Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет информатики и   
радиоэлектроники»

Факультет компьютерного проектирования

Кафедра инженерной психологии и эргономики

Дисциплина: Криптографические технологии

Отчет

**по Практическому заданию №2**

на тему: «Маршрутные и подстановочные шифры»

Студент: гр. 910902 Шарупич К. А.

Руководитель: Давыдович К.И.

Минск 2022

**Цель работы:** ознакомиться с шифрами маршрутной перестановки и шифром Плейфера, научиться шифровать и дешифровать сообщения с помощью данных шифров.

**Ход работы**

**Задание 1**

Найти ключ по шифру Плейфера.

**Открытый текст:**

«Please note that spaces and punctuation characters have been removed before encryption».

**Шифротекст:** «LMBEUDOPUASIIYUNEDDUDOENSPARTEYOPODGCTEDUASTIDZBCBDPUCNPZBACBKMTDZDPGWZOYOPO»

**Выполнение задания**

Первоначальный вид ключа

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

Разобьем на биграммы.

1) PL – LM

2) EA – BE **// А – левее Е**

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

3–9) SE – UD, NO – OP, TE – UA, TH – SI, AT – IY, SP – UN, AC – ED

10 – 15) ES – DU, AN – DO, DP – EN, UN – SP, CT – AR, UA – TE

16 – 21) TI – YO, ON – PO, CH – DG, AR – CT, AC – ED, TE – UA

22 – 27) RS – ST, HA – ID, VE – ZB, BE – CB, EN – DP, RE – UC

28 – 33) MO – NP, VE – ZB, DB – AC, EF – BK, OR – MT, EX – DZ

34 – 38) EN – DP, CR – GW, YP – ZO, TI – YO, ON – PO

**Ключ: BCD.**

**Задание 2**

Необходимо зашифровать свою фамилию и имя шифром маршрутной перестановки.

**Выполнение задания**

Шарупич Ксения **Маршрут вписывания**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| У | К | С | Я |  |
| Р | П |  | Е | И |
| Ш | А | И | Ч | Н |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Маршрут выписывания**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Зашифрованный текст:** \_ИНЯЕС КПУРШАИЧН

**Задание 3**

Зашифровать фамилию и имя с помощью шифра Плейфера.

**Выполнение задания**

Ключ: Monday

Sharupich Kseniya - Sh ar up ic hK se ni ya - QK NT MU RI IL XK CR FM

**Зашифрованный текст: QKNTMURIILXKCRFM**

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

**Вывод.** В ходе лабораторной работы был практически примененшифрмаршрутной перестановки и шифр Плейфера.