Příklad

1. RSA `n = 143`, `p = 11`, `q = 13`, `e = 7`. Vypočítat d, napsat VK, PK a zašifrovat číslo 9.

$p = 11$

$q = 13$

$n = pq = 143$

$e = 7$

$\Phi(n) = (p-1)(q-1)$

$\Phi(143) = 10 \cdot 12 = 120$

$e \cdot d \bmod \Phi(n) = 1$

$7d \bmod 120 = 1$

$d = 103$

$VK = (n, e) = (143, 7)$

$SK = (n, d) = (143, 103)$

$m = 9$

$120x + 7y = 1$

$\gcd(120, 7)$

P_1: $120 = 17(7) + 1$

P_2: $1 = 120 - 17(7)$

$-17(7) = 1$

$-17 + 120 = 103$

$C = m^e \bmod n = 9^7 \bmod 143 = 4\,782\,969 \bmod 143 = \underline{48}$

$m = c^d \bmod n = 48^{103} \bmod 143 = \underline{9}$