1. Naloga
2. 19+16+15+3+6 = 59, 59%7 = 3, (3+1)\*9 = 36, ce -> ec
3. 14+16+18+11+6 = 65, 65%7 = 2, (2+1)\*9 = 27, bf -> fb
4. 17+13+1+1+1+25+1 = 59, 59%7 = 3, (3+1)\*9 = 36, ce -> ec
5. Naloga

Odpri okno na stežaj

1. Naloga

Zakleni vrata in daj ključe pod predpražnik

1. Naloga

010010

1. Naloga

Asimetrična zadeva

2 ključa -> javni in zasebni (public and private)

1. Zberemo 2 praštevili: p in q
2. Izračunamo **n** = p\*q
3. Izračunamo m = (p-1)\*(q-1)
4. Izberemo **e**: e in m sta tuji(en skupni delitelj) – 1<e<m
5. Izberemo **d**: (e\*d)mod m = 1 // e\*d = x\*m+1 – 0<d<m

Javni ključ: n in e

Zasebni ključ: n in d

n in n -> mod, e in d -> exp

Šifriranje: M^e mod n = C – M = sporočilo

Dešifriranje: C^d mod n = M

Počasen, uporabljen za šifriranje ključev

1. N = 15, m = 8
2. D: med 0 in 8, (e\*d)mod m = 1 // 11\*d mod m = 1 -> 11\*d = 8x+1 -> d = 3
3. JK:(15,11); ZK:(15,3)
4. 3^11 mod 15 = 177147 mod 15 = 12
5. 12^3 mod 15 = 3
6. Naloga
7. N = 33, m = 20
8. E = 3 ali 7; (d\*e)mod m = 1 -> d\*3 mod 20 = 1 -> d = 7 ali 3
9. JK(33, 3), ZK(33, 7)
10. 2^3 mod 33 = 8
11. Naloga

P = 11, q = 7

N = 77

M = 60

E = 7 ali 11 ali 13

D: d\*7 mod 60 = 1; d = 43….. 43\*7 = 301

E = 11 -> d = 11

E = 13 -> d = 37