Znajdowanie klucza

- $p = 5, q = 11$
- $N = pq = 55$
- $\phi = (p - 1)(q - 1) = 40$
- $e = 3$
- $ed \pmod{\phi} \equiv 1$
- $3*27 \pmod{40} = 1$
- $d=27$

Liczby {e, N} stanowią klucz publiczny, który ujawniamy
Liczby {d, N} stanowią klucz prywatny, który powinien być ściśle chroniony

Public key = {3,55}
Secret key = {27,55}

Szyfrowanie

- **m = 14**
- 14<55
- c ≡ 14^e (mod N)
- e = 3
- N = 55
- 14^3 (mod 55) = 2744 (mod 55) = **49 = c**