Szyfrowanie asymetryczne - RSA

- Blokowy algorytm szyfrowania ze zmienną długością bloków
- Klucz szyfrujący o długości 1024, 2048, 4096 bity

Algorytm RSA

- Wybieramy dwie duże liczby pierwsze: {p, q}
- Obliczamy ich iloczyn (łatwo): N = pq
- Wybieramy losowo liczbę e < N
- Liczba e będzie kluczem **szyfrującym**
- Znajdujemy liczbę d taką, że $ed \equiv 1 \pmod{(p-1)(q-1)}$ lub inaczej $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
- Liczba d jest kluczem **deszyfrującym**