**1. Kėlinių generavimas.**

1. **1234 1234 1243 1243**
2. **1243 1243 1342 1324**
3. **1324 1324 1342 1342**
4. **1342 1342 1432 1423**
5. **1423 1423 1432 1432**
6. **1432 1432 2431 2134**
7. **2134 2134 2143 2143**
8. **2143 2143 2341 2314**
9. **2314 2314 2341 2341**
10. **12345678 12345678 12345687 12345687**
11. **12345687 12345687 12345687 12345768**
12. **12345768 12345768 12345786 12345786**
13. **12345786 12345786 12345876 12345867**
14. **12345867 12345867 12345876 12345876**
15. **12345876 12345876 12346875 12346578**
16. **12346578 12346578 12346587 12346587**
17. **12346587 12346587 12346785 12346758**

**2. Vokiečių lauko ADFGVX šifras.**

Šis šifras pradėtas naudoti pirmojo pasaulinio karo pabaigoje. Perduodamas naudojant belaidę telegrafiją. Anksčiau šifras buvo vadinamas ADFGX, kuris buvo nulaužtas, po to ADFGVX, kuris taip pat buvo nulaužtas.

Pats pavadinimas tai yra iš kokių raidžių jis yra užšifruojamas. Raidžių pasirinkimas toks, kad Morzės abėcėlėje kuo labiau skirtųsi.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | A | D | F | G | V | X |
| A | a | b | c | d | e | f |
| D | g | h | i | j | k | l |
| F | m | n | o | p | q | r |
| G | s | t | u | v | w | x |
| V | y | z | 0 | 1 | 2 | 3 |
| X | 4 | 5 | 6 | 7 | 8 | 9 |

EGZAMINAS – AVDAVDAAFADFFDAAGA

SAUSIS – GAAAGFGADFGA

KTU - DVGDGF

**3. Jei studentus iš grupės suskirstysime po 2, liks 1. Jei skirstysime po 3, liks 2. Jei skirstysime po 4, liks 1. Kiek studentų gali būti grupėje?**

x= 2 mod 3

x = 1 mod 4

M = 3\*4 = 12

Yi + M/Mi\*Xi = 1

1)

M1 = 3

3Yi + 4Xi = 1

|  |  |  |  |
| --- | --- | --- | --- |
| Xi | Yi | Di | Ki |
| 1 | 0 | 4 |  |
| 0 | 1 | 3 |  |
| x1-x2\*k3= 1 | y1-y2\*k3 = -1 | 1 | 1 |
|  |  | 0 | 3 |

L1 = 4\*1 = 4

2)

M2 = 4

4Yi + 3Xi = 1

|  |  |  |  |
| --- | --- | --- | --- |
| Xi | Yi | Di | Ki |
| 1 | 0 | 4 |  |
| 0 | 1 | 3 |  |
| x1-x2\*k3= 1 | y1-y2\*k3 = -1 | 1 | 1 |
|  |  | 0 | 3 |

L2 = 3\*(-1) = -3

X= 4 \* 2 + (-3)\*1= 5

X2 = 5 + 12 = 17

X3 = 17 + 12 = 29