Attacking Weak Symmetric Ciphers

HW1 - CNS Sapienza

Pietro Borrello

02 Nov 17

1 Introduction

Due to the continuous increasing of computational power, every encryption algorithm will eventually become obsolete. Any algorithm for which a bruteforce attack is computationally feasible, is considered weak, and must not be used. In this article we present an analysis on the bruteforce attack against such an algorithm as DES, for which we provide an implementation and performance results.

DES, first published in 1975 by IBM, has been considered obsolete since 1998, thanks to the EFF DES cracker [1] that managed to broke a DES encrypted message in 56 hours exploiting the limited key space. Apart form bruteforce more advanced attacks exist, as Differential and Linear Cryptanalysis on DES [2] that can break the chiper in less than the complexity of the exhaustive search in the key space. Such attacks are not considered in this article, that has the aim to show that DES is attackable only with a dumb bruteforce attack. Thus providing the thesis that using DES should be foolish.

2 Resources Used

To test the implementation a 2 GHz Intel Core i5 (dual core, with 4 virtual cores thanks to hyperthreading) with 16 GB of RAM has been used.

References

[1] S. Landau, *Standing the test of time: The data encryption standard*, Notices of AMS, 2000.

[2] Eli Biham, Adi Shamir, *Differential Cryptanalysis of the Full 16-Round DES*, Springer, 1993.