# Generator RSA

**Generator oparty na trudności z faktoryzacją liczb**.

1.) Wybieramy dwie liczby pierwsze *p* i *q* (*N* = *pq*) oraz liczbę *e* względnie pierwszą z (*p* − 1)(*q* − 1).

2.) Wybieramy losową liczbę (zarodek) $x_0$ mniejszą od N, a następnie obliczamy:

$$x_{i+1} = x_i^e \pmod N$$

3.) Generowanym bitem jest najmłodszy bit $x_i$