

Minimum Key length for AES 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 cost 10 dollars

Suppose the Moore's law is true.

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 dollars.

$$2^{128} = 3.47 \times 10^{38} \Rightarrow \text{total Keys}$$

We can buy

100,000 processors

$$1 \text{ week} \Rightarrow (60)(60)(24)(7) = 604,800 \text{ sec} \\ 6.048 \times 10^{18}$$

$$2^n (6.48 \times 10^{18}) = 3.47 \times 10^{38}$$

$$2^n = 5.6216 \times 10^{19}$$

$$\log_2 5.6216 \times 10^{19} = n$$

$$n = 66 \Rightarrow \text{number of periods}$$

$$66 \times 18 = 1,188 \Rightarrow \text{months}$$

$$1,188 / 12 \Rightarrow \underline{99 \text{ years}}$$