 2, 2, 0, 1, 0, 2, 1, 1, 2, 0, 1, 2]	[2, 0, 0, 1, 0, 2, 2, 1, 0, 2, 2, 0, 1, 0, 1, 0, 0, 2, 0, 1]	[1, 0, 2, 1, 0, 2, 0, 1, 1, 0, 2, 0, 1, 0, 0, 0, 2, 2, 1, 0]	146,258,544
[0, 2, 2, 0, 1, 0, 2, 0, 2, 0, 1, 0, 1, 0, 2, 0, 1, 0]	[2, 0, 0, 0, 1, 0, 2, 0, 1, 0, 2, 0, 1, 0, 1, 0, 0, 0, 1, 0]	[0, 0, 0, 1, 0, 1, 0, 1, 0, 2, 0, 2, 0, 1, 0, 0, 1, 0, 2, 2]	158,673,586

Table 1. Orbit Lengths

Theorem. The size of the set generated by the EDES encryption functions is larger than the symmetric group S_{96}.

Substitution Box in Simplified EDES

Figure 3 represents one of the three S-Boxes designed for simplified EDES. The S-Boxes are designed to produce high level of security based on the criteria for perfect secrecy. Using Shannon's theory of diffusion and confusion the S-Box will obfuscate similar traits in the key and the ciphertext increasing the security of the cryptosystem exponentially.

```
[[[24, 25, 6, 16,  3, 7,  1, 18, 26,  5, 10,  9, 19, 23, 13, 12, 15,  8, 20, 17,  2, 11,  0, 21, 14,  4, 22],
  [17, 18, 26, 9, 23, 0, 21, 11, 19, 25,  3,  2, 12, 16,  6,  5,  8,  1, 13, 10, 22,  4, 20, 14,  7, 24, 15],
  [16, 17, 25, 8, 22,26, 20, 10, 18, 24,  2,  1, 11, 15,  5,  4,  7,  0, 12,  9, 21,  3, 19, 13,  6, 23, 14],
  [10, 11, 19, 2, 16,20, 14,  4, 12, 18, 23, 22,  5,  9, 26, 25,  1, 21,  6,  3, 15, 24, 13,  7,  0, 17,  8],
  [21, 22, 3, 23, 0,  4, 25, 15, 23,  2,  7,  6, 16, 20, 10,  9, 12,  5, 17, 14, 26,  8, 24, 18, 11,  1, 19],
  [26, 0,  8, 18, 5,  9,  3, 20,  1,  7, 12, 11, 21, 25, 15, 14, 17, 10, 22, 19,  4, 13,  2, 23, 16,  6, 24],
  [3,  4,  12,22, 9, 13,  7, 24,  5, 11, 16, 15, 25,  2, 19, 18, 21, 14, 26, 23,  8, 17,  6,  0, 20, 10,  1],
  [5,  6,  14,24, 11,15,  9, 26,  7, 13, 18, 17,  0,  4, 21, 20, 23, 16,  1, 25, 10, 19,  8,  2, 22, 12,  3],
  [11, 12, 20, 3, 17,21, 15,  5, 13, 19, 24, 23,  6, 10,  0, 26,  2, 22,  7,  4, 16, 25, 14,  8,  1, 18,  9]],
```

Figure 3. S-Box

Round Function in EDES (S-Box)

- Expansion permutation E is applied to R
- E(R) is added modulo to k_i
- The output is exactly 18 characters in length
- Output is ran through three S-Boxes
- Resulting set of numbers is 15 characters in length
- Applying permutation P completes the round function

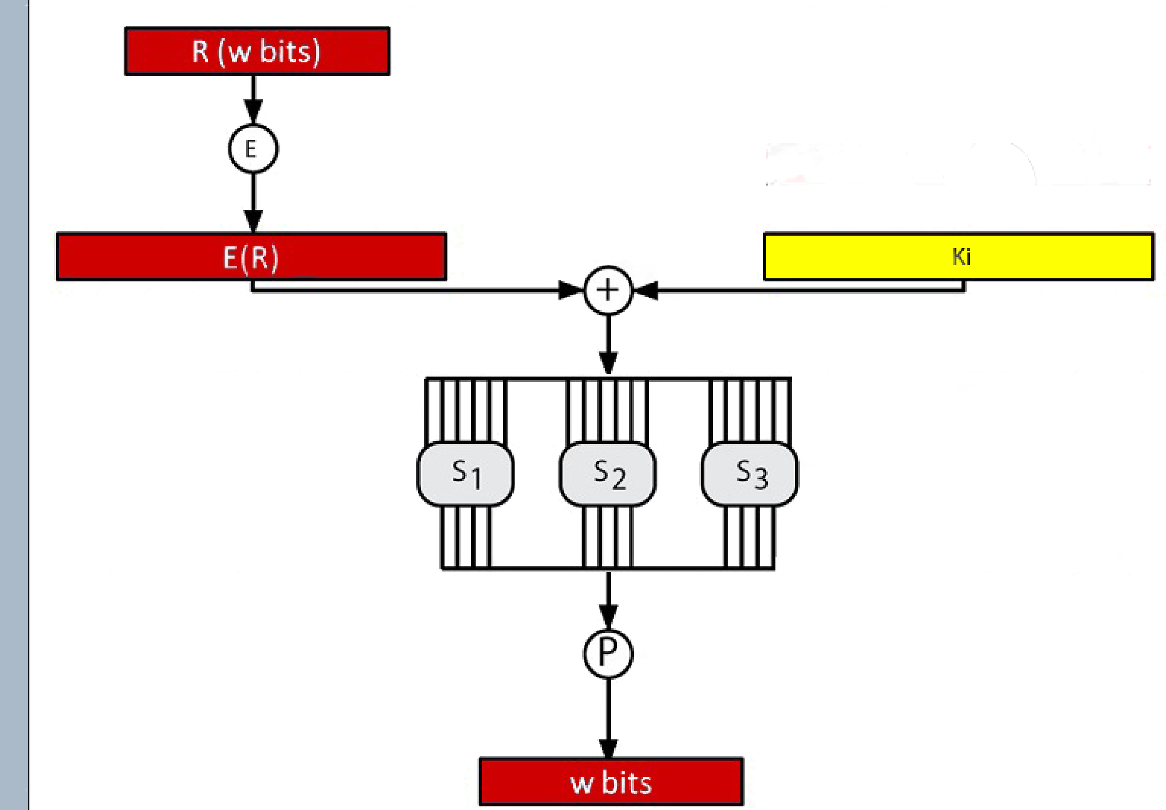

Figure 2. Round Function

Theorem. The set of DES and EDES encryption permutations are not a group[1],[3]. Thus multiple DES and EDES encryptions can improve their security.

Future Work

- Continue to improve the lower bound of the group generated by the set of encryption functions by this cryptosystem
- Investigate security of simplified DES over $\mathbb{Z}_3$
- Determine if the cryptosystem has weak or semi-weak keys
- Design a cryptosystem simplified version of DES over $\mathbb{Z}_5$ and analyze its security

References

[1] L. Babinkostova et al., *A Simplified and Generalized Treatment of DES Related Ciphers*, Cryptologia (2014).

[2] D. Coppersmith, *The Data Encryption Standard (DES) and its strength against attacks*, IBM Journal of Research and Development, Vol. 38 (1994), 243-250.

[3] B.S. Kaliski, R.L. Rivest, and A.T. Sherman, *Is the Data Encryption Standard a Group?*, Journal of Cryptology, Vol. 1 (1988), 3-36.

Acknowledgements

Special thanks to the National Science Foundation and the Science, Technology, Engineering, and Mathematics Talent Expansion Program (STEP) for funding, supporting, and making this project possible.

NSF Idaho STEP Grant: #0856815