Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования

Кафедра ИПиЭ

Дисциплина: Криптографические технологии

Отчет
**по Лабораторной работе №2**
на тему «Маршрутные и подстановочные шифры»

Студент гр. 910902 Шпак В.А.

Проверил Давыдович К.И.

Минск 2022

***Цель работы:*** изучить шифр маршрутной перестановки и шифр Плейфера, научиться дешифровать текст.

***Ход работы:***

**Задание 1.**

Открытый текст:

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

Шифротекст:

LMBEUDOPUASIIYUNEDDUDOENSPARTEYOPODGCTEDUAS TIDZBCBDPUCNPZBACBKMTDZDPGWZOYOPO

1. Для начала в качестве ключа был взят алфавит.

Ключ:

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

Результат:

pl ad te no qe th dt sp dc et yi cp un bq ud ti on bi ds dc qe rs dy we ba eo se mo we eb eg or ey eo br yp ti on

Открытый текст:

Pl ea se no te th at sp ac es an dp un ct ua ti on ch ar ac te rs ha ve be en re mo ve db ef or ex en cr yp ti on

2. Возьмем первую биграмму, которая не совпадает и попытаемся поменять ключ для правильного дешифрования. Так как биграмма BE->ea, но у нас BE->ad, то сместим B в первую ячейку и A перед E.

Ключ:

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

Результат:

pl ea re no te th at sp ab er am cp un dt ua ti on wd as ab te rs ga ve de em se mo ve cd ef or ew em dr yp ti on

Открытый текст:

Pl ea se no te th at sp ac es an dp un ct ua ti on ch ar ac te rs ha ve be en

re mo ve db ef or ex en cr yp ti on

3. Возьмем следующую биграмму. При нашем ключе UD->re, в то время как должна UD->se. Как можем заметить UD образует прямоугольник и для верной расшифровки было принято решение переместить букву D в столбец с буквой S, т.е. поменять D и C местами. Тогда получаем следующий ключ:

Ключ:

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

Результат:

pl ea se no te th at sp ac es an dp un ct ua ti on ch ar ac te rs ha ve be en re mo ve db ef or ex en cr yp ti on

Открытый текст:

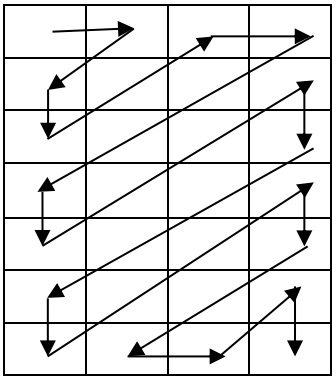
Pl ea se no te th at sp ac es an dp un ct ua ti on ch ar ac te rs ha ve be en re mo ve db ef or ex en cr yp ti on

Как можем заметить наш результат полностью совпал с исходным открытым текстом. В итоге ключевым словом оказалось: BCD.

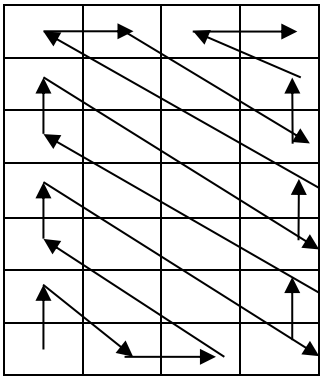
**Задание 2.**

| | | | |
|---|---|---|---|
| S | H | _ | V |
| P | K | I | I |
| A | K | Y | A |
| T | R | _ | N |
| O | A | A | D |
| L | X | R | N |
| E | O | V | A |

Исходная таблица



Маршрут вписывания



Маршрут выписывания

Исходный текст:

SHPAK_VIKTORYIA_ALEXANDROVNA

Зашифрованная фраза:

ELOVXOTARANARAPK_DNYKSHIAI_V

**Задание 3**. Зашифровать ФИО с помощью шифра Плейфера

Ключ

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

Открытый текст:
Shpak Viktoryia Alexandrovna
Шифртекст:
Sh pa kV ik to ry ia Al ex an dr ov na
QK WG FY CH ZE DV NB EG BZ GA EA UZ AG

**Вывод:** таким образом, в ходе лабораторной работы были изучены шифр маршрутной перестановки и шифр Плейфера, а также получены навыки шифрования и дешифрования с помощью изученных шифров.