

# Project proposal

## Cryptanalysis of DES



03003802	996CB7BA	0EG0161B	G0021C06
BA7CE203	G0030200	01208600	37D14D00
1B7125G0	024FG002	53D03C00	AD722500
BD03C00	887525C1	01A07700	37D14D00
B7125G0	024FG002	53D03C00	AD722500
BD03C00	887525C1	4F553D	53414242
F4F3D41	4242434E	3D4A6	6469204
6C2F4F	553D4553	414	4F3D414
425604	00312E30	424	0003424
003042	4C0	024E4E4F	00B1D3
2254F1	21	8833B0CC	2957EE
3ECAA	CB3EE8EF	DF038D7F	A14217
2AA4D	04143B75	4F571C83	535C04
7DED9	B57C659E	C820EE07	FA49F
96DB	7D7F743D	9A36DD29	454E0
014D	410800C8	9A54E072	5A14C

Prepared for: Jason Hinek, Doctor of Philosophy (PhD), Computer Science (Cryptography)

Prepared by: Team AbDou

November 2<sup>nd</sup>, 2016

## Objective

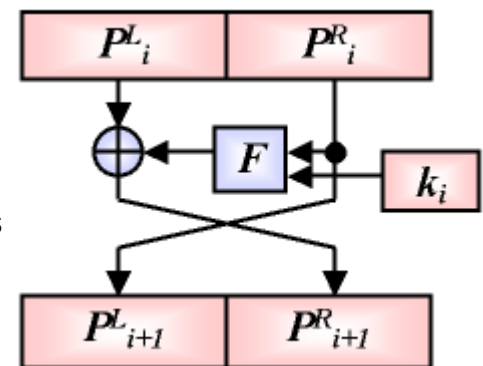
Provide an implementation of a comprehensive method to break the DES encryption in several minutes on a regular PC utilizing cryptanalysis of the DES standard and contrasting different ideas from research papers.

## Goals

The main goal is to explore and understand more about the DES encryption method in depth and outline key factors noted in different differential and linear cryptanalysis studies that were done over the past few decades. Try to implement an attack using differential cryptanalysis and show its feasibility compared to a brute-force method.

## Overview

Our attack assumes we have a plaintext-ciphertext pair and that we are trying to determine the key. Each of the 16 rounds can be described as follows: the input to each round is broken into 32-bit halves, only the left half is modified in each round. Also, for each round, a different 48-bit subkey is derived from the 56-bit key. This is the basis of Shamir and Biham's attack. Pictured on the right is one iteration through one of the 16 rounds.



## Resources

1. Eli Biham, Adi Shamir :Differential Cryptanalysis of the Full 16-round DES (2007)  
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.720.215&rep=rep1&type=pdf>
2. Cetin Kaya Koc :Differential Cryptanalysis  
<http://cs.ucsb.edu/~koc/ccs130h/notes/dc1.pdf>
3. Eli Biham, Adi Shamir : Differential Cryptanalysis of DES- like Cryptosystems (1990)  
<http://www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/Biham-DC.pdf>
4. Howard M. Heys :A Tutorial on Linear and Differential Cryptanalysis  
[https://www.engr.mun.ca/~howard/PAPERS/ldc\\_tutorial.pdf](https://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf)
5. Eli Biham, Adi Shamir : Differential Cryptanalysis of the Data Encryption Standard  
<http://www.cs.technion.ac.il/~biham/Reports/differential-cryptanalysis-of-the-data-encryption-standard-biham-shamir-authors-latex-version.pdf>