Introduction to Cryptography (462)
Homework 01
Alexander Kellermann Nieves
Section: 3

1

I wrote a C program that would rotate through all 25 different rotations of the text. Then I just sifted through the 26 lines of text to find which one ended up being regular English. The cleartext is:

`Ifweallunitewewillcausetheriverstostainthegreatwaterswiththeir`

The passage was written by Tecumseh, from the passage Address to the Osages.

2

1. Given a budget of 1 Million, and an overhead of 100% where each ASIC costs 50 dollars, we can use the following formula to extrapolate how many ASICS can be run in parallel. $1,000,000/(50 \times 2)$ gives us the answer of $40,000$. Now we have to find how many keys are there in an average AES Brute force attack. That would just be half of the total keyspace. $2^{128}/2 = 2^{127}$ total keys. Each ASIC can check 5×10^8 keys per second. If we assume that there's no overlap between the ASIC's and we have 40,000 of them, then we can use the following formula to determine how long the search would take.

$$\frac{2^{127}}{5 \times 10^8 \times 40,000}$$

which is equal to:

$$8.5 \times 10^{24} seconds$$

or

$$2.69 \times 10^{17} years$$

$$\frac{2.69 \times 10^{17}}{10^{10}} = 2.69\% \texttt{ of the total age of the universe}$$

2. Now, in order to break AES with an average search time of 24 hours, we need to understand that it means we need to be able to generate 2^{127} keys within 24 hours. We still have the same 40,000 ASICS from before, so we need to solve the following equation to determine how many periods (of 18 months being 1 period) to find out how many years it'll take to get the necessary compute power.

$$5 \times 10^8 \; times \, 2X = 2^{127}$$

where X = the time in periods. Solving for X we get $X = 1.7 \times 10^{29}$ Divide that by 1.5 to get years. Either way, it's significantly long. Longer than any one of us will be here to see become an issue.

3

1. Each letter is 2^7 possible choices. Therefore, the total keyspace of 8 letters would be:

$$2^7 \times 2^7 \times 2^7 \times 2^7 \times 2^7 \times 2^7 \times 2^7 \times 2^7$$

or

$$2^{56}\,\texttt{total keys}$$

which is 72057594037927936 bits.

2. if we only have 26 lowercase letters, then that means we have 26^8 total keys in our keyspace. That is 208827064576 bits.