Cryptography Attack Plan

Benjamin Russell, fdmw97

January 16, 2021

Initial Analysis

Brute Force the Key

I initially experimented with a pure brute-force attack on the 8 byte key used to encrypt the DES message. I constructed an algorithm that leveraged multiple cores and parallelism, however when tested on an Intel i7 processor using 8 threads I was still only able to brute force approximately 24 million keys per second. Since on average it takes brute forcing half the total number of keys 2^{55} as the total is 2^{56} it would take me approximately 46 years to brute force the key by this method.

Differential Cryptanalysis

Differential Cryptanalysis was also infeasible as it would require me to generate 2^{47} chosen plaintext ciphertext pairs, using the previous value for encryptions per second (24 million) this would take me approximately 2 months to generate which is once again infeasible. This approximation does not even take into account the added complexity of choosing the correct plaintext ciphertext pairs which would add even more overhead to the crack.

Linear Cryptanalysis

Linear Cryptanalysis proved infeasible for the same reason as the previous two methods as it requires 2^{43} known plaintext ciphertext pairs this would take me approximately 4 days using the previous value for encryptions per second (24 million). This runtime plus the overhead of having to store 2^{43} plaintexts each of size 8 bytes totalling 65536GB of data make this attack infeasible as well.

Chosen Attack Plan

The attack plan I used instead took advantage of the known structure of the input string (an English what3words address), that it is three words separated by two dots and 16 characters long. The FAQs for what3words state that for the English language what3words uses words

ranging from 4-18 characters long[1]. This means that the total length of the three words can only be fourteen characters meaning only words of length four, five, and six characters need be considered. This meant that the words can only appear as a permutation of two five letter words and a four letter word, or two four letter words and a six letter word (assuming no padding was used in the message). I used the Unix dictionary to sample lists of four, five, and six letter words resulting in lists of length 3784, 6915, and 10605 words for four, five, and six letters respectively. This gives approximately 9.98×10^{11} plaintexts to brute force. Since each plaintext is 16 characters long this should be treated as 1.996×10^{12} DES encryptions to perform. Using my previous approximation of 24 million encryptions per second this should take approximately 2.5 hours to bruteforce.

Result

I did carry out the attack in reality it took longer than expected as I had to carry it out using the provided Oracle and on a weaker Windows machine (Intel i5 4 core). I left the attack running overnight for multiple nights (approximately 15 hours) eventually the plaintext "tile.bills.print" encrypted to "90 34 08 ec 4d 95 1a cf ae b4 7c a8 83 90 c4 75". This corresponds to Four Seasons Total Landscaping in Pennsylvania or more popularly known as the place Donald Trumps campaign team mistakenly booked for a speech.

References

[1] Day, C. What are the shortest and longest words used? Retrieved from https://support.what3words.com/en/articles/2212810-what-are-the-shortest-and-longest-words-used