Superior School of Computer Sciences (ESCOM)
Instituto Politécnico Nacional (IPN)

How long would it take to break AES?

Partial 2

Oscar Andrés Rosas Hernandez

October 16, 2019

Chapter 1

Exercise

So, we have 128 bits, that means that we have to test 2^{128} keys.

- We have a butget of 1000000 dollars.
- Each processor cost 10 dollars.
- So, we can have up to 100000 processors.
- Each processor take t time to check a key. (let $t = 10^{-9}$ seconds)
- So all of them will take $\frac{t}{100000}$ to check a key.

Now, we have to divide the result by $\frac{1}{60*24}$ to get days, not seconds.
So, the expression look something like:

$$num\_days = 2^{128} \times \frac{t}{100000} \times \frac{1}{60 * 24}$$

Now, Moore's law says that each 18 months we double we performance, so:

$$num\_days = 2^{128}(0.5)^{times} \times \frac{t}{100000} \times \frac{1}{60 * 24}$$

We can solve for times and get this formula:

$$times = log_{0.5}\left(\frac{7}{2^{128} \times \frac{t}{100000} \times \frac{1}{60*24}}\right)$$

This gives: 68.2 iterations, that means 102.291 years.