2.3 / nr. 22 Calculează inversul lui 23 în modulo 97.

$97 = 23 \cdot 4 + 5$

$23 = 5 \cdot 4 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 2 \cdot 1 + 0$

↓

am aplicat algoritmul extins al lui Euclid

cmmd $(23, 97) = 1$

$(23, 97) = 1$

$1 = u \cdot 23 + v \cdot 97$

$1 \equiv u \, 23 \pmod{97}$

deci $\exists \, a^{-1} = u$

$x_{97} = (1, 0) \quad x_{23} = (0, 1)$

$x_5 = x_{97} - 4 \cdot x_{23}$

$= (1, 0) - 4 (0, 1)$

$= (1, 0) - (0, 4)$

$= (1, -4)$

$x_3 = x_{23} - 4 \cdot x_5$

$= (0, 1) - 4 (1, -4)$

$= (0, 1) - (4, -16)$

$= (-4, 17)$

$x_2 = x_5 - x_3$

$= (1, -4) - (-4, 17)$

$= (5, -21)$

$x_1 = x_3 - x_2$

$= (-4, 17) - (5, -21)$

$= (-9, 38)$

$1 = -9 \cdot 97 + 38 \cdot 23 \,/ \bmod 97$

$1 \equiv 38 \cdot 23 \pmod{97}$

38 este inversul lui 23 în modulo 97.

Criptografie

Seminar 1

Ex 2/0

MR 22

Găsiți CMMDC pentru 44453 și 55469 cu ajutorul algoritmului lui extins și determinați coeficienții Bezout.

55469 = (1,0) și 44453 = (0,1)

55469 = 44453 · 1 + 11016

44453 = 11016 · 4 + 389

11016 = 389 · 28 + 124

389 = 124 · 3 + 17

124 = 17 · 7 + 5

17 = 5 · 3 + 2

5 = 2 · 2 + 1

2 = 1 · 2 + 0

(55469, 44453) = 1

1 = 18284 · 55469 − 22815 · 44453

$x_{11016} = x_{55469} - x_{44453}$

= (1,0) − (0,1)

= (1, −1)

$x_{389} = x_{44453} - 4 \cdot x_{11016}$

= (0,1) − 4(1, −1)

= (0,1) − (4, −4)

= (0 − 4, 1 + 4) = (−4, 5)

$x_{124} = x_{11016} - 28 \cdot x_{389}$

= (+1, −1) − 28 · (−4, 5)

= (1, −1) − (−112, 140)

= (1 + 112, −1 − 140) = (113, −141)

$x_{17} = x_{389} - 3 \cdot x_{124}$

= (−4, 5) − 3(113, −141)

= (−4, 5) − (339, −423)

~~= (−4, 5) − (3~~

= (−4 − 339, 5 + 423)

= (−343, 428)

$x_5 = x_{124} - 7 \cdot x_{17}$

= (113, −141) − 7(−343, 428)

= (113, −141) − (−2401, 2996)

= (113 + 2401, −141 − 2996)

= (2514, −3137)

$x_2 = x_{17} - 3 \cdot x_5$

= (−343, 428) − 3(2514, −3137)

= (−343, 428) − (7542, −9411)

= (−343 − 7542, 428 + 9411)

= (−7885, 9839)

$x_1 = x_5 - 2 \cdot x_2$

= (2514, −3137) − 2(−7885, 9839)

= (2514, −3137) − (−15770, 19678)

= (2514 + 15770, −3137 − 19678)

$x_1 = (18284, -22815)$

1 = 18284 · 55469 − 22815 · 44453