- javni RSA ključ $(n,e) = (527, 61)$ $\quad e = 61 = 1+4+8+16+32$
- sporočilo v čistopisu : 40
- šifriranje sporočila : $c = E(m) = m^e \bmod n \Rightarrow c = 40_{61} \bmod 527 = ?$

$40_1 \bmod 527 = 40$ Če je št. manjša od 527 samo prepišemo

$40_2 \bmod 527 = (40_1 \bmod 527)_2 \bmod 527 = 19$

$40^2 = 1600 \quad : 527 = 3,036\ldots \quad -3 = 0,036$

rabmo samo ostanek

$0,036 \cdot 527 = 19$

(ostanek · 527)

$40_4 \bmod 527 = (40_2 \bmod 527) \bmod 527 = 361$

$19^2 = 361 \Rightarrow$ prepišeš ker je manjše od 527

$40_8 \bmod 527 = (40_4 \bmod 527) \bmod 527 = 152$

$361^2 = 130321 : 527 = 247,288\ldots \quad -247 = 0,288\ldots$

ostanek pomnožiš z 527

$0,288 \cdot 527 = 152$

TKO DELAŠ DO 40_{128}

$c = (40 \cdot 361 \cdot 152 \cdot 443 \cdot 205) \bmod 527 = \boxed{350}$

prepišeš samo tiste ki so v e-ju (1,4,8,16,32)

① $(40 \cdot 361) \bmod 527 = 211$ Daredimo v delih :

② $(152 \cdot 443) \bmod 527 = 407$

③ $(205 \cdot 407) \bmod 527 = 169$

④ $(211 \cdot 169) \bmod 527 = \boxed{350}$ Rezultat