Захист інформації в телекомунікаційних системах

Лекція № 3

Криптографічний захист інформації: загальні принципи побудови та найпростіші алгоритми

ХНУРЕ, факультет ІК, кафедра ІМІ
тел. 702-14-29, e-mail: d_cn@nure.ua

Доцент, к.т.н. Золотарьов Вадим Анатолійович

Література

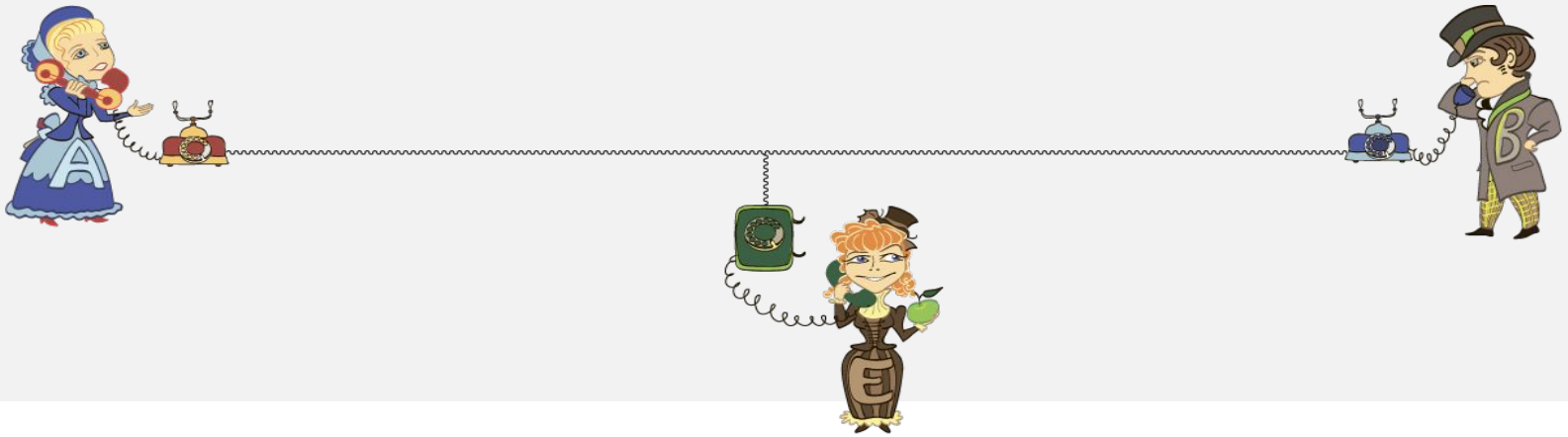
1. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів,БаК, 2003. – 144 с.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – Москва, Радио и связь, 1999.- 328 с.
3. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – Киев, Корнийчук, 2000. – 152 с.
4. Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. – Москва, СОЛОН-Пресс, 2002. – 256 с.

Питання 1

Основні терміни та визначення

Криптогра́фія (від грецького *kryptós* — прихований і *gráphein* — писати)

- наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації.



- **Криптографічна система захисту інформації** — це сукупність криптографічних алгоритмів, протоколів і процедур формування, розподілу, передачі й використання криптографічних ключів.
- Саме повідомлення називається **відкритим текстом**.
- Зміна виду повідомлення з метою приховати його суть називається **шифруванням**.
- Шифроване повідомлення називається **шифротекстом**.
- Процес перетворення шифротексту у відкритий текст називається **розшифруванням**.

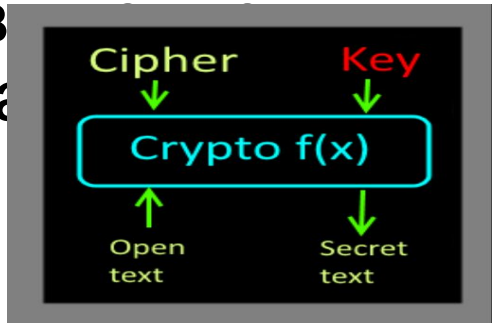
- **Криптоаналізом** називається розділ прикладної математики, що вивчає моделі, методи, алгоритми, програмні й апаратні засоби аналізу криптосистеми або її вхідних і вихідних сигналів з метою отримання секретних параметрів, включаючи відкритий текст.
- Криптоаналіз займається завданнями, які в математичному змісті зворотні завданням криптографії.
- Система криптографії й криптоаналізу утворює **криптологію**.

- Позначимо відкритий текст (повідомлення) як *M*.
- Позначимо шифротекст як *C (chipertext)*.
- Функція шифрування *E (is encryped)* діє на відкритий текст, створюючи шифротекст $E(M) = C$.
- Процес відновлення відкритого тексту по шифротексту є розшифруванням і виконується за допомогою функції розшифрування (is decoded)

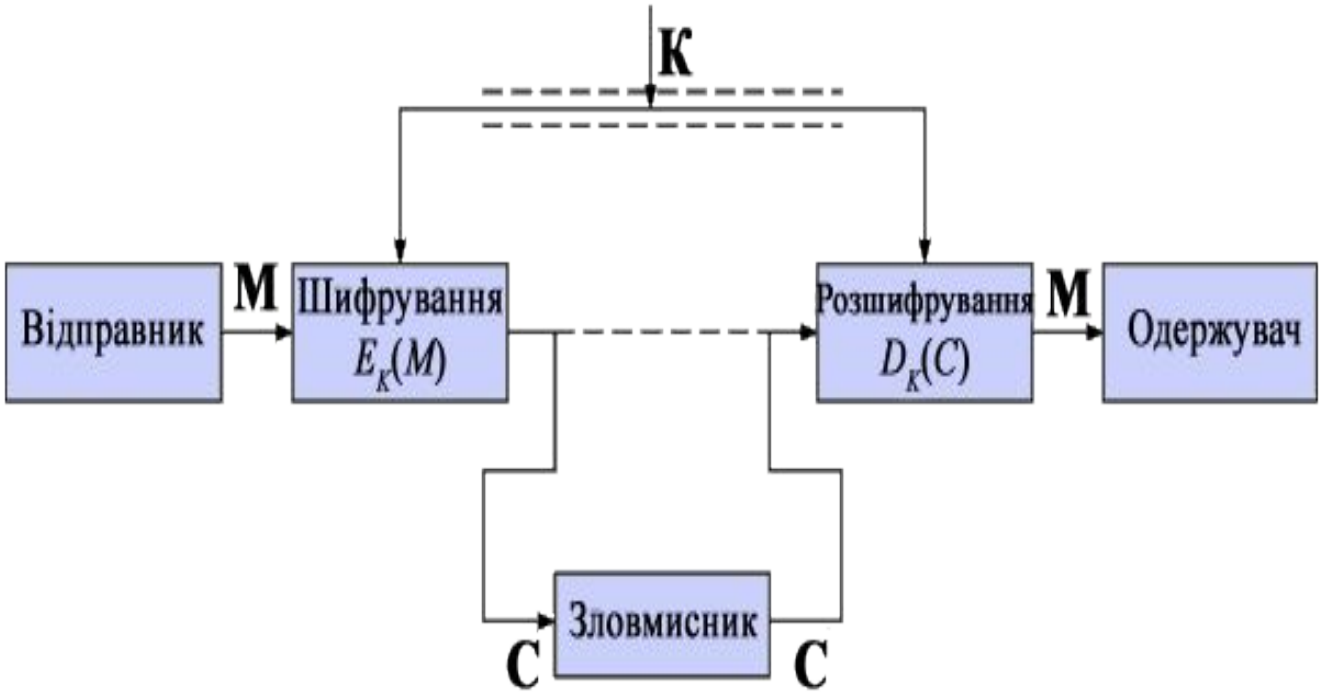
$$D{:}D(C) = M.$$

- Оскільки змістом шифрування й наступного розшифрування повідомлення є в… первісного відкритого тексту, то ма… виконуватися тотожність

$$D(E(M)) = M.$$



Узагальнена схема криптосистеми



- **Криптографічний алгоритм**, також називаний **шифром**, являє собою математичну функцію, яка використовується для шифрування й розшифрування.
- Якщо безпека алгоритму заснована на збереженні самого алгоритму в таємниці, це **обмежений алгоритм**.
- Сучасна криптографія розв’язує проблеми обмежених алгоритмів за допомогою ключа *K*.
- **Ключ** — це конкретний секретний стан певних параметрів алгоритму криптографічного перетворення даних, що забезпечує вибір тільки одного варіанта перетворення з усіх можливих для даного алгоритму.
- Множину можливих ключів називають **простором ключів**.
- Ключ, що використовується для ініціалізації системи, часто називають **майстер-ключем системи**.

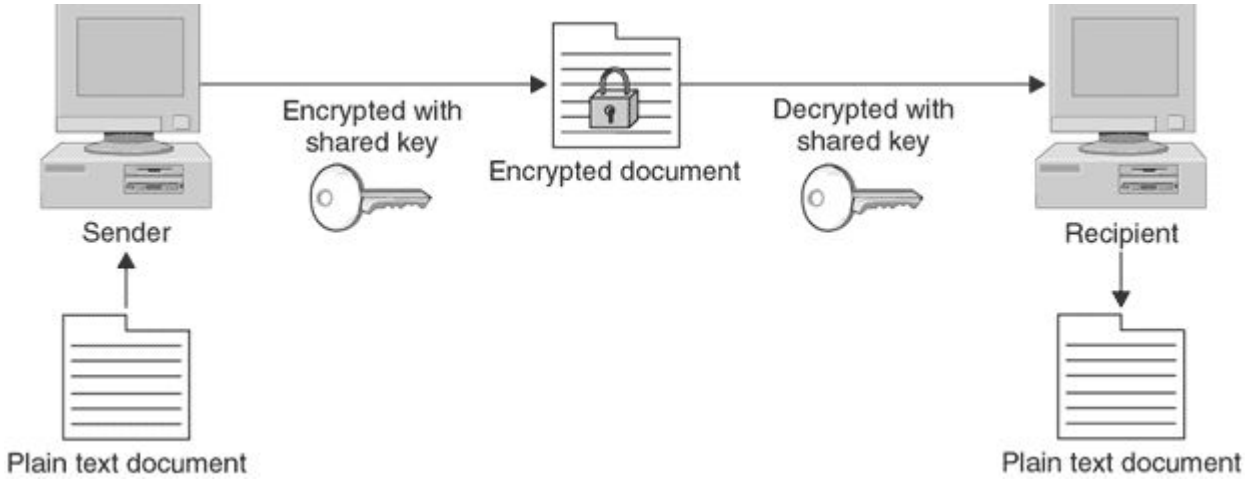
- З урахуванням використання ключа, функції шифрування й розшифрування запишуться як $C = E_K(C)$ і $D_K(C) = M$.
- При цьому має виконуватися тотожність

  $D_K(E_K(M)) = M$.
- Однак для деяких алгоритмів при шифруванні й розшифруванні використовуються різні ключі.
- У цьому разі $C = E_{K1}(M)$, $D_{K2}(C) = M$, а $D_{K2}(E_{K1}(M)) \equiv M$.
- Якщо алгоритм перетворення даних залежить від ключа, тобто застосовуються управляючі операції, шифр називається **шифром, що управляється** або керованим шифром

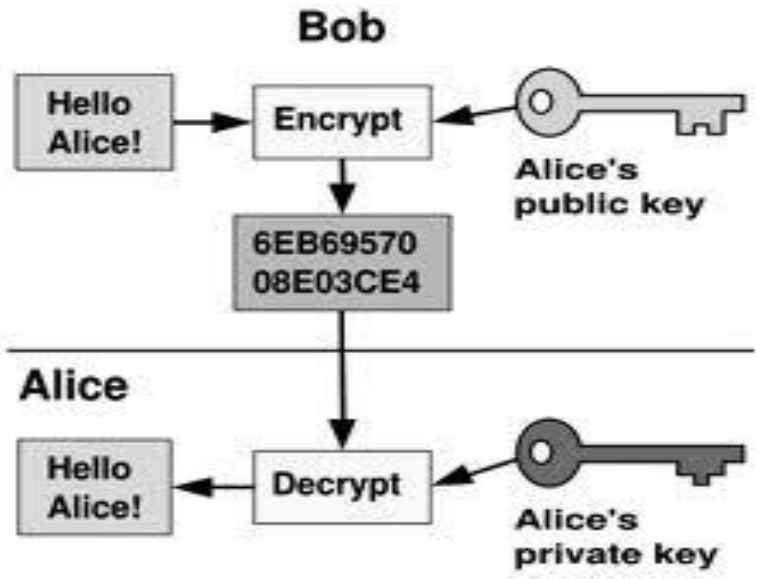
Криптографічні системи, у загальному випадку, класифікуються на основі таких трьох незалежних характеристик

- тип операцій з перетворення відкритого тексту в шифрований;
- число ключів, що використовуються;
- метод обробки відкритого тексту.

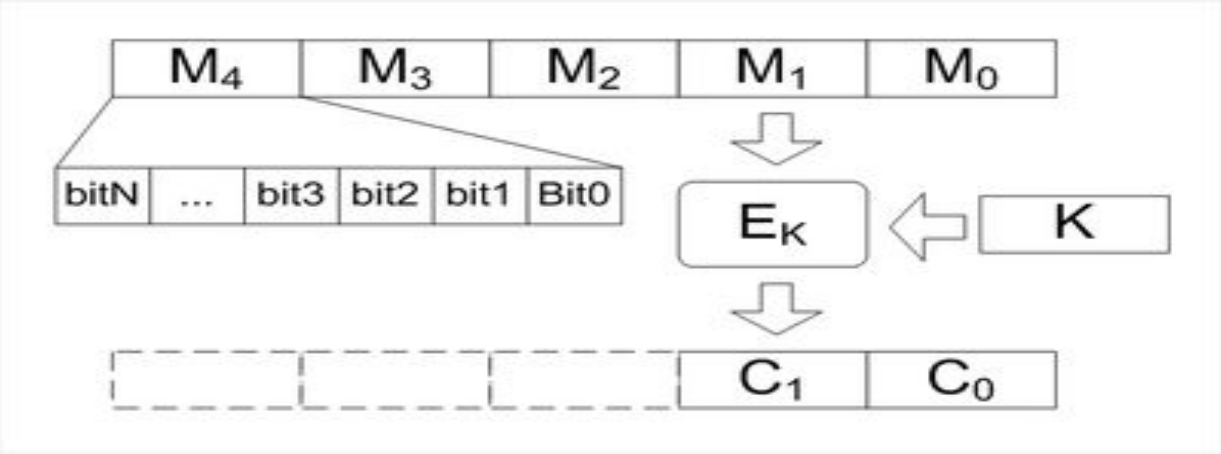
Якщо і відправник, і одержувач інформації використовують той самий ключ, система називається **симетричною**, системою з одним ключем або системою з секретним ключем



Якщо відправник і одержувач використають різні ключі (один відкритий, а інший секретний (таємний)), система називається **асиметричною**, системою із двома ключами або схемою шифрування з відкритим ключем.



Блокове шифрування передбачає обробку відкритого тексту блоками, так що в результаті обробки кожного блоку виходить блок шифрованого тексту.



При **потоковому шифруванні**

- шифрування всіх елементів відкритого тексту здійснюється послідовно, одне за іншим, у результаті чого на кожному етапі отримують по одному елементу шифрованого тексту.

До шифрів, які використовуються для криптографічного захисту інформації, висувають низку вимог:

- статистична безпека алгоритмів;
- надійність математичної бази алгоритмів;
- простота процедур шифрування й розшифрування;
- незначна надмірність інформації за рахунок шифрування;
- простота реалізації алгоритмів на різній апаратній базі.

Тією чи іншою мірою цим вимогам відповідають:

- шифри перестановок;
- шифри заміни;
- шифри гамування;
- шифри, засновані на аналітичних перетвореннях даних.

- Основним питанням аналізу будь-якої криптографічної системи захисту інформації є визначення ступеня її стійкості.
- **Стійкість криптографічної системи захисту інформації** є її здатність протистояти атакам порушника на інформацію

ься.

Питання № 2

ШИФРИ ПЕРЕСТАНОВКИ

Шифри перестановки

- Це симетричні шифри, в яких елементи вихідного тексту відкритого тексту міняються місцями.
- Елементами тексту можуть бути окремі символи, пари літер, трійка літер, тощо
- Типовий приклад - анаграми

Анаграма (грецькою *ανα-* — знову та *γράμμα* — літера)

- переставлення літер у слові , завдяки чому утворюється нове значення, прочитуване у зворотному напрямку (*тік — кіт*), постають псевдоніми (*Симонов — Номис*) чи слова (*мука — кума, літо — тіло*).

Олександр Ірванець

«Майже ідеальна рима»

Стодола, рів

Сто, доларів

Шифри перестановок

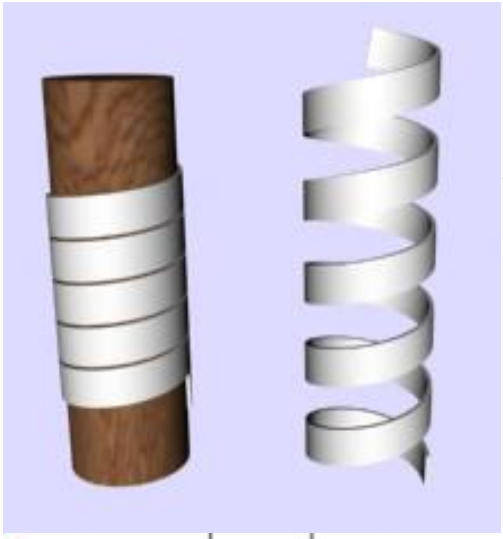
Шифри простої перестановки

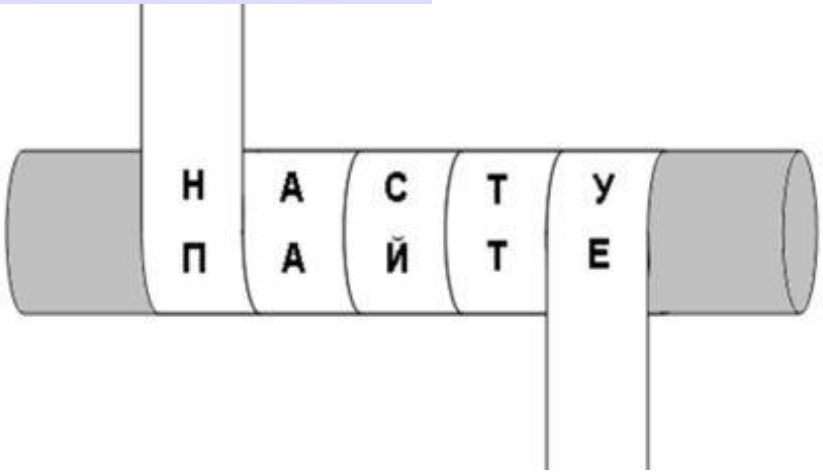
- Під час шифрування символи відкритого тексту переміщуються з вихідних позицій один раз

Шифри складної перестановки

- Під час шифрування символи відкритого тексту переміщаються з вихідних позицій в нові кілька разів

Сциталь (грецькою - σκυτάλη, жезл)





НПАСТУ
ПАЙТЕ

Математичний опис шифру «Сциталь»

- Зазвичай відкритий текст розбивається на відрізки рівної довжини і кожний відрізок шифрується (тобто в ньому переставляються літери) незалежно.
- Нехай, наприклад, довжина відрізків дорівнює n и σ – взаємооднозначне відображення множини $\{1,2, \ldots, n\}$ на себе.
- Тоді шифр перестановки працює так: відрізок відкритого тексту $x_1 \ldots x_n$ преобразуется перетворюється у відрізок шифрованого тексту $x_{\sigma(1)} \ldots x_{\sigma(n)}$.

Шифр частоколу (висота 2)

К^{р}и^{п}т^{о}г^{р}а^{ф}і^{я}

рпорфякитгаі

Матричні (табличні) шифри

- Явний текст записують послідовно рядок за рядком у таблицю.
- Літери криптограми виписують з цієї ж таблиці по стовпцям

Матричні (табличні) шифри

- Явний текст записують послідовно рядок за рядком у таблицю. Літери криптограми виписують з цієї ж таблиці по стовпцям
- пнкуаріувкитп ацпьотіисвиї

п	р	и	п	и
н	і	т	ь	с
к	у	п	о	в
у	в	а	т	и
а	к	ц	і	ї

Матричний (табличний) шифр з ключем

- Черговість стовпців визначена ключем шифру.
- ИСВИЇПНКУАПЬОТІ РІУВКИТПАЦ
- Крім того, можна використовувати два ключі – як для рядків, так і для стовпців

Б	І	Р	Ж	А
2	4	5	3	1
П	Р	И	П	И
Н	І	Т	Ь	С
К	У	П	О	В
У	В	А	Т	И
А	К	Ц	І	Ї

ИВСЇИУКНАПТОЫІПВУІКРАПТ ЦИ

		Б	І	Р	Ж	А
		2	4	5	3	1
Т	5	П	Р	И	П	И
О	3	Н	І	Т	Ь	С
В	2	К	У	П	О	В
А	1	У	В	А	Т	И
Р	4	А	К	Ц	І	Ї

		А	Б	Ж	І	Р
		1	2	3	4	5
А	1	И	У	Т	В	А
В	2	В	К	О	У	П
О	3	С	Н	Ь	І	Т
Р	4	Ї	А	І	К	Ц
Т	5	И	П	П	Р	И

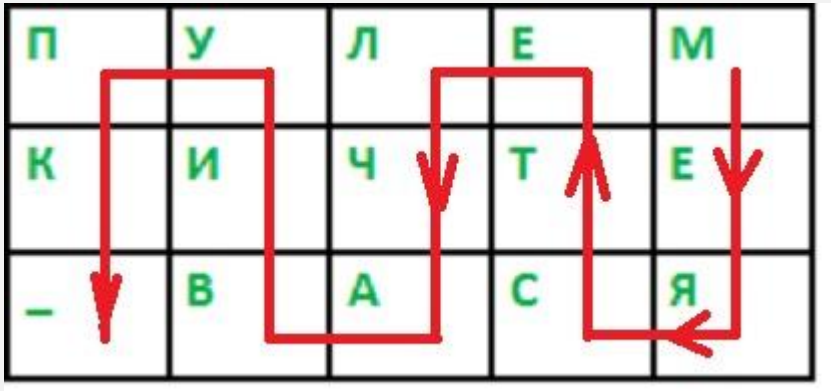
Кількість варіантів подвійної перестановки

Розмірність таблиці		Кількість перестановок		
M	n	M!	N!	Загалом
3	3	6	6	36
4	4	24	24	576
5	5	120	120	14400
5	6	120	720	86400
6	6	720	720	518400

Шифри перестановки з ускладненням по маршруту: поняття, приклади

Маршрутні табличні перестановки за нелінійним законом

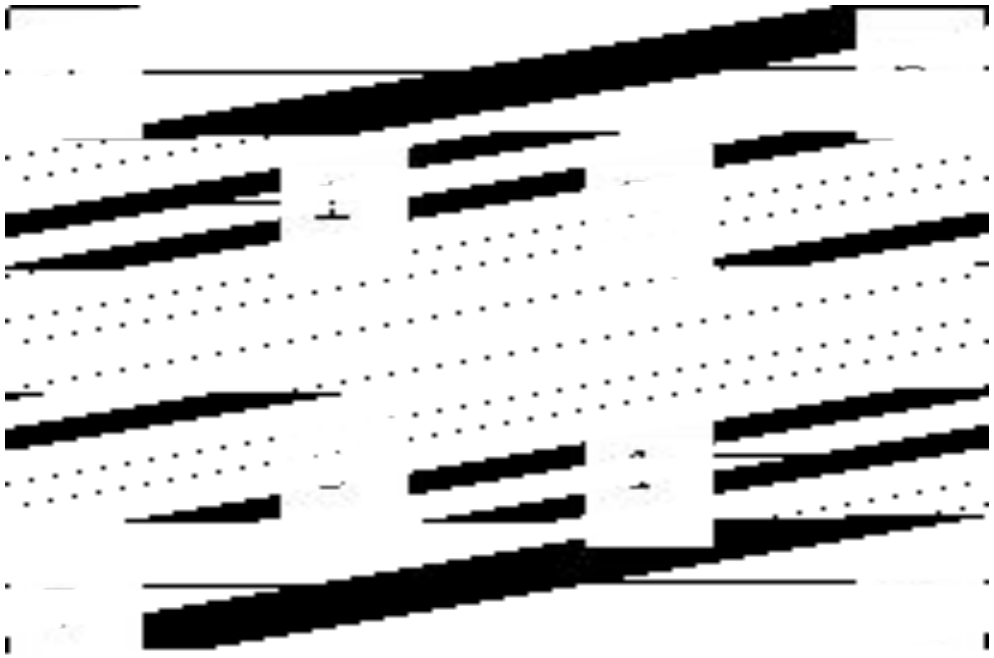
- Повідомлення записується до матриці послідовно по рядкам, а зчитування відбувається “змійкою”



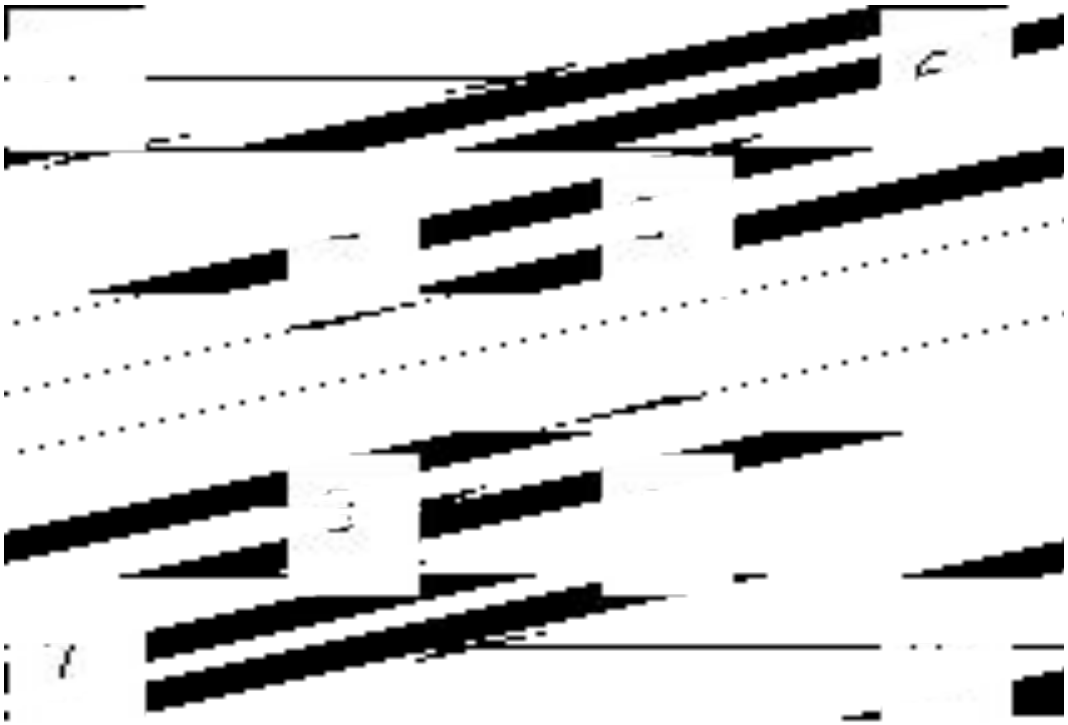
Маршрути Г`амільтона

- Крок 1. Вихідна інформація розбивається на блоки. Якщо довжина інформації, що шифрується не кратна довжині блоку, то на вільні місця останнього блоку розміщуються спеціальні службові символи – заповнювачі(наприклад*).
- Крок 2. Символами блоку заповнюється таблиця, в якій для кожного порядкового номера символу відводиться цілком визначене місце
- Крок 3. Зчитування символів з таблиці здійснюється за одним з маршрутів. Збільшення кількості маршрутів підвищує криптостійкість шифру. Маршрути вибираються або послідовно, або їхня черговість задається ключем К.
- Крок 4. Зашифрована послідовність символів розбивається на блоки фіксованої довжини L. Величина L може відрізнятися від довжини блоків, на які розбивається вихідна інформація на кроці 1.

Структура трьох мірного гіперкубу: Номера вершин кубу визначає послідовність його заповнюється символами тексту, що шифрується, при формуванні блоку. У загальному випадку
n-мірний гіперкуб має n^2 вершин. Для n=3



Послідовність перестановки символів 5-6-2-1-3-4-8-7



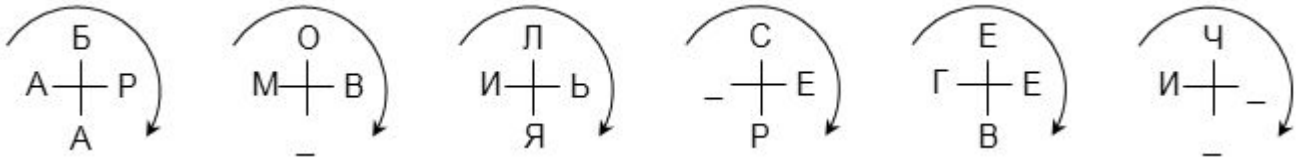
Послідовність перестановки символів 5-1-3-4-2-6-8-7

Шифр «Перехрестя»

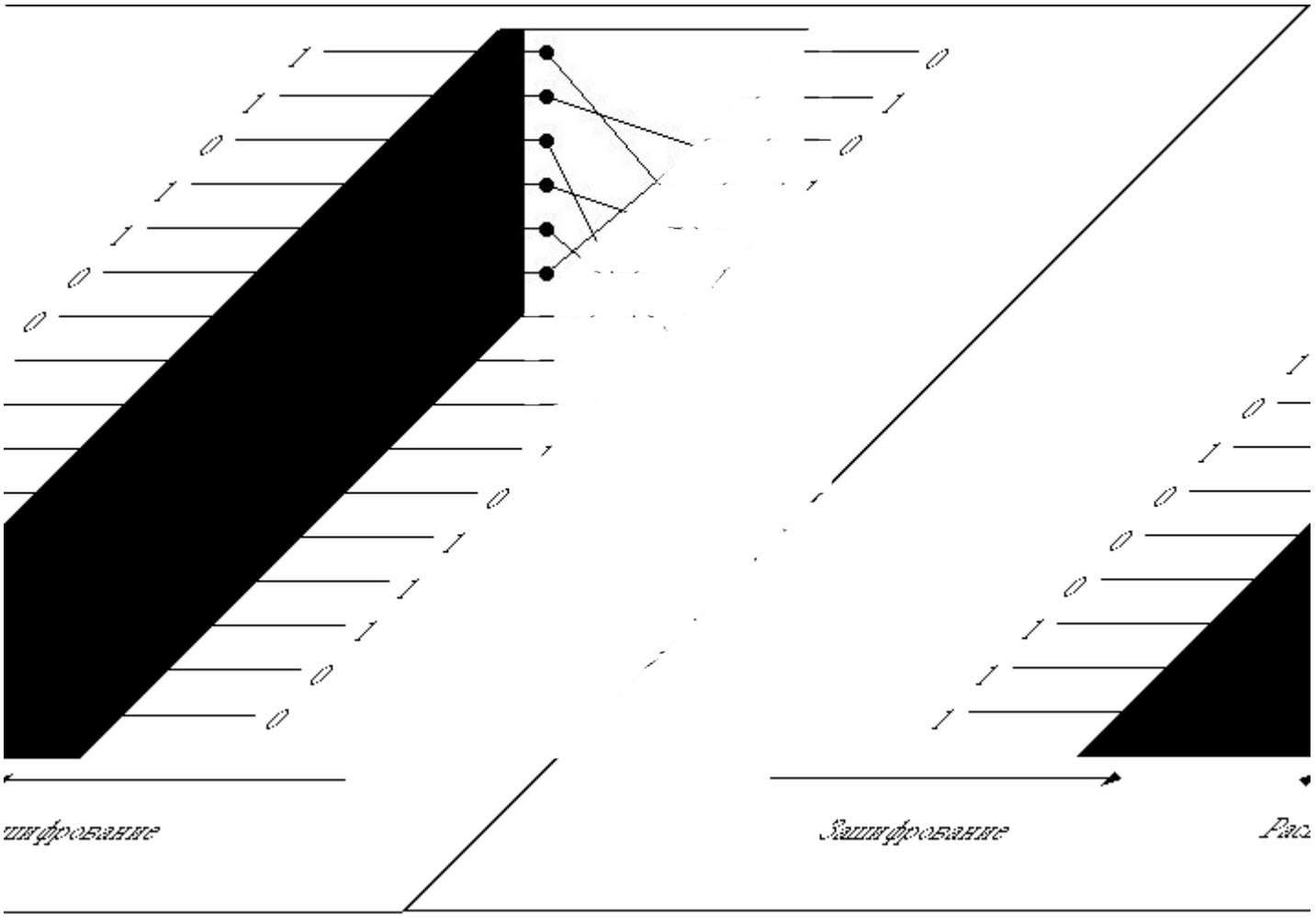
Літери беруться по рядкам. Спочатку береться певна кількість літер (N) з першого рядка, потім (2N) з 2-го рядка і знову (N) з третього рядка.

Для (N=3) Абрамов Илья Сергеевич =

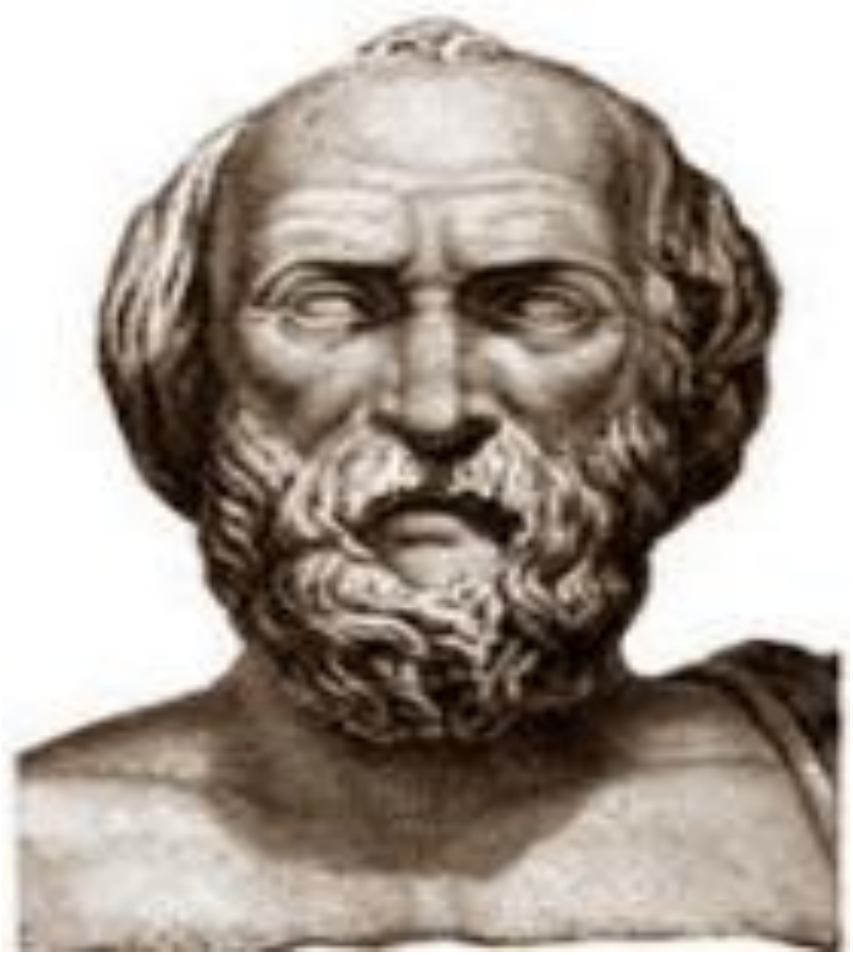
болармвиьа_ясеч_егеи_рв_

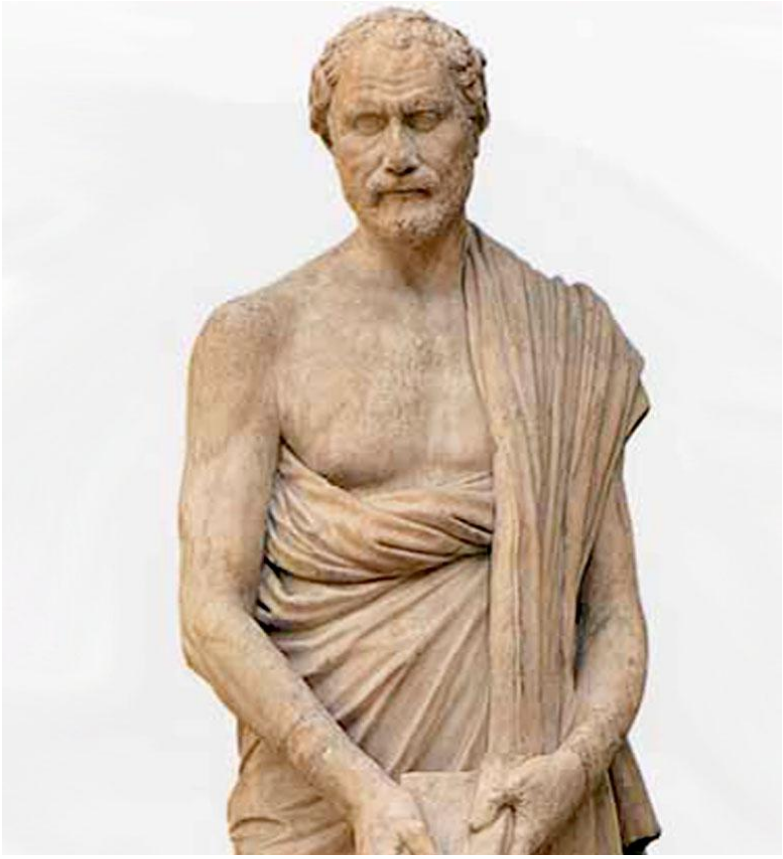


Апаратна реалізація методів перестановок



Поліб́ій (грецькою *Πολιβιος*, лат. *Polybius*, близько 201 до н. е., — близько 120 до н. е.)





Ρολιβιος

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	χ
χ	ν		φ	ι

- 2,1
- 2,5
- 1,1
- 5,1
- 3,3
- 5,1
- 2,5
- 2,2

Застосування абетки в’язниці

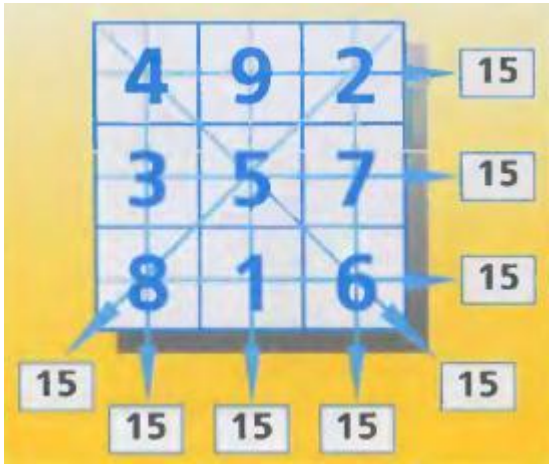
- Для тексту “ **Доцент**” криптограма виглядає так: 16_41_53_21_36_45

	1	2	3	4	5	6
1	А	Б	В	Г	Г`	Д
2	Е	Є	Ж	З	И	І
3	Ї	Й	К	Л	М	Н
4	О	П	Р	С	Т	У
5	Ф	Х	Ц	Ч	Ш	Щ
6	Ь	Ю	Я		`	.

“Тарабарська” мова – «Хапай мішок хутчіше»

- ТАРА – ХА – БАРА – ПАЙ – ТАРА – МІ-БАРА – ШОК- ТАРА – ХУТ- БАРА-ЧІ-ТАРА - ШЕ

Магічні квадрати



А́льбрехт Дю́рер (*Albrecht Dürer)*, 21.05.1471 – 06.04.1528

Квадрат Дюрера – «Меланхолія»

Прилітаю восьмого

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	М
І	О	С	Ю
В	Т	А	Ь
Л	Г	0	П

Кількість варіантів магічних квадратів перестановки (не рахуючи обертів на 90 градусів)

Розмір таблиці	Кількість варіантів
3 x 3	1
4 x 4	880
5 x 5	250000

Арма́н-Жан дю Плессі́ де Рішельє (*Armand-Jean du Plessis, duc de Richelieu*; 9 вересня 1585, — 4 грудня 1642)

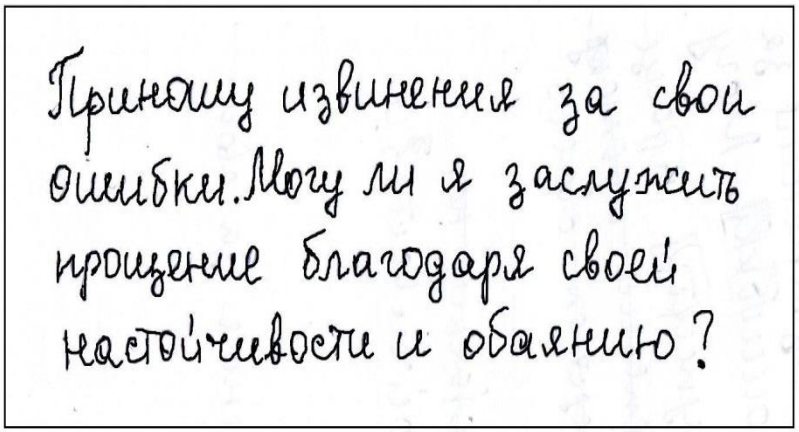
Шифр Рішельє

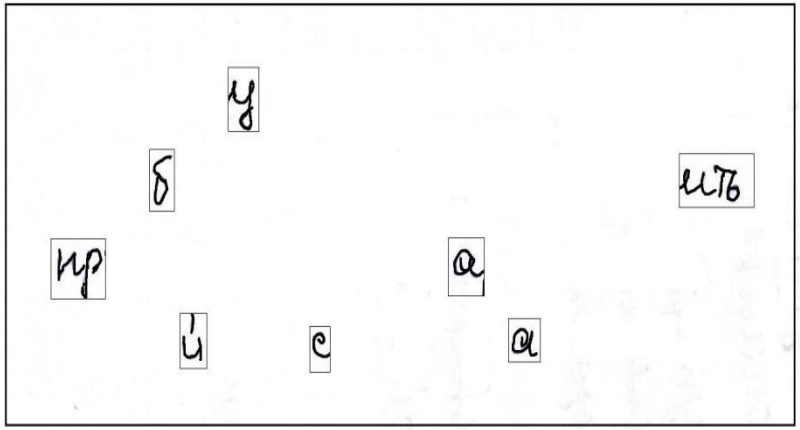
- Відкритий текст розбивається на відрізки,
- Всередині кожного відрізка літери переставляються у відповідності до фіксованої перестановки

Шифр Рішельє

- Відкритий текст: «шифр Рішельє»
- Шиф рршш ельє
  Ключ: (312) (4132) (3142)
  Зашифрованный текст: фши шршр ьеєл

Решітки (трафарети)

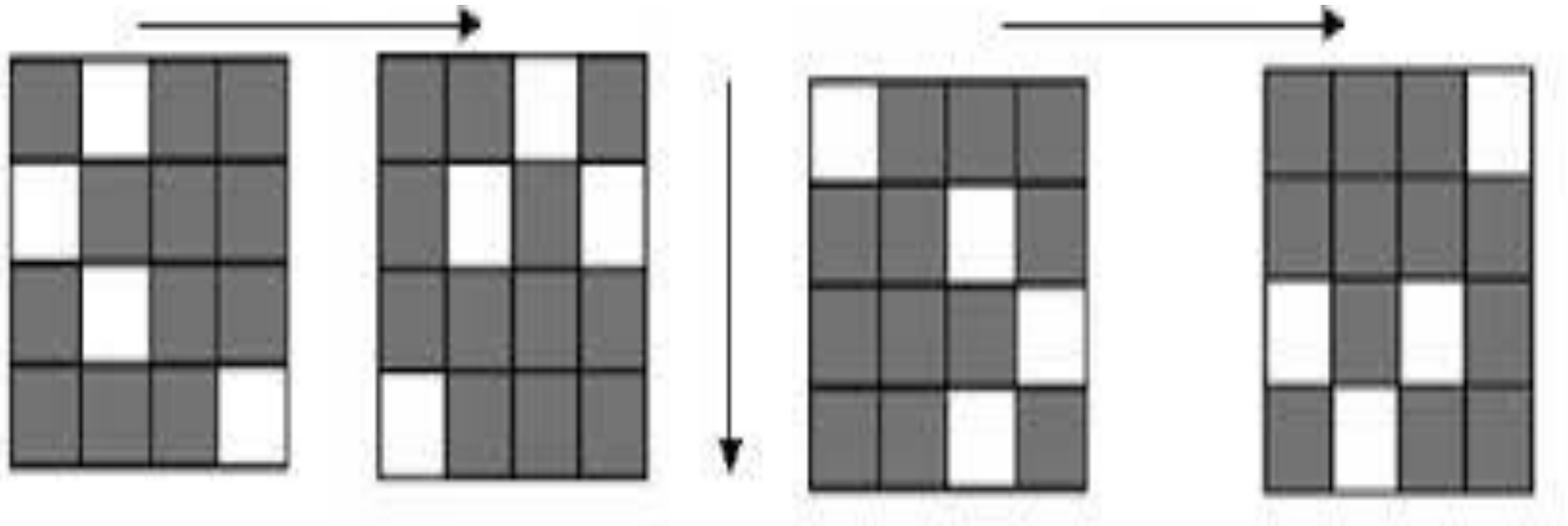




Магічні квадрати

- Квадрат картону з прорубленими всередині віконцями, який у вигляді маски накладався на таблицю такого ж розміру як і він сам, а у віконця записували текст повідомлення.
- Після одного заповнення квадрат обертався на 90 градусів три рази і ця процедура повторювалася.
- Магічні квадрати вирізняються тим, що після кожного оберту прорублені віконця опинялися над незаповненими чарунками.

Принцип дії решітки



Застосування магічних квадратів- “ПРИЛІТАЮ ВОСЬМОГО”

ВИГЛЯД ТРАФАРЕТУ			
Х	**Х**		**Х**
Х	Х	Х	
Х		Х	Х
	Х	Х	Х

0 градусів			
		П	
			Р
	И		
Л			

Застосування магічних квадратів-2

Оберт на 90 градусів

І			
	Т		
			А
		Ю	

Оберт на 180 градусів

			В
		О	
С			
	Ь		

Застосування магічних квадратів-3

Оберт на 270 градусів

	М		
О			
		Г	
			О

Шифр

І	**М**	**П**	**В**
О	Т	О	Р
С	И	Г	А
Л	Ь	Ю	0

Джероламо Кардано (1501-1576)

латинською мовою

Hieronymus Cardanus,

Італійською мовою

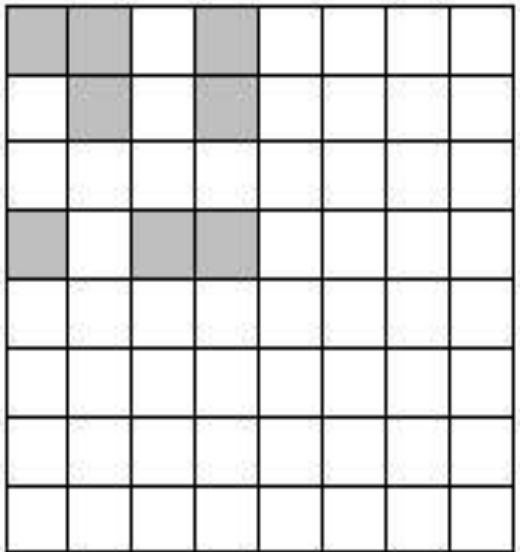
- *Girolamo Cardano*,
- *Gerolamo Cardano*

Конструктор Кардано

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

- Чарунки слід вирізати таким чином, щоб серед вирізаних чарунок не було з однаковими номерами
- Чарунки кількох номерів (бажано щоб їхня кількість була від 5 до 9) лишалися невирізаними

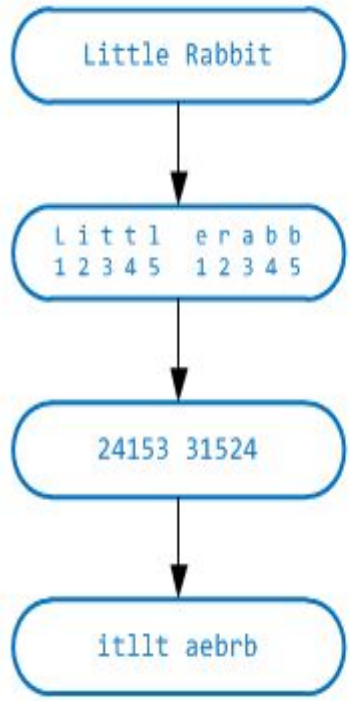
Решітка Кардано 8 x 8



Псевдомагичні квадрати

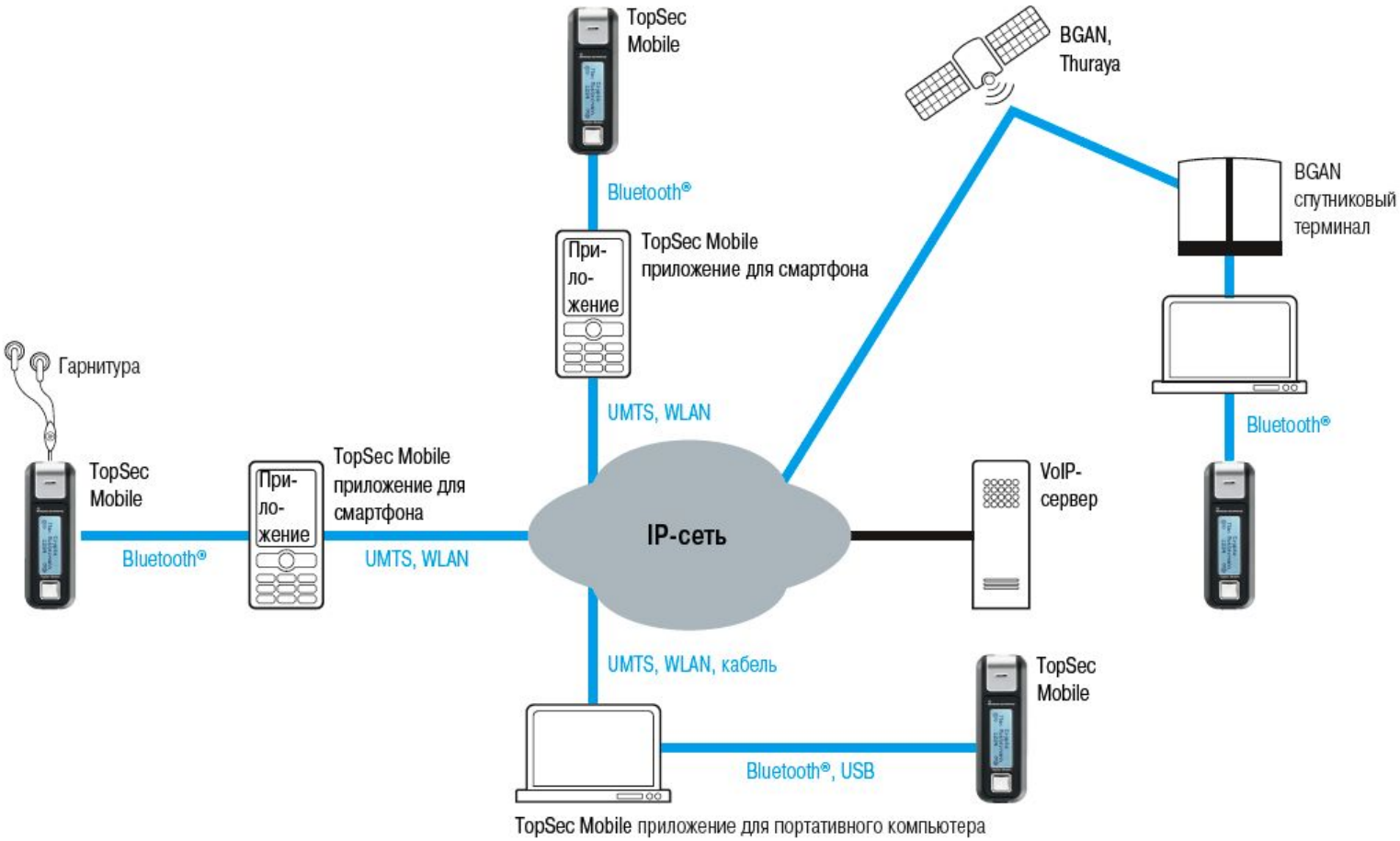
- Вирізняються від магічних тим, що після трьох обертів у кінцевій таблиці лишаються вільні чарунки, які для більшої омани супротивника заповнюються випадковими літерами

Шифр перестановки



Повідомлення
Повідомлення розбивається на групи
Ключ
Шифротекст

Скремблер для захисту телефонних розмов



Смуговий частотно-інверсний скремблер з ключем 3с1і4і2с

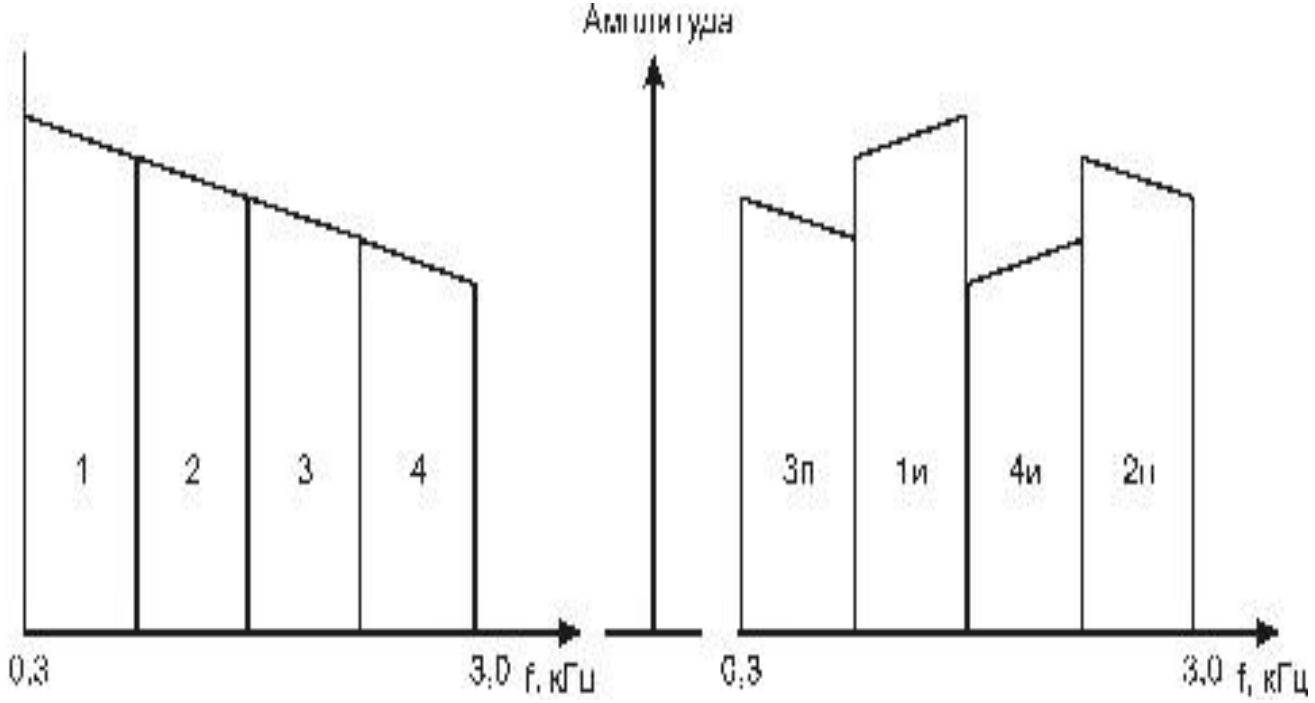
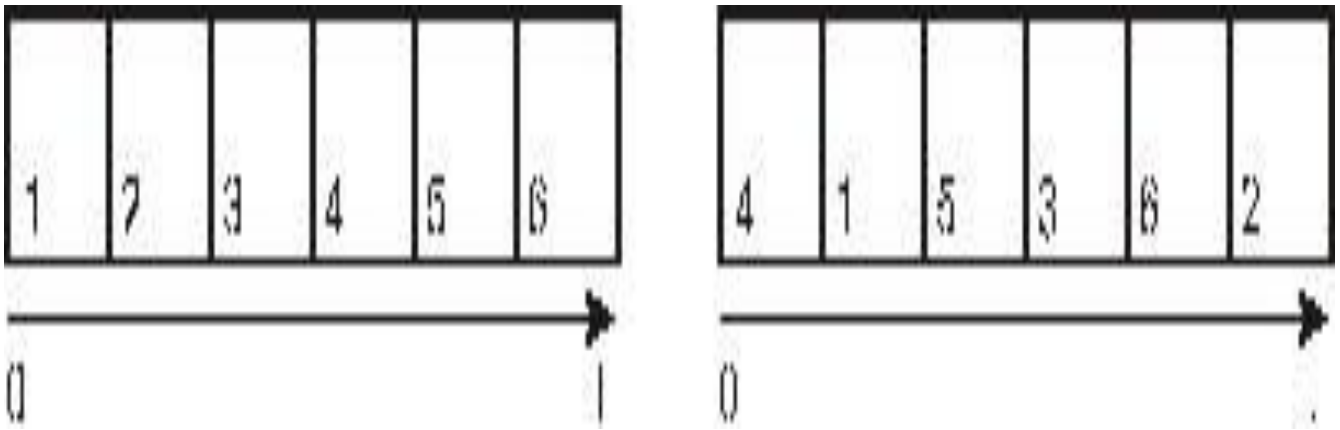


Схема роботи часового скремблера з перестановкою у фіксованому кадрі з ключем 415362



Частоти появи англійських літер

Літера	Частота	Літера	Частота	Літера	Частота
a	0.0804	b	0.0154	c	0.0306
d	0.0399	e	0.1251	f	0.0230
g	0.0196	h	0.0549	i	0.0726
j	0.0016	k	0.0067	l	0.0414
m	0.0253	n	0.0709	o	0.0760
p	0.0200	q	0.0011	r	0.0612
s	0.0654	t	0.0925	u	0.0271
v	0.0099	w	0.0192	x	0.0019
y	0.0173	z	0.0009		

Частоти появи українських літер

Літера	Частота	Літера	Частота	Літера	Частота
а	0.062	л	0.035	ц	0.004
б	0.014	м	0.026	ч	0.012
в	0.038	н	0.053	ш	0.006
г	0.013	о	0.090	щ	0.003
д	0.025	п	0.023	и	0.016
е	0.072	р	0.040	ь	0.014
ж	0.007	с	0.045	є	0.003
з	0.016	т	0.053	ю	0.006
і	0.062	у	0.021	я	0.018
й	0.010	ф	0.002	пробіл	0.174
к	0.028	х	0.009		

Частота появи літер в російській мові

Буква	Относительная частота	Буква	Относительная частота
а	0,062	р	0,040
б	0,014	с	0,045
в	0,038	т	0,053
г	0,013	у	0,021
д	0.025	ф	0,002
е, ё	0,072	х	0,009
ж	0,007	ц	0,004
з	0,016	ч	0,012
и	0,062	ш	0,006
й	0,010	щ	0,003
к	0,028	ы	0,016
л	0,035	ь, ъ	0,014
м	0,026	э	0,003
н	0,053	ю	0,006
о	0,090	я	0,018
п	0,023		

Дешифрування шифрів перестановки

- Базується на аналізі частот появлення пар літер.
- Наприклад, нехай маємо криптограму

  іркуьтіпизопзіїцулит

Припустимо, що квадрат має розмір 4 на 4

Розділемо криптосистему на блоки довжини 4 та запишемо у вигляді

1	2	3	4
І	Р	К	У
Ь	Т	І	П
И	З	О	П
З	І	ї	Ц
У	Л	И	Т

- Криптоаналіз полягає в перестановці стовпців і грунтується на тому факті, що деякі пари літер практично не трапляються в українській мові.
- Бачимо, що не можуть бути поряд:

Продовження розшифровки

1	2	3	4
І	Р	К	У
Ь	Т	І	П
И	З	О	П
З	І	ї	Ц
У	Л	И	Т

- Стовпці 1 і 4 (бо опиняться поряд літери і та у)
- 1 і 3 (и та о)
- 2 і 4 (і та ц)

Продовження розшифровки-2

- Отримуємо два можливі варіанти розташування стовпців
- 1,2,3,4, що відповідає зашифрованому тексту,
- 4, 3, 2, 1

4	3	2	1
У	К	Р	І
П	І	Т	Ь
П	О	З	И
Ц	І	Ї	З
Т	И	Л	У