DES Encryption Attack Report

wcrr51

January 2021

1 Introduction

This report looks to explore an attack plan to decrypt the following 16-byte ciphertext:

`0x903408ec4d951acfaeb47ca88390c475`

The following information is provided:

- The corresponding plaintext is a *What Three Words* location
- The ciphertext was encrypted using DES in ECB mode with a 64-bit key

Firstly, as the *What Three Words* format is $a.b.c$ where a, b, c are words such that $n_a+n_b+n_c+2 \leq 16$ where n_x is the length (in characters) of word x.

Secondly, a (relatively) slow encryption oracle is provided.

2 Key-identification Attack

While the key is advertised to be 64-bit, DES only uses 56 - the remaining 8 are either discarded or used as parity bits. This means the keyspace can be reduced by a factor of 256 by ignoring the last bit of each byte. Thus, a full brute-force attack would take up-to 2^{56} attempts. Since the plaintext must contain two full stop characters (`0x2e`), without an oracle these could be used to help check for a valid plaintext. Given access to the encryption oracle, this can theoretically be reduced by many factors of 2 using techniques such as linear cryptanalysis and differential cryptanalysis. On a single machine, with GPU acceleration and the reduced keyspace, this may take several days to months.

3 Attack Results

After around 3 hours of carrying out the attack on an i7-6700k using multithreading, the key `0x98a0bef23454dc02` is found, decrypting the provided ciphertext yields the 16-byte plaintext `tile.bills.print`. In *What Three Words*, this refers to the coordinates `40.026102, -75.030026` in Philadelphia, Pennsylvania, USA.