INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Problema AES

La seguridad de los cifradores simetricos recae en el tamaño de la llave.

Por equipos de prácticas lean con atención y respondan el siguiente problema a mano.

Minimum key length for AES algorithm is 128 bits. Suppose a general purpose machine can test one key in 10 nano seconds using one processor and suppose that processors may be parallelized and each one costs 10 dollars.

Suppose also that Moore´s Law wich states that processor performance doubles every 18 months is valid.

How long it may build a key search machine for AES to be able to break the algorithm in 7 days and that its cost will be less than a million of dollars.

Dra. Nidia A. Cortez Duarte