NA T-EXKURZI
TEORIE ČÍSEL

1

AHOJ,
VÍTÁM VÁS

PETR PUPÍK

POZNÁMKY

2

MYŠLENKY

3

BEZOUTOVA
IDENTITA JE …

JE MI
ROZUMĚT?

BEZOUTOVA
IDENTITA
(113,50)=52 *
- 23*113
(A,B)=AX +BY

4

BĚHEM T-EXKURZE JSME SE DOST NAUČILI.

KONGRUENCE
φ(2000)=80
BEZOUTOVA
IDENTITA
(113,50)=52 *50
- 23*113
(A,B)=AX +BY

KONGRUENCE
ELIPTICKÉ KŘIVKY
φ(2000)=800
BEZOUTOVA
IDENTITA
RSA
(113,50)=52 *50 -
23*113
(A,B)=AX +BY

KONGRUENCE
φ(2000)=800
RSA
DIGITÁLNÍ
PODPIS
ELIPTICKÉ KŘIVKY
BEZOUTOVA
IDENTITA
TEORIE ČÍSEL V PRAXI
(113,50)=52 *50 -
23*113
(A,B)=AX +BY

KONEC T-EXKURZE

5

6

AHOJ

AHOJ

CO SE TI HONÍ
HLAVOU?

7

(113,50)=52
*50 - 23*113

PODPIS
DIGITÁLNÍ
(25,15)=5
ZBYTKOVÉ
TŘÍDY
RSA
DĚLITEL
PRVOČÍSLO
MALÁ
FERMATOVA
φ(2000)
ŠIFROVÁNÍ
NEJMENŠÍ
SPOLEČNÝ
NSN
NÁSOBEK

VEŘEJNÝ
KLÍČ

(A,B)= AX +BY
KONGRUENCE
EULEROVA
FUNKCE
KLÍČ
MODUS
NEJVĚTŠÍ
SPOLEČNÝ
NSD
DĚLITEL
BEZOUTOVA
IDENTITA

HASHOVACÍ
FUNKCE
KONGRUENCE
BOB A ALICE
ŠIFRUJÍ
ELIPTICKÉ
KŘIVKY