Introduction to IT Security

Homework 2 Question 5

Abraham Murciano

September 1, 2020

We are to find the expected time that it would take to find an AES 256 bit key by brute force using my personal computer. We can assume that we have a single encrypted block of 32 bytes to crack, and that it takes one thousand CPU cycles to check if one key decrypts the block.

Since the key is made up of 256 bits, there are

$$2^{256} = 1.1579209 \times 10^{77}$$

possible keys. That is approximately one hundred and fifteen quattuorvigintillion different keys.

My personal computer has a processor which is clocked at 2 GHz. Meaning it can run through two billion cycles every second. Therefore it can try two million keys every second.

$$\frac{2,000,000,000}{1,000} = 2,000,000$$

So to try all the possible keys it would take approximately fifty-seven duovigintillion seconds.

$$\frac{2^{256}}{2,000,000} = 5.78960446 \times 10^{70}$$

Since there are 31,556,952 seconds in a year, it would take about one vigintillion eight hundred thirty-four novemdecillion six hundred fifty-two octodecillion six hundred septendecillion years to check every possible key.

$$\frac{5.78960446 \times 10^{70}}{31,556,952} = 1.8346526 \times 10^{63}$$

Therefore on average, it would take half as long.