

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ  
Кафедра кібербезпеки

**Дисципліна “Системи та засоби криптоаналізу”**

**Звіт до лабораторної роботи № 7-8**  
**на тему “ Поліграмний шифр Хілла і дослідження методів його**  
**криптоаналізу. Частина 1-2. ”**

Студент

Борщ Д.О.

Варіант

№ 1

Група

КБ-01

Перевірила

Лаврик Т.В

**Суми 2023**

## ЗВІТ

**Завдання** (10 б.). Здійснити шифрування і розшифрування тексту, використовуючи шифр Хілла.

Для шифрування вибрати самостійно україномовний текст/

У якості ключа взяти власне прізвище та ім'я (довжина має бути кратна числу 3),  $m = 3$ .

*У звіті подати детально всі дії, що виконуються під час шифрування та розшифрування. Результат може супроводжуватися програмною реалізацією.*

### Результати роботи

**Частина 1.** Зашифрувати текст, використовуючи шифр Хілла для  $m=3$ .

```
dmytro@thonkpad ~/Study/SZK/Lab_7-8 main $ python -m HillCipher --key ДМИ
ТРОБОР --encrypt
Enter input text: ТЕСТТЕКСТ
Input text:
ТЕСТТЕКСТ

Input matrix:
[[22 22 14]
 [ 6 22 21]
 [21  6 22]]
Key array:
[[ 5 22  1]
 [16 20 18]
 [10 18 20]]
Output Matrix:
[[ 263  850  748]
 [ 600  900  736]
 [ 554 1040  958]]

Encrypted text is:
ЯХТЕЗИЦНБ
dmytro@thonkpad ~/Study/SZK/Lab_7-8 main $
```

## Результат шифрування

### Частина 2. Розшифрувати текст, використовуючи шифр Хілла для $m=3$ .

```
dmytro@thonkpad ~/Study/SZK/Lab_7-8 main $ python -m HillCipher --key ДМИ  
ТРОБОР --decrypt  
Enter input text: ЯХТЕЗИЦНБ  
Input text:  
ЯХТЕЗИЦНБ  
  
Input matrix:  
[[32  6 26]  
 [25  9 17]  
 [22 10  1]]  
Key array:  
[[ 5 22  1]  
 [16 20 18]  
 [10 18 20]]  
Inverted key:  
[[31. 25.  4.]  
 [28. 15. 28.]  
 [22.  7. 24.]]  
Output Matrix:  
[[1705. 1887. 1407.]  
 [ 451.  583.  435.]  
 [1235. 1011.  715.]]  
  
Decrypted text is:  
ТЕСТЕКТ  
dmytro@thonkpad ~/Study/SZK/Lab_7-8 main $
```

## Приклад роботи з великим текстом:

```
[ 414 468 386]
[ 526 746 724]
[ 421 982 892]
[ 337 908 810]
[ 572 908 834]
[ 473 618 598]
[ 168 656 480]
[ 553 1188 1034]
[ 500 740 660]
[ 650 1128 954]
[ 484 748 708]
[ 294 416 338]
[ 193 626 608]
[ 94 508 440]
[ 159 408 266]
[ 335 642 508]
[ 552 708 558]
[ 479 670 544]
[ 140 436 336]
[ 551 1152 994]]

Encrypted text is:
СЕШЕШГШЦГЬБАВАІФУІАРНСМРВПЧИЕЛАОГЦЗИОЖДЕІЧНФЦХОЙРІОСШЖЬУГЙУОИФВГДЕЛСГФДП
ІНІСМГФГШКАНОГЖСВОЕЯШРДЗВГЕВОВГМАЗЯЕІДРЕФЖМДФЮЯІБШСУЗЯЧУЮБЗУЖЧООНВАЗЮ
ВРШФРІАБРСЧИСУОКФЕІЯЦБАБФЖСКІДЕЙШСЪТЦБОЖСІІВОВІФЦМИНСМГГЯДИОЖАЗМРЛЧПЮЖНЗЕ
ГОЦИРМШРДЯІІЧІМБШЖЧОЙОВІЙФКЧЯДПМЦААНЬЛЯЧЕРЯПСЮАЧАШЕМОЕОЕЯНЖЖГАЕФВСОУВЗ
ШУАШКМУФЩЦЛІЩХХЦЕГКСПРШЧЕФЮЩЕЕМОЮЩОНВРМЦІТДІРХДШХХСГЯДДШХЖЧІСГІШЯІР
ЧСЧЛІІЯММАЧЧЛСУННЕЛГОЩЕЯДЦШОЗЛМГІЗЯТЯТДСФЯЕЯТЯДЦЕРУЧІЗОГКСЦАКЕДІЧЮЯОПЯ
БЕТЖЕІЯМНДРНОЩЖЕПЦЮЯПІРННРІПШЩШХПЧОІЧДТІГДГЗСАЧНЧФЦМИІФПВЧИПУАІРЦПЦ
ФДЦЧХДЛІІЗИДЖІББНОЛІНЖКГФІДЯЗИЦЦЕФЩБЗУЧДФЕИМШДКЮТПШДГПШБЕЗІТІЙЕФЖЧЕВЧИЦ
ШХІУТУІМБХЗШІТЖБББПШДПЖВМЧІУБЬЦІЦЛОСЧДЛДГІПЦУХІГДФУНОГДЧГІДГОКСХ
ВШІХІДЛВФГЦПФЮЖРЮТКГВЕТХІМЗЗОФШУЗБІГІОБГРХХШЦРІОААЙІДСДЕБЗУУШЖДШІЦІ
ЮЦЦПЕЩІОБЕФРГХЕШЩХЭПУМСЕБЯНСІІЛНРЯСКЕЕГФГВЩЮЗКМІНХІБФДЛДЮДХЦЗІАЙШПОАТІ
ХШЮІЯІЗРПЗНЖАДЮАМПАЛЬУВЛПХШУТРОЕУЮРХХБЕЗОІНЗІОГГЦХОХАІДКАБЕТТБЕРШЯКШІІ
ЧІВДЛДЛФЛНІМЖЕУБГ

dmytro@thonkpad ~/Study/SZK/Lab_7-8 main $

[ 800. 1238. 990.]
[1585. 2036. 1566.]
[1404. 1103. 749.]
[ 514. 835. 649.]
[ 802. 815. 577.]
[ 957. 780. 506.]
[ 890. 1023. 701.]
[ 819. 1008. 814.]
[ 505. 350. 208.]
[ 983. 1574. 1268.]
[1260. 1142. 806.]
[1462. 1364. 992.]
[1724. 1656. 1176.]
[1237. 1287. 971.]
[1145. 992. 726.]
[ 550. 505. 335.]
[1239. 1737. 1353.]
[ 841. 1074. 828.]
[ 447. 497. 369.]
[1479. 1206. 812.]]

Decrypted text is:
ТИСЯЧІТОНЕСЕНЬКИХДУДОЧОКРАПТОМЗАГРАВАЛИУДІДАВСЕРЕДИНІКАШЕЛЬКЛЕКОТІВУНЬОГОВ
ГРУДЯХКЛАВАУВУЛКАНІДОВГОІГРІЗНОІДУЖЕНЕСКОРОПІСЛЯНАЙВИЩИХНОТКОЛІДІБВУЖЕВ
ЕСЬСИНІЯЯКВІТКАКРУЧЕНОГОПАНИЧАВУЛКАНПОЧИНАВДІЯТИТОДІМІТІКАЛИХТОКУДІАВСЛІ
ДНАМДОВГОЩЕНЕСЛИЯДІДОВІГРОМІБЛАЖЕННЕКРЕКТИННЯТІКАЮЧИОДДІДОВОГОРЕВУОДНОГО
РАЗУСТРІБНУВЯЗПІДПОРІЧОКПРЯМОВТІВІНТЮТІВУВВИСОКИЙІГУСТИЙПРЕГУСТИЙІНСАМЕЦ
ВІВВЕЛИКИМИЗОЛОТИНИГРОНАМИЯКУПОПАНАРИЗАХАНАДРИЗАМИНОСИЛІСЯБДЖОЛИВИДИМОНЕВИ
ДИМОВЕЛИКЕТІЮТЮНЕЛИСТЯЗРАЗУОБПЛУТАЛОМЕНЕЯУПАВВЗЕЛЕНУГУШАВИНУЙПОЛІЗПОПІДЛИ
СТЯМПРОСТОДОІГРІВВОІРКАХТЕЖУЛІБДЖОЛИВОНИПОРАЛІСЬКОЛОЦВІТУІТАКПРУДКОЛІТ
АЛІДОСОНЯШНИКАДОМАКУДОДОМУІТАКІМБУЛОНІКОЛИЩОСІЛЬКІЯНАМАГАВСЬЯКНЕДРАЖНИ
ВІХТАКНОДНАЧОМУСЬМЕНЕЯНЕВКУСИЛАБДЖОЛЯЧЕЖАЛОХОЧІБОЛІТЬЗАТЕЖЕЖОЛИПОЧНЕСПЛ
АКАТІДІДУЖЕЧИНАТИДАЮТЬЗРАЗУНІДНУКОПІКУЯКУТРЕБАПРИКЛАДАТИДОБОЛЮЧОГОМІСЦЯТО
ДІБІЛЬШВИДКОПРОХОДИВАЗАКОПІКУМОЖНАБУЛОКУПИТИУНАСІЯЖОТИРИЦУКЕРКІВЖЕСМАК
УВАТИДОСАМОГОВЕЧОР

dmytro@thonkpad ~/Study/SZK/Lab_7-8 main $
```