**Ciphers**

**Substitucia - monoalfabeticke**

**Atbas** – zoberie sa pismeno, spocita sa jeho vzdialenost od zaciatku abecedy a nahradi sa pismenom ktore je tak isto vzdialene od konca abecedy.

|  |  |
| --- | --- |
| Plaintext | OKO ALBATROS |
| Ciphertext | LPL ZOYZGILH |

**Albam** – zoberie sa index pismena z prvej polky abecedy, vrati sa index pismena v druhej polovici

|  |  |
| --- | --- |
| Plaintext | OKO ALBRATROS |
| Ciphertext | BXB NYONGEBF |

**Polybiov stvorec** – pismena abecedy sa ulozia do tabulky o rozmeroch napr 6x6, potom sa sifruje podla indexu riadka a stlpca = kazdemu pismenu su priradene dve cisla. Skomplikovat sa to moze heslom, kde v heslo odstranime duplikaty pismen hesla, ulozime do tabulky, zvysne miesto v tabulke doplnime zvysnymi znakmi v abecede.

|  |  |
| --- | --- |
| Plaintext | KNIHA SIFER |
| Key | PAVEL |
| Cipher text | 34 41 32 31 12 45 32 24 14 44 |

Table:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| X | 1 | 2 | 3 | 4 | 5 |
| 1 | P | A | V | E | L |
| 2 | B | C | D | F | G |
| 3 | H | I | J | K | M |
| 4 | N | O | Q | R | S |
| 5 | T | U | W | X/Y | Z |

**Caesarova sifra** – kazde pismeno je zamenene o tri znaky dalsie, prip. Kluc moze byt cislo ktore udava o kolko sa posuva abeceda.

|  |  |
| --- | --- |
| Plaintext | MUNDUS VULT DECIPI SVET CHCE BYT KLAMAN |
| Key | 3 |
| Ciphertext | PXQGV YXOW GHFLSL VYHW FKFH EBW NOPQDQ |

**Jedno-dvojmiesta zamena** – kazdme pismeno abecedy plaintextu sa nahradi bud jednocifernym alebo dvojcifernym cislom. Pouziva sa k tomu tabulka. Zvycajne tu je 4 riadky a 7 stlpcov. Riadky sa oznacuju od druheho, takze pouzijem tri cisla a tieto tri cisla nemozu byt v oznaceniach pre riadky. Vsetko su to cislice od 1 do 10. Tabulku vyplnam ako Polybiov stvorec, zadam heslo, potom zvysne znaky. Na konci mozem cisla potriedit do 5-miestnych skupin.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| X | 0 | | 1 | 2 | 3 | 4 | 7 | 8 |
|  | A | | E | I | O | U | V | T |
| 5 | B | | P | C | Q | D | R | F |
| 6 | G | | S | H | U | J | W | K |
| 9 | L | | X | M | Y | N | Z |  |
| Plaintext | | JEN MALA UKAZKA TOHO JAK VYPADA VYSLEDNY SIFROVY TEXT | | | | | | |
| Ciphertext | | 64 1 94 92 0 90 0 4 68 0 97 68 0 64 0 68 7 93 51 0 54 0 7 93 61 90 1 54 94 93 61 2 58 57 3 7 93 8 1 91 8 | | | | | | |

**Substitucia – polyalfabeticke**

**TABULA RECTA** – tabulka zostavena z 26 zoradenych abecied

**Trithemiova sifra** – pismeno plaintextu sa vyhlada v prvom riadku, jeho siforvy ekvivalent sa nejde pod nim v abecede, ktora odpoveda poradiu znaku v plaintexte, teda prvy znak pomoocu prvej, druhy pomocou druhej…

|  |  |
| --- | --- |
| Indexes | 1 2 3 4 5 6 7 8 9 10 11 |
| Plaintext | O K O A L B A T R O S |
| Ciphertext | OLQ DPGGAZXC |

**Vigenere – periodicke heslo** – vyuzitie tabulky ako pri Trithemiusoej sifre. Vyber prevodovej abecedy urcuje znak hesla. Heslo si odosielatel napise opakovane nad text, aby vedel aku abecedu ma pouzivat.

|  |  |
| --- | --- |
| Key | O K N O O K N O |
| Plaintext | A L B A T R O S |
| Ciphertext | O V O O H B B G |

**Vigenere – autokey** – kluc tvori dohodnute heslo spojene s textom

|  |  |
| --- | --- |
| Key | D A L B A T R O |
| Plaintext | A L B A T R O S |
| Ciphertext | D L M B T K F G |

**Gronsfeld**  - namiesto Tabula Recta o 26 zoradenych abecedach sa pouziva zjednodusena tabulka o 10 zoradenych abecied. K vyberu abecedy sa pouziva kluv ktory sa periodicky zapise nad plaintext. Sifrovy text sa urci dalej ako vo Vigenerovom systeme. Kluc urci riadok…

|  |  |
| --- | --- |
| Key | 5297 35267352 |
| Plaintext | DNES NEPRIJDU |
| Ciphertext | IPNZ QJRAPMIW |

**Beaufort** – heslo sa zapise periodicky nad plaintext. Teraz sa vyberie riadok ktory zacina prvym pismenom plaintextu, ocami sa vyhlada prvy znak kluca v tomto riadku a potom sa pozrie do tabulky na znak v prvom riadku v tom isto stlpci.

|  |  |
| --- | --- |
| Key | P A V E L P A V |
| Plaintext | A L B A T R O S |
| Ciphertext | P P U E S Y M D |

**Playfair** – cely plaintext zapiseme velkymi pismenami, bez medzier a napr odstranime pismeno Q, to budeme nahradzat pismenom K. Nasledne text rozdelime na bigramy – dvojice pismen. Pokial by v bigrame boli dve rovnake pismena, oddelime ich X a Z, tymto nam vznikne namiesto jednoho bigramu dva. Pokial je dlzka plaintextu neparna, na koniec doplnime este X. Teraz vytvorime abecedny stvorec sifry Playfair. K tou potrebujeme heslo, najlepsie s dlzkou 5 pismen a viac. Kazde pismeno v nom moze byt pouzite iba raz. Teraz vytvorime stvorec s hranou dlhou 5. Najprv sa don zapise heslo, potom sa zaplni ostavajucimi pismenami okrem Q. Sifrovanie je zalozene na skutocnosti, ze bigram sa moze vyskytnut len v jednom z troch stavov: moze byt spolocne v jednom riadku, jednom stlpci alebo kazde z pismen je v inom riadku a inom stlpci. Potom sa sifruje podla pravidiel:

1. Pokial lezia obe pismena v jednom riadku, je kazde pismeno bigramu nahredene pismenom leziacom v tabulke napravo od neho. Posledne pismeno v riadku sa nahradi prvym pismenom toho isteho riadku.
2. Pokial lezia obe pismena v jednom stlpci, je kazde pismeno bigramu nahradene pismenom pod nim. Ak je pismeno v poslednom riadku, je nahradene prvym pismenom toho isteho stlpca
3. Pokial je kazde pismeno v inom riadku a stlpci, je kazde z nich nahradene pismenom nachadzajuceho sa v priesecniku jeho vlastneho riadku a stlpca obsahujuceho druhe pismeno. Najskor sa urcuje priesecnik riadku prveho pismena.
4. Vysledny text sa uklada do patic, do poslednej patky mozeme doplnit X

|  |  |
| --- | --- |
| Key | HESLO |
| Plaintext | TATO SIFRA JE DOCELA JEDNODUCHA |
| Ciphertext | PDULE KCUBG LBSFS OBGLB UFFTA SFVXX |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| H | E | S | L | O |
| A | B | C | D | F |
| G | I | K | M | N |
| P | Q | R | T | U |
| V | W | X | Y | Z |

**Transpozicia**

**Jednoducha transpozicia**  - najprv si text prepiseme do medzinarodnej abecedy. Teraz zvolime kluc, ten urcuje velkost transpozicnej tabulky a poradie, v akom sa z nej vypisuju stlpce. Zvykne byt okolo 20 tich pismen dlhy. Pomocou permutacneho vycislenia sa ziska permutacny kluc. To spravim priradenim cisel podla toho, ako idu pismena za sebou v abecede. Pokial je viac pismen v texte, nizsie cislo ma to viac nalavo. Pokial su dve pismena vedla seba, odstrania sa duplikaty. Potom zostavime tabulku. Koniec tabulky zaplnim nahodnymi znakmi. Text sa ziska vypisnaim stlpcov v poradi, v akom je dane permutacne vycislenie, potom dam text do patic.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5 | 2 | 7 | 8 | 3 | 1 | 9 | 4 | 10 | 6 |
| K | D | Y | Z | S | E | N | A | S | V |
| E | T | E | O | B | J | E | V | I | O |
| P | R | A | V | D | O | V | Y | G | E |
| N | I | U | S | P | O | Z | N | A | T |
| E | H | O | P | O | D | L | E | T | O |
| H | O | Z | E | S | E | P | R | O | T |
| I | N | E | M | U | S | P | I | K | N |
| O | U | V | S | I | C | H | N | I | H |
| L | U | P | A | C | I | D | Q | W | E |

|  |  |
| --- | --- |
| Key | N E P R E C T E T O |
| Perm key | 5 2 7 8 3 1 9 4 10 6 |
| Plaintext | KDYZ SE NA SVETE OBJEVI OPRAVDOVY GENIUS POZNATE HO PODLE TOHO ZE SE PROTI NEMU SPINKOU VSICHNI HLUPACI |
| Ciphertext | EJOOD ESCID TRIHO NUUSB DPOSU ICAVY NERIN QKEPN EHIOL VOETO TNHYE EAUOZ EVPZO VSPEM SANEV ZLPPH DSIGA TOKIW |

**Jednoducha transpozicia – neuplna tabulka** – je to to iste ako predchadzajuce ale nedoplnime tabulku o nahodne znaky na konci. Tento system je silnejsi.

|  |  |
| --- | --- |
| Key | N E P R E C T E T O |
| Perm key | 5 2 7 8 3 1 9 4 10 6 |
| Plaintext | KDYZ SE NA SVETE OBJEVI OPRAVDOVY GENIUS POZNATE HO PODLE TOHO ZE SE PROTI NEMU SPINKOU VSICHNI HLUPACI |
| Ciphertext | EJOOD ESCID TRIHO NUUSB DPOSU ICAVY NERIN KEPNE HIOLV OETOT NHYEA UOZEV PZOVS PEMSA NEVZL PPHSI GATOK I |

**Uhlopriecko – stlpcova transpozicia** – ako aj pri predchodzej si z kluca odstran pismena ktore idu hned po sebe, potom z toho spravim permutacny kluc a vytvorim tabulku. Teraz si urcim pismena A, pri sifrovani ziskam polohu tohoto pismena v kluci (moze byt aj viac poloh) a idem uhloprieckovo zlava hore doprava dole. Text sa sifruje v tomto poradi. Potom si zoberiem pismena B. Idem od konca kluca, najdem kazdy vyskyt a uhlopriecka teraz pojde zprava hore do lava dole a takto ukldadam pismena do sifroveho textu. Tie pismena ktore som pouzil v prvej uhlopriecke sem nedavam. Potom idem postupne v poradi permutacneho kluca a beriem pismena po stlpcoch zhore dole ako v predchadzajucej sifre. Tie pismenka ktore sa vyskytli uz v jednej alebo v druhej uhlopriecke nezapocitavam.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **E** | **I** | **F** | **E** | **L** | **O** | **V** | **A** | **V** | **E** | **Z** |
| **2** | **6** | **5** | **3** | **7** | **8** | **9** | **1** | **10** | **4** | **11** |
| L | A | S | K | A | T | E | M | E | R | N |
| A | H | R | A | Z | U | J | E | M | Y | S |
| L | E | N | I | L | A | S | K | A | J | E |
| H | O | R | O | U | C | I | Z | A | P | O |
| M | E | N | U | T | I | N | A | V | S | E |
| C | H | N | O | O | S | T | A | T | N | I |
| A | P | O | T | O | M | Z | A | D | E | J |
| T | E | A | B | Y | V | A | S | E | N | B |
| Y | L | A | L | O | G | I | C | K | A |  |

|  |  |
| --- | --- |
| Uhlopriecka 1. | L H N O T S Z S K K Z A I A T E B R S |
| Uhlopriecka 2. | E E S C O O E Y E U L N H A |
| Ciphertext | lhnot szskk zaiat ebrse escoo eyeul nhamk zaaca lhmct aiutb lyjps nnasr rnaaa eoepl auooy otimv gjnta imaav deneo  eij |
| Key | E I F F E L O V A V E Z |

**Zlomkove**

**Bifid** – vytvorim polybiov stvorec na zaklade nejakeho hesla. Prejdem kazde pismeno v slove a najdem jeho riadok a stlpec vo stvorci. Tieto udaje zapisem do dvoch riadkov, medzi kazdym slovom vynechavam v tychto riadkoch medzery. Teraz nam vysli obdlzniky v dvoch riadkoch – kazde slovo tvori obdlznik. Citam znaky v obldzniku po dvoch po riadku, prve cislo v dvojici urcuje riadok a druhe stlpec sifroveho textu v tabulke. Takto vytvorim cely text.

|  |  |
| --- | --- |
| Plaintext | NOVY TYP SIFRY |
| Key | ALBATROS |
| Ciphertext | MZFT RPP CFWKY |

**Trifid** – funguje tak isto ako bifid ale pouzivaju sa tri tabulky, teda sa udavaju tri cisla.