

# Math engine

Step by step nástroj pro řešení algoritmických problémů v rozsahu předmětu diskretní matematika pro potřeby zkoušek v distanční formě.

## Vybrané funkcionality:

- Postup výpočtu primitivního kořene

lin.kód	RSA	Rovnice	Inverze	Umocňovač	Rabin.kód	Pri.kořen	Diff-Hellman
---------	-----	---------	---------	-----------	-----------	-----------	--------------

primitivní kořen mod

$\phi 31 = 30$   
 $30 = 2 \cdot 15 = 3 \cdot 5 = 5 \cdot 1$   
unikatní delitele jsou :2,3,5,  
budeme tedy kontrolovat že  $a^{15} a^{10} a^6$  nejsou kong. s 1 mod 31  
.....

pro  $a = 2$   
 $2^1 \equiv 2$   
 $2^2 \equiv 2 \cdot 2 \equiv 4$   
 $2^4 \equiv 4 \cdot 4 \equiv 16$   
 $2^8 \equiv 16 \cdot 16 \equiv 8$   
.....  
 $2^{12} \equiv 2^8 \cdot 2^4 \equiv 128 \equiv 4$   
 $2^{14} \equiv 2^{12} \cdot 2^2 \equiv 16 \equiv 16$   
 $2^{15} \equiv 2^{14} \cdot 2^1 \equiv 32 \equiv 1$

pro  $a = 3$   
 $3^1 \equiv 3$   
 $3^2 \equiv 3 \cdot 3 \equiv 9$   
 $3^4 \equiv 9 \cdot 9 \equiv 19$   
 $3^8 \equiv 19 \cdot 19 \equiv 20$   
.....  
 $3^{12} \equiv 3^8 \cdot 3^4 \equiv 380 \equiv 8$   
 $3^{14} \equiv 3^{12} \cdot 3^2 \equiv 72 \equiv 10$   
 $3^{15} \equiv 3^{14} \cdot 3^1 \equiv 30 \equiv 30$   
 $3^1 \equiv 3$   
 $3^2 \equiv 3 \cdot 3 \equiv 9$   
 $3^4 \equiv 9 \cdot 9 \equiv 19$   
 $3^8 \equiv 19 \cdot 19 \equiv 20$

- Výpočet postupu algoritmu pro bezpečnou výměnu klíčů v síti

lin.kód	RSA	Rovnice	Inverze	Umocňovač	Rabin.kód	Pri.kořen	Diff-Hellman
---------	-----	---------	---------	-----------	-----------	-----------	--------------

prvočíslo p:  primitivní kořen g:  a:  b:

Alice spočítá a pošle:  $g^a \equiv 7^7$   
 $\equiv 1 \cdot 7 \cdot (7^2)^3$   
 $\equiv 7 \cdot 49 \cdot (49^2)^1$   
 $\equiv 343 \cdot 22 \equiv 38 \cdot 22 \equiv 43$   
Bob spočítá a pošle:  $g^b \equiv 7^{11}$   
 $\equiv 1 \cdot 7 \cdot (7^2)^5$   
 $\equiv 7 \cdot 49 \cdot (49^2)^2$   
 $\equiv 343 \cdot (22^2)^1$   
 $\equiv 343 \cdot 57 \equiv 38 \cdot 57 \equiv 31$   
Alice spočítá spol. soukromý klíč jako:  $(g^b)^a$   
 $\equiv 1 \cdot 31 \cdot (31^2)^3$   
 $\equiv 31 \cdot 46 \cdot (46^2)^1$   
 $\equiv 1426 \cdot 42 \equiv 23 \cdot 42 \equiv 51$   
Bob spočítá spol. soukromý klíč jako:  $(g^a)^b$   
 $\equiv 1 \cdot 43 \cdot (43^2)^5$   
 $\equiv 43 \cdot 19 \cdot (19^2)^2$   
 $\equiv 817 \cdot (56^2)^1$   
 $\equiv 817 \cdot 25 \equiv 24 \cdot 25 \equiv 51$

- Postup výpočtu soustavy 2 rovnic lineárních kongruencí

lin.kód	RSA	Rovnice	Inverze	Umocňovač	Rabin.kód	Pri.kořen	Diff-Hellman
---------	-----	---------	---------	-----------	-----------	-----------	--------------

$c \equiv$    $\text{mod}$  
     
  $c \equiv$    $\text{mod}$  
     

$$31c \equiv 8 \cdot 31 \equiv 248$$

$$23c \equiv 24 \cdot 23 \equiv 552$$

---


$$8c \equiv 248 - (1 \cdot 552) \equiv -304$$

$$7c \equiv 552 - (2 \cdot -304) \equiv 1160$$

$$1c \equiv -304 - (1 \cdot 1160) \equiv -1464$$

$$c \equiv -38 \pmod{713} \equiv 675 \pmod{713}$$