Afininiai šifrai:



Tarkim a = 15, b = 4, o koduosime B raide;

B raide lenteleje yra 1, tai:

1 \* 15 + 4 = 19

19 mod 26(abeceleje raidziu skaicius) = 19; jeigu atsakymas daugiau nei yra raidziu(26), 28-26 = 2

19 pozicija = T, tai B raide keiciama i T;

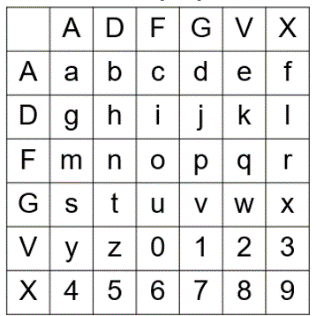
Cezario šifras:



Kai raktas = 2;

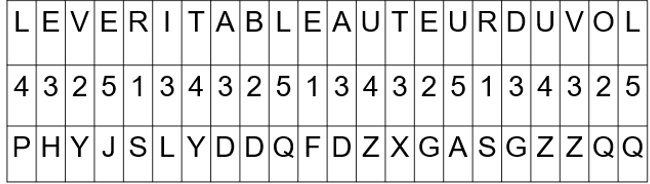
Rokas = Tqmcu

Vokiečių lauko ADFGVX šifras



Rokas = FXFFDVAAGA

Vižinerio šifras



Rokas

124

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| R | O | K | A | S |
| 1 | 2 | 4 | 1 | 2 |
| S | Q | O | B | U |



To be or not to be

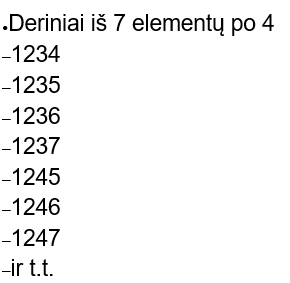
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T | O | B | E | O | R | N | O | T | T | O | B | E |
| 2 | 1 | 2 | 4 | 2 | 1 | 2 | 4 | 2 | 1 | 2 | 4 | 2 |
| V | P | D | I | Q | S | P | S | V | U | Q | F | G |

2124

**Derinių generavimas leksikografine tvarka.**

<https://calculla.com/combinations_generator?fbclid=IwAR3Sj4edt3XMjczIknWRJ_LT_Y-BrBx8-E3eb7e3AUzobzAO0N1aLwHfE8g>

1234567



1256

1257

1267

1345

1346

1347

1356

1357

1367

1456

1457

1467

1567

2345

2346

2347

2356

2357

2367

2456

2457

2467

2567

3456

3457

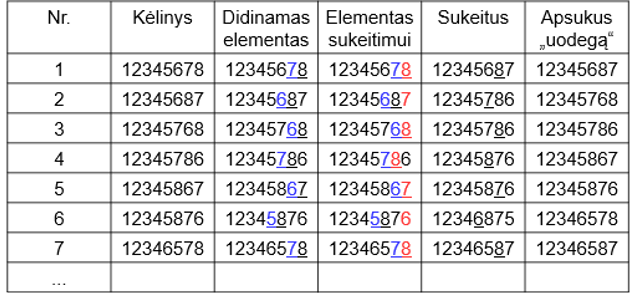
3467

3567

4567

**Kėlinių generavimas leksikografine tvarka**

https://calculla.com/permutations\_generator?fbclid=IwAR3Sj4edt3XMjczIknWRJ\_LT\_Y-BrBx8-E3eb7e3AUzobzAO0N1aLwHfE8g



1. 1234 1234 1234 1243 1243
2. 1243 1243 1243 1342 1324
3. 1324 1324 1324 1342 1342
4. 1342 1342 1342 1432 1423
5. 1423 1423 1423 1432 1432
6. 1432 1432 1432 2431 2134
7. 2134 2134 2134 2143 2143
8. 2143 2143 2143 2341 2314
9. 2314 2314 2314 2341 2341

**Euklido algoritmas**

|  |  |
| --- | --- |
| 4053 | 2222 |
| 4053-2222 = 1831 | 2222 |
| 2222 – 1831 = 391 | 1831 |
| 1831 – 391 = 1440 | 391 |
| 1440 – 391 = 1049 | 391 |
| 1049 – 391 = 658 | 391 |
| 658 – 391 = 267 | 391 |
| 391 – 267 = 124 | 267 |
| 267 – 124 = 143 | 124 |
| 143 – 124 = 19 | 124 |
| 124 – 19 = 105 | 19 |
| 105 – 19 = 86 | 19 |
| 86 – 19 = 67 | 19 |
| 67 – 19 = 48 | 19 |
| 48 – 19 = 29 | 19 |
| 29 – 19 = 10 | 19 |
| 19-10 = 9 | 10 |
| 10-9 = 1 | 9 |
| 9 – 1 = 8 | 1 |
| 8-1 = 7 | 1 |
| 7-1=6 | 1 |
| 6-1=5 | 1 |
| 5-1 | 1 |
| 4-1 | 1 |
| 3-1 | 1 |
| 2-1 | 1 |
| 1 | 1 |

|  |  |
| --- | --- |
| 4053 | 2222 |
| 4053/2222 = 1831 | 2222 |
| 2222/1831 = 391 | 1831 |
| 1831/391 = 267 | 391 |
| 391/267 = 124 | 267 |
| 267/124 = 19 | 124 |
| 124/19 = 10 | 19 |
| 19/10 = 9 | 10 |
| 10/9 = 1 | 9 |
| 9/1 | 0 |

**Išplėstinis Euklido algoritmas**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | X | Y | D | K |
| 1. | 1 | 0 | 150 |  |
| 2. | 0 | 1 | 65 |  |
| 3. | x1-x2\*k3 = 1 | y1-y2\*k3 = -2 | 20 | 2 |
| 4. | X2-x3\*k4 = -3 | Y2-y3\*k4 = 7 | 5(DBD) | 3 |
| 5. |  |  | 0 | 4 |
|  |  |  |  |  |

**150x+65y = 5**

**150 \* (-3) + 65 \* 7 = 5**

**RSA**

P = 13, q = 17

N = 13\* 17 = 221

Fi = (13-1)(17-1) = 192

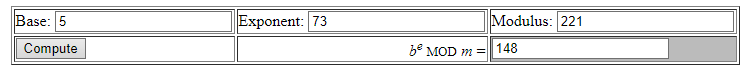
E = 73(pirminis skaicius)

73\*x = 1 mod 192

E^-1 = 121

C = 5(sifruojama zinute)^73 mod N(221)

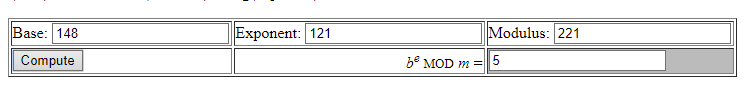
<https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html>



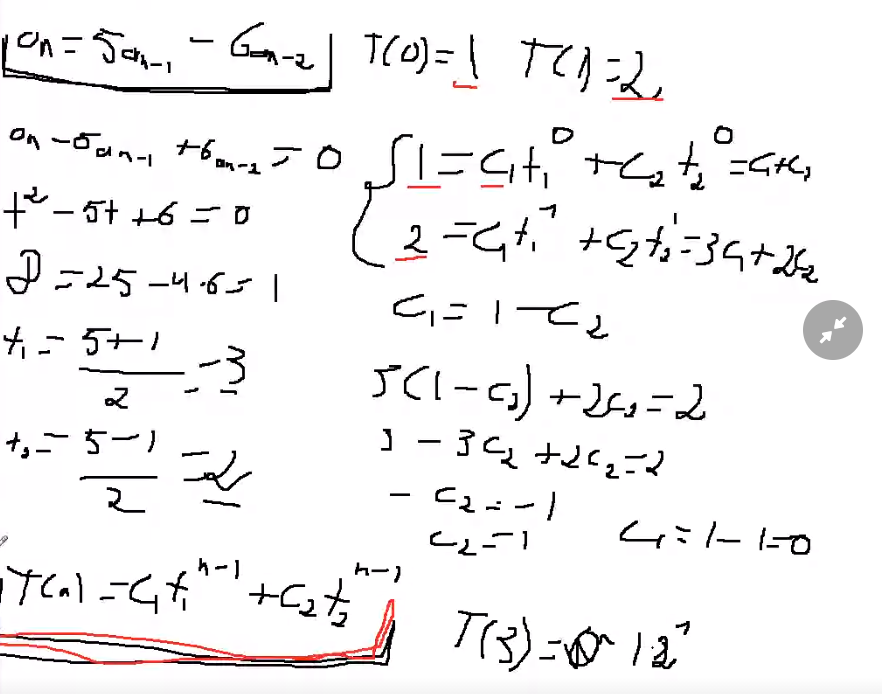
C = 148

ATSIFRAVIMAS:

T = 148^121 mod 221



**REKURENCIJA**



**KINŲ TEOREMA**

x = 2 mod 5 (5,7) (5,4) (7,4) – tarpusavy pirminiai visi lyginiai tinka

x = 3 mod 7

x = 1 mod 4

M = 5\*7\*4 = 140

1)

M1 = 5 5\*Yi + M/Mi \* Xi = 1

5Yi + 28Xi = 1

|  |  |  |  |
| --- | --- | --- | --- |
| Xi | Ti | Di | Ki |
| 1 | 0 | 28 |  |
| 0 | 1 | 5 |  |
| x1-x2\*k3= 1 | y1-y2\*k3 = -5 | 3 | 5 |
| X2-x3\*k4 = -1 | Y2-y3\*k4 = 6 | 2 | 1 |
| X3-x4\*k5 =2 | Y3-y4\*k5 = -11 | 1 | 1 |
|  |  | 0 | 2 |

5\*(-11) + 28\*2 = 1;

L1 = 28 \* 2 = 56;

-----------------------------------------------------------------------------------------------------------------------------------

7Yi + 20Xi = 1

|  |  |  |  |
| --- | --- | --- | --- |
| Xi | Ti | Di | Ki |
| 1 | 0 | 20 |  |
| 0 | 1 | 7 |  |
| x1-x2\*k3= 1 | y1-y2\*k3 = -2 | 6 | 2 |
| X2-x3\*k4 = -1 | Y2-y3\*k4 = 3 | 1 | 1 |
|  |  | 0 | 6 |

7\*3+20\*(-1) = 1

L2 = 20\*(-1) = -20

-----------------------------------------------------------------------------------------------------------------------------------

4Yi + 35Xi = 1

|  |  |  |  |
| --- | --- | --- | --- |
| Xi | Ti | Di | Ki |
| 1 | 0 | 35 |  |
| 0 | 1 | 4 |  |
| x1-x2\*k3=1 | y1-y2\*k3 =-8 | 3 | 8 |
| X2-x3\*k4 = -1 | Y2-y3\*k4 = 9 | 1 | 1 |
|  |  | 0 | 3 |
|  |  |  |  |

4\*9 + 35\*(-1) = 1

L3 = 35\*(-1) = -35

X = 56\*2 + (-20)\*3 + (-35)\*1 = 17

X2 =17+ 140 = 157

X3 = 157 + 140 = 297

**ISSIGELBEJIMUI:**

**x = 3 mod 5 x = b1 mod n1**

**x = 1 mod 7 x = b2 mod n2**

**x = 6 mod 8 x = b3 mod n3**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bi** | **Ni** | **Xi** | **BiNiXi** |
| **B1** | **N1 = n2\*n3** | **X1** | **B1N1X1** |
| **B2** | **N2 = n1\*n3** | **X2** | **B2N2X2** |
| **B3** | **N3 = n1\*n2** | **X3** | **B3N3X3** |

**N = n1\*n2\*n3;**

**Ni = N/ni**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bi** | **Ni** | **Xi** | **BiNiXi** |
| **3** | **n2\*n3 = 7\*8 = 56** | **1** | **3\*56\*1=168** |
| **1** | **n1\*n3 = 5\*8 = 40** | **3** | **1\*40\*3=120** |
| **6** | **n1\*n2 = 5\*7 = 35** | **3** | **6\*35\*3=630** |

**N = n1\*n2\*n3 = 5\*7\*8 = 280**

**56x1 = 1 mod 5**

**x1 = 1 mod 5**

**40x2 = 1 mod 7**

**5x2 = 1 mod 7**

**x2 = 3 mod 7**

**35x3 = 1 mod 8**

**3x3 = 1 mod 8**

**x3 = 3 mod 8**

**Paskutinis veiksmas:**

**X = 168 + 120 + 630 = 918**

**X = 918 mod 280**

**X = 78**

**ATVIRKŠTINIS MODULIU**

23 \* x = 1 mod 41

23 \* x – 41y = 1

23\*x + 41(-y) = 1

Sprendžiam išplestiniu euklido būdu:

|  |  |  |  |
| --- | --- | --- | --- |
| X | Y | D | K |
| 0 | 1 | 41 |  |
| 1 | 0 | 23 |  |
| x1-x2\*k3=-1 | y1-y2\*k3 =1 | 18 | 1 |
| X2-x3\*k4=2 | Y2-y3\*k4 =-1 | 5 | 1 |
| X3-x4\*k5 = -7 | Y3-y4\*k5 = 4 | 3 | 3 |
| X4-x5\*k6=9 | Y4-y5\*k6 =-5 | 2 | 1 |
| X5-x6\*k7=-16 | Y5-y6\*k7 = 9 | 1 | 1 |
|  |  | 0 | 2 |

23\*(-16) + ~~41\*(-9)~~ = 1

23\*(-16) = 1 mod 41

41 – 16 = 25

23\*25 = 1 mod 41

25 = 23^-1 mod 41

Atsakymas: 25

**OILERIO FUNKCIJA**

136|2

68 |2

34 |2

17 |17

1

2\*2\*2\*17 = 136;

2^3\*17

136 \* (1-1/2)\*(1-1/17) = 136\*16/34 = 64