A Comparative Analysis of Symmetric and Asymmetric Data Encryption Techniques with Existing Vulnerabilities

Samamtha Barua Chowdhury
Department of Electrical and Computing Science, University of Alberta
Edmonton, Alberta, Canada
sc12@ualberta.ca

1 Abstract

In this proj

2 Introduction

(the first section of the paper and should include: context of the presented topic, why it is important, motivation, brief summary of presented solution, list of research contributions)

3 Background and Terminology

optional and may be spread out through the paper depending on the topic

4 Motivating/Running Example

optional, depending on the nature of the presented topic

5 Overview of Approach

a general high-level overview of the presented approach, usually accompanied with an illustrative diagram such as a workflow diagram

6 More Details about Approach

probably multiple sections

DES: Data is ciphered taking 64 bits block of data at a time and performing permutations and substitution on it with the help of secret key. The process occurs in 16 rounds, where each encrypted block is dependent on all other previous blocks. [1]

Block Size: 64 bit

Key Size: 56bit. Of them, 8 bits are used for parity, which leaves 48 bits for encryption, making it more vulnerable to attacks.

Speed:

Complexity: O(2^{55})

Attacks:

1. Since the key size determines the number of possible keys, by brute force, it would take an attacker a maximum of 2^{56} or 72,057,594,037,927,936 attempts to find the correct key. [1].
2. More vulnerable to Linear cryptanalysis than differential cryptanalysis, using 2^{43} pair of known plaintexts, though it's claimed to be quite impractical in reality.[2]

Uses:

7 Evaluation

including experimental setup, research questions, discussion of results beyond just stating some statistics such as discussing why your approach is superior for some benchmarks but not for others

8 Discussion

optional, depending on how the evaluation section of the paper is written

9 Related Work

what other papers are related to your presented topic, more importantly how your work is different or similar to those papers, as well as what limitations your work has addresses or insights it has drawn from those papers

10 Conclusion

summarize the presented problem, how you addressed it, brief summary of results, and optionally briefly discuss future work

References

[1] "Network Security data encryption standard," https://searchsecurity.techtarget.com/definition/Data-Encryption-Standard, accessed: 2020-03-27.

[2] "Ch-6, data encryption standard," https://academic.csuohio.edu/yuc/security.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn