[FALL 2025 CS485/585]

Project proposal: Cryptanaylsis of Reduced-Round DES

Jarren Calizo Benjamin Chong Wesley Grzemkowski

Department of Computer Science
Portland State University

{*calizo,chongben,wesleyg*}*@pdx.edu*

November 4, 2025

1 The topic

DES is a 64 bit block encryption scheme that has proven itself secure in its design. However, its relatively small key space makes it trivial to brute force with modern computers rendering the algorithm obsolete. DES encryption uses 16 rounds of permutation to mask its input. It also employs an algorithm to generate a key for each round. When DES was first brought up in class, we were curious why 16 rounds specifically were used and how the scheme's security would change given varying numbers of rounds, and building on that curiosity decided to explore reduced-round DES.

We found from our preliminary research that the choice of 16 rounds is not just an arbitrary design decision, but something that has been stress-tested for decades using various attack models. Classical differential and linear cryptanalysis do become effective once you peel away enough rounds. Biham and Shamir famously gave a differential attack on a 8-round DES [BS91] as well as a full 16-round DES [BS93] that beats brute force in the chosen-plaintext model, while Matsui's linear cryptanalysis uses carefully crafted 14-round approximations and around 2^{43} known plaintexts to recover the key more efficiently than exhaustive search [Mat94].

More recently, researchers have revisited reduced-round DES with modern tools, using machine-learning aided linear and differential-linear cryptanalysis to build stronger distinguishers and key-recovery attacks on 6 to 8 round variants, effectively using DES as a playground for testing new cryptanalytic ideas [HRC25a] [HRC25b]. Against this, our project aims to construct and experimentally validate a distinguisher for reduced-round DES, so we can see, in a hands-on way, how the cipher's statistical effectivity fades as rounds are added and how close we can push simple distinguishers toward current research.

2 The goal

For this project, we want to attempt to construct a distinguisher or similar attack for a reduced-round DES schema. Our goal is to further explore the security of DES and its design, and how reducing the number of rounds affects its security. Ideally, as a final deliverable, we want to present

a practical attack against round-reduced DES. We would like to accomplish this by doing our own cryptanalysis using Python, and then build a demo attack from the results of that analysis.

We believe this is a topic worth exploring, because even though DES has been proven obsolete because of its small key size, its design has proven quite robust in the face of extensive research and scrutiny. In addition, the techniques applied to break down DES are being applied to modern algorithms such as AES. Finally, by looking at DES with a reduced number of rounds, we hope to have a version of DES which is feasible for us to construct an attack against, while also giving insight into how the number of rounds used affects DES as a construction.

In our presentation, we will hopefully be able to demonstrate a distinguisher for reduced-round DES and explain how such a distinguisher functions. It is possible that this analysis does not go as planned given our short time frame. So, failing that, we will still be able to present on the research that has been put into distinguishing reduced round DES, and also provide a look into cryptanalysis in practice. We also have potential strategies to avoid this, such as further reducing the number of rounds in DES or reducing its key size.

Some of the resources we plan on pulling from are Biham and Shamir's original papers on differential cryptanalysis of 8 and 16 round DES [BS91] [BS93], and Matsui's paper showing a linear cryptanalysis based attack [Mat94].

3 The plan

We have 5 weeks to complete our final. Below are the rough deadlines for each major milestone.

- **11/3 - 11/9 (Week 6)**
  - Review literature
  - Have a functioning reduced-round DES in Python
- **11/10 - 11/16 (Week 7)**
  - Write the intro section of the report
  - Write code needed for our cryptanalysis in Python
- **11/17 - 11/23 (Week 8)**
  - Write our methodologies into the report
  - Execute the cryptanalysis and gather our results
- **11/24 - 11/30 (Week 9)**
  - Construct a practical attack and have demo in Python
  - Write the results section of the report
  - Presentation/demo ready by the end of week 9
- **12/1 - 12/7 (Week 10)**
  - Finish report with our results and conclusions
  - Review paper and practice demo

References

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, Jan 1991.

[BS93] Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round des. In Ernest F. Brickell, editor, *Advances in Cryptology — CRYPTO' 92*, pages 487–496, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

[HRC25a] Ze-zhou Hou, Jiong-jiong Ren, and Shao-zhen Chen. Machine learning-aided differential-linear attacks with applications to des and speck32/64. *Journal of King Saud University Computer and Information Sciences*, 37(8):228, Sep 2025.

[HRC25b] Zezhou Hou, Jiongjiong Ren, and Shaozhen Chen. Improved machine learning-aided linear cryptanalysis: application to des. *Cybersecurity*, 8(1):22, Apr 2025.

[Mat94] Mitsuru Matsui. Linear cryptanalysis method for des cipher. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 386–397, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.