

http - без шифрования
https - шифрование простые числа

разложение на простые множители

$$30=2*15=2*5*3$$

23707

2,3,4,5,6,7,8... 151

$$23707= \text{очень долго}=151*157$$

$$151*157=\text{очень быстро}=23707$$

**никто не умеет быстро раскладывать числа
на простые множители**

RSA 1970 году - алгоритм шифрования
с тех пор они получают 3 млрд
долларов в год за то что все пользуются
их алгоритмов

MIT Массачусетский Технологический

2 огромных простых числа
100 знаков длиной

они перемножены, получается число 200 знаков длиной

10 ГГц

1 ГГц = 1000 000 000 операций в секунду

твой компьютер 10 000 000 000 делений в секунду 10^{10}

10^{200} - столько проверок надо сделать

сколько понадобится секунд?

$$10^{200}/10^{10}=10^{190} \text{ секунд}=10^{190} / 10^8 = 10^{182} \text{ лет}$$

в году 31 000 000 секунд =100 000 000 секунд= 10^8 секунд в году

15 000 000 000 лет