

# **Безпека програм та даних**

**Навчальна дисципліна  
для студентів 4-го курсу  
Спеціальності 121 - «Інженерія  
програмного забезпечення»**

**Частина I. Основи криптографії**

(Лектор — проф. Остапов С.Е.)

# Основи криптографії

Курс складається: 30 лекційних годин;  
30 годин лабораторного практикуму;

Дисципліна складається з 2 модулів: 7 тижнів та 8 тижнів на модуль.

Модуль 1- 30 балів=12 б.(4 роботи x 3 бали: 1,3,4,9)+8 б.

Практ.+10 б. КР

Модуль 2 – 40 балів=18 (3x4б.:5,7,8+6б.:10р.)+12 пр.+10 КР.

Іспит – 30 балів.

Якщо набрано за семестр не менше 20 балів – допуск до іспиту.

Більше 65 балів – іспит автоматом.

Модульні контрольні – дистанційно.

# Основи криптографії

## Теми лекцій:

1. Вступ. Нарис історії криптографії.
2. Класичні техніки шифрування;
3. Теорія секретних систем Клода Шеннона. Поняття ідеального шифру.
4. Вимоги до сучасних криптосистем.
5. Симетричні криптосистеми. Data Encryption Standart.
6. Сучасний стандарт AES.
7. Український стандарт шифрування. Шифр «Калина».
8. Асиметричні криптосистеми. Криптосистема RSA.
9. Криптосистема Ель Гамаля.
10. Поняття про електронний цифровий підпис.
11. Криптографічні функції хешування.
12. Елементи криптоаналізу.
13. Генератори випадкових та псевдовипадкових чисел.

# Основи криптографії

## Лабораторний практикум:

1. Шифр Цезаря.
2. Шифр простої заміни.
3. Афінна система Цезаря.
4. Шифр гаммування.
- 5,6. Система блокового шифрування S-DES.
7. Цифровий підпис на основі RSA.
8. Відкритий розподіл криптографічних ключів Діффі-Хеллмана.
9. Поточковий шифр на основі генератора BBS.
10. Використання CryptoAPI для розробки ПЗ.

# Основи криптографії

## Лабораторний практикум: роботи підсиленого рівня

11. Вивчення розповсюдження помилки в різних режимах роботи симетричних шифрів.
12. Вивчення можливостей статистичного пакету NIST STS.
13. Порівняльні дослідження властивостей потокового шифру власної розробки.
14. Розробка та дослідження генератора випадкових чисел за допомогою пристроїв персонального комп'ютера.
15. Коди аутентифікації повідомлень на основі хеш-функцій.
16. Електронний цифровий підпис на основі симетричного шифру

# Основи криптографії

## Додаткові активності:

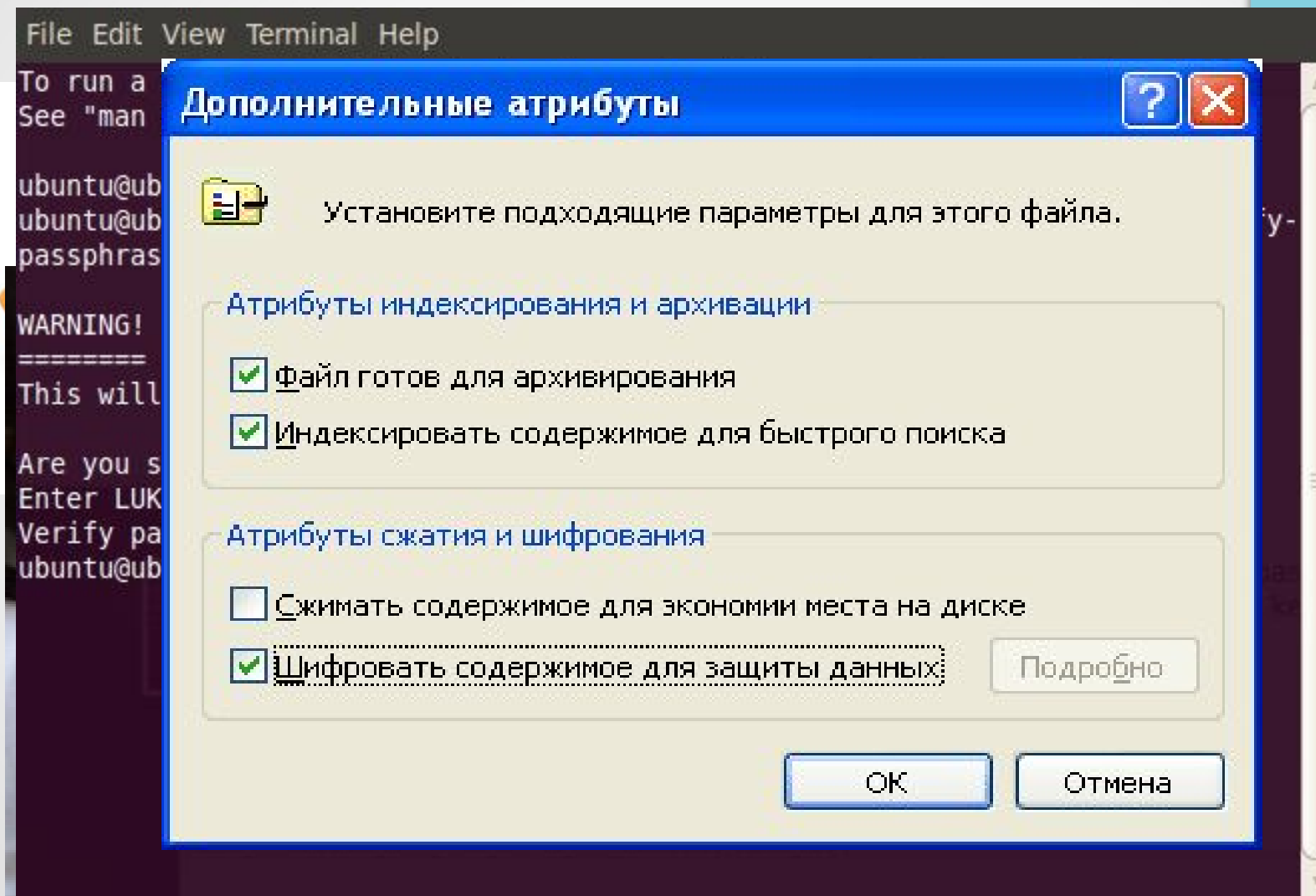
1. Реалізація складних алгоритмів шифрування (IDEA, AES; DES; Калина; Сварог ...)
2. Додаткові розробки програмних засобів.
3. Реферати, аналітичні огляди.

# Основи криптографії

## Література:

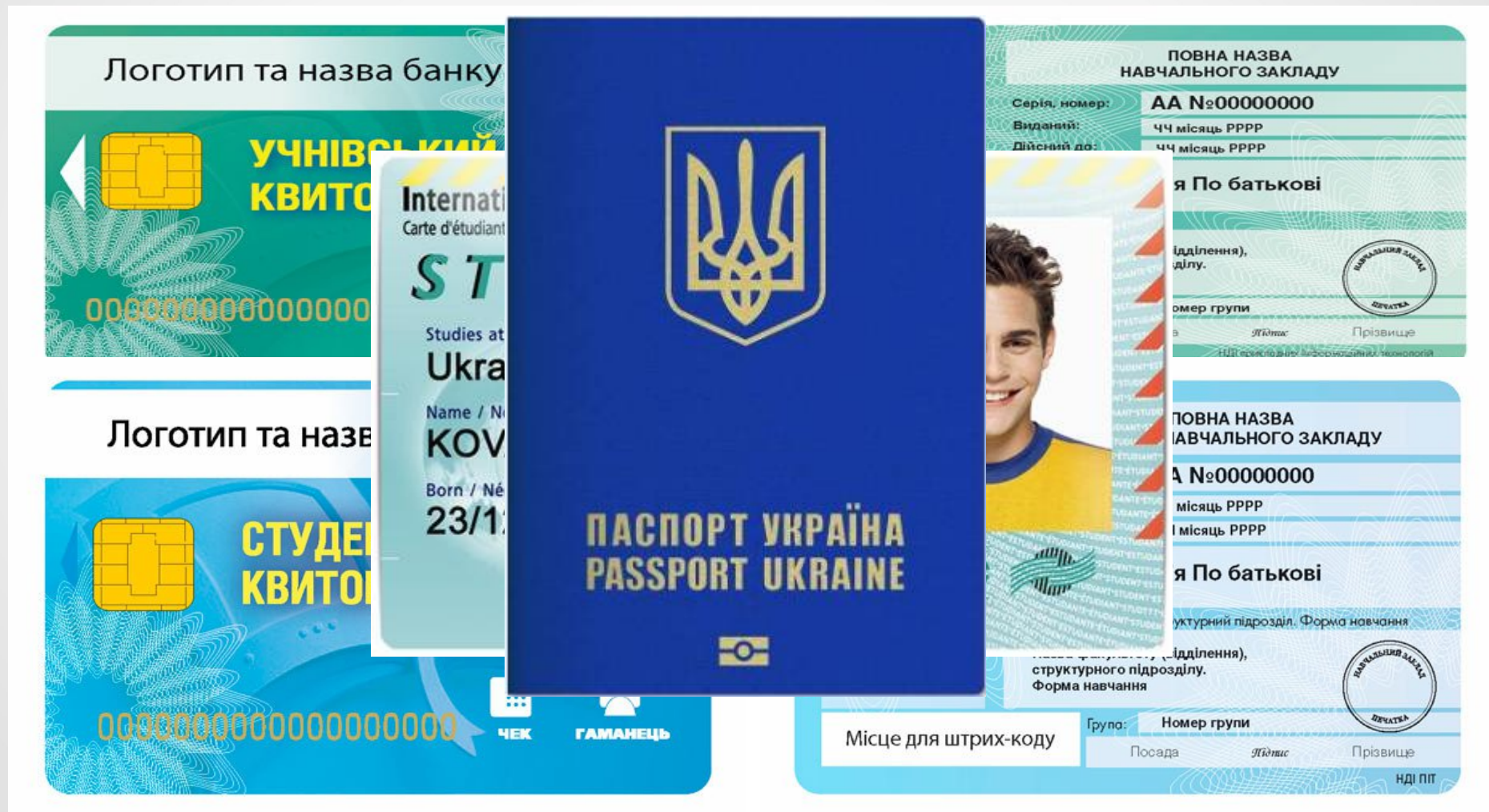
- Остапов С.Е., Валь Л.О. Основи криптографії.
- Остапов С.Е., Євсєєв С.П., Король О.Г. Технології захисту інформації.
- Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття.
- Столингс В. Криптография и защита сетей.
- Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С.
- Горбенко І.Д. Прикладна криптологія:теорія, практика, застосування.
- =====
- Сингх С. Книга шифров.
- Кан Д. Взломщики кодов.

# Де використовують шифрування?





# Електронні документи



# Що значить “шифрується”?

Відкритий текст: “Програмне забезпечення”

Зашифровані тексти:

“яннечепзебаз енмаргорп»

“рганаепчня пормезбзеен”

“оаебпея ррназчн пгмзеен”

24 17 21 09 16 20 29 13 00 03 10 15 16 00 08 10 31

(@\*^&)”!?”~’&?[~>

# Шифри в літературі

Артур Конан Дойль, “Танцюючі чоловічки”:



# Шифри в літературі

Едгар По, “Золотий жук”: криптограма Кідда

53##+305))6\*;4826)4#)4#);806\*;48

+8 ||60))85;;]8\*::#\*8+83(88)5\*+46

(;88\*96\*?;8)\*#(;485);5\*+2:\*#(;4956

\*2(5\*-4)8

||8\*;4069285);)6+8)4###;1(#9;48081;8:8#1;48+8

5;4)485+528806\*81(#9;48;(88;4(#?34;48)4#;16

1;:188;#?;

# Шифри в літературі

Жюль Верн, “Мандрівка до центру Землі”:

Ж. А. К. М. Н.	Х. Ч. А. Т. П. Т. Р.	У. Т. Т. К. І. В. Р.
Н. У. Т. Ч. Ч. У. Ф.	П. К. Т. Т. І. Т. Ф.	К. І. Т. В. А. Г. Т.
Г. Т. Ч. Т. У. К.	Т. Т. А. Т. Т. Т. Ч.	Ч. П. Р. В. А. А. К.
Т. У. Т. К. Т. Т. І.	К. П. Т. Т. К. Т.	А. А. І. Р. Ч. Т.
Т. Т. П. Т. Т. А.	. К. Ч. К. А. К.	І. Т. Т. Т. В. Ч.
К. К. В. А. У. І.	Т. Т. П. Т. П. Р.	Ф. А. Т. К. Т. П.
В. Т. , І. Т. К.	В. Ч. Т. І. В. К.	К. Т. В. І. І. І.

# Криптографія

Cryptos – таємниця;

Graphos – пишу.

Криптографія - «тайнопис».



# Криптографія

**Криптографія** – наука, яка вивчає методи перетворення інформації у незрозумілу для сторонніх осіб форму.

**Криптоаналіз** – це наука про методи подолання криптографічного захисту.

**Криптологія** – наука про шифри.  
Складається з криптографії та криптоаналізу.

# Історія криптографії

Історія криптографії складається з 4 етапів:

- I — Наївна криптографія (до початку XIV ст.);
- II — Формальна криптографія (XIV — поч. XX ст.);
- III — Наукова криптографія (30-60 рр. XX ст.);
- IV — Комп'ютерна криптографія (70-рр. - сьогодні).



# Принцип Керкхофса

Стійкість криптосистеми повинна забезпечуватися не секретністю алгоритму, а секретністю ключа.

Історія криптографії містить багато цікавих загадок, частина з яких не розв'язана й по сьогоднішній день.

# Таємниці криптографії

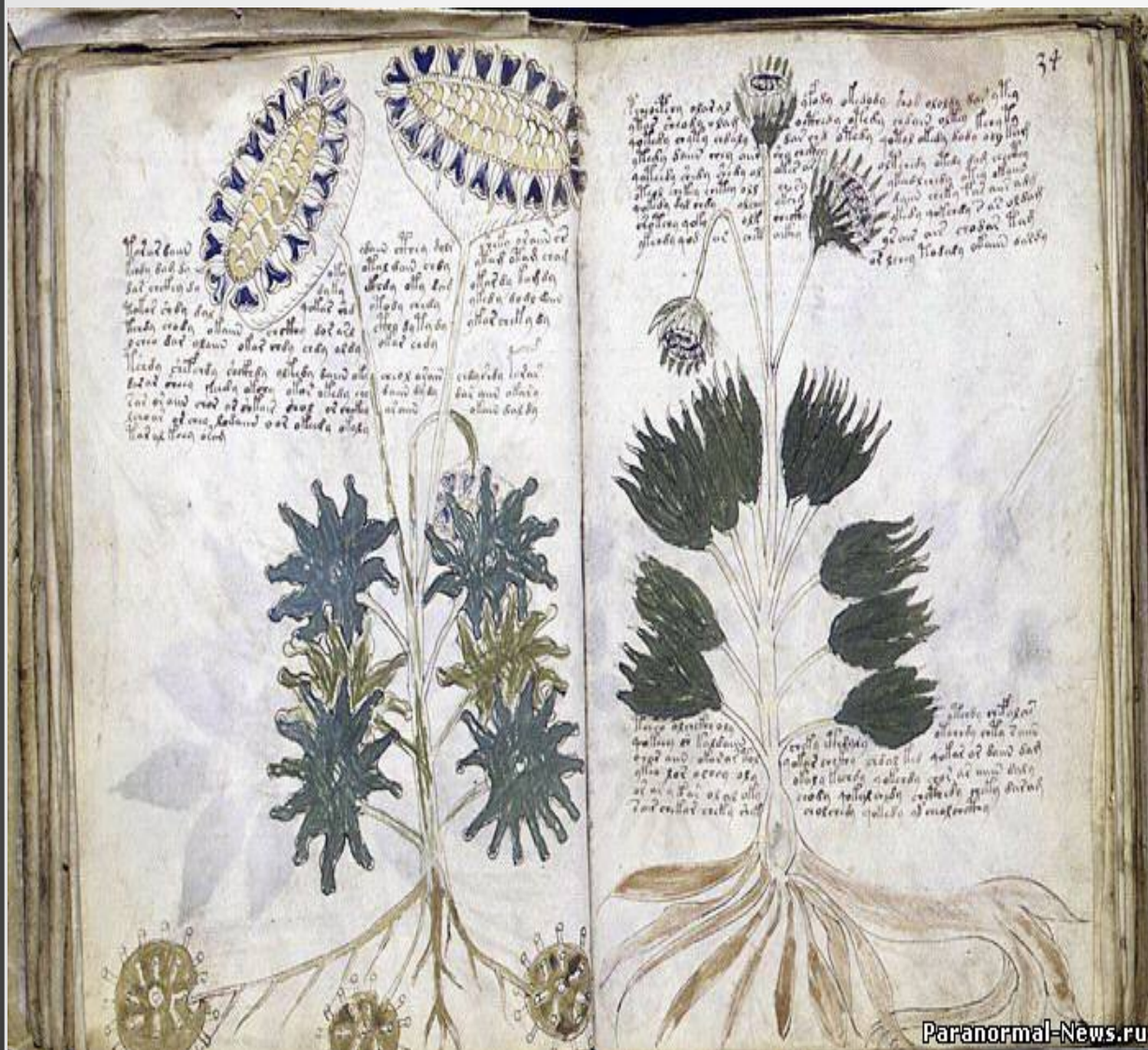


## Фестський диск

Однією з найважливіших загадок криптографії став Фестський диск, знайдений на острові Крит 1903 року. Спеціалісти змогли розрізнити на ньому 45 різних знаків, але що вони значать – досі загадка. Найкращі криптологи світу ламають голову над цією загадкою....



# Таємниці криптографії



## Манускрипт Войнича

Загадкова книга, яка зберігається у бібліотеці Єльського університету. Рукопис було куплено 1912 року в одному з італійських монастирів. Походження рукопису невідоме. Книга містить зашифрований текст, мова якого досі не ідентифікована.

Зустрічаються символи, схожі на латинські та грецькі літери, але більшість – ієрогліфи, які досі не зустрічалися в жодному іншому рукописі.



# Таємниці криптографії

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56, 239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122, 106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140, 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41, 78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196, 81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 191, 122, 43, 234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46, 10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113, 140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107, 603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8, 14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53, 79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515, 125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115, 48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121, 12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41, 85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49, 47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2, 270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31, 10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250, 557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106, 160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27, 8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51, 50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140, 112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150, 112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811, 30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205, 185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50, 154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205, 38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37, 38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84, 125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30, 150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140, 485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811, 125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302, 246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51, 63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

## Криптограми Бейла

Три криптограми, які було опубліковано невідомим автором у 1865 році. Розказують, що в криптограмах описано як знайти захований скарб золота, срібла, коштовних каменів, вартість якого на сьогодні оцінюють під 30 млн. доларів. Скарб заховано десь у штаті Вірджинія поблизу Баффордса.

Другу записку розшифрували, а першу й третю й до сьогодні не можуть.

Вважають, що можливим автором може бути Едгар Алан По.



# Таємниці криптографії

## THE CODE

## THE KEY

K1 EMUFPHZLRFAXYUSDJKZLDKRNSHG NFIVJ  
YQTQUXQBQVYU VLLTREVJYQTMKYRDMFD  
VFPJUDEEHZWETZYV GWHK KQETGFQJNCE  
GGWHKK?DQMC PFQZDQMMIAGPFXHQRLG  
TIMVMZJANQLVKQEDAGDVFRPJUNGEUNA  
QZGZLECGYUXUEENJTB JLBQCRTBJDFHRR  
YIZETKZEMVDUFKSJ HKFWHKUWQLSZFTI  
K2 HHDDDUVH?DWKBFUFPWNTDFIYCUQZERE  
EVLDKFEZMOQQJLTTUGSYQPFEUNLAVIDX  
FLGGTEZ?FKZBSFDQVGOGIPUFXHHDRKF  
FHQNTGPUAECNUVPDJMQCLQUMUNEDFQ  
ELZZVRRGKFFVOEEXBDMVPNFQXEZLGRE  
DNQFMPNZGLFLPMRJQYALMGNUVPDXVKP  
DQUMEBEDMHDAFMJGZNUPLGEWJLLAETG

ABCDEFGHIJKLMNOPQRSTUVWXYZABCD  
AKRYPTOSABCDEFGHIJLMNQUVWXZKRYPT  
BRYPTOSABCDEFGHIJLMNQUVWXZKRYPT  
CYPTOSABCDFFGHIJLMNQUVWXZKRYPTO  
DPTOSABCDEFGHIJLMNQUVWXZKRYPTOS  
ETOSABCDEFGHIJLMNQUVWXZKRYPTOSA  
FOSABCDEFGHIJLMNQUVWXZKRYPTOSAB  
GSABCDEFGHIJLMNQUVWXZKRYPTOSABC  
HABCDEFGHIJLMNQUVWXZKRYPTOSABCD  
IABCDEFGHIJLMNQUVWXZKRYPTOSABCDE  
JABCDEFGHIJLMNQUVWXZKRYPTOSABCDEF  
KABCDEFGHIJLMNQUVWXZKRYPTOSABCDEFG  
LEFGHIJLMNQUVWXZKRYPTOSABCDEFGHI  
MFGHIJLMNQUVWXZKRYPTOSABCDEFGHI

K3 ENDYAHR OHNLSRHEOCPT EOIBIDYSHNAIA  
CHTNREYULDSL LSLN OHSNOSMRWXMNE  
TPRNGATIHN RARPES LNNELEBLPIIACAE  
WMTWNDITEENRAHCTENEUDRETNHAE OE  
TFOLSEDTIWENHAEIOYTEYQHEENCTAYCR  
EIFTBRSPAMHHEWENATAMATEGYEERLB  
TEEFOASFIOTUETUAEO TOARMAEERTNRTI  
BSEDDNIAAHTTMSTE WPIEROAGRIEWFEB  
AECTDDHILCEIHSITEGOEAOSDDRYDLORIT  
RKLML EHA GTD HARD PNEOHMGFMFEUHE  
K4 ECDMRIPFEIMEHNLS STTRTVDOHW?OBKR  
UOXOGHULBSOLIFBB WFLRVQQPRNGKSSO  
TWTQSJSSEKZZWATJKLUDIAWINFBNYP  
VTTMZFPKWGD KZXTJCDIGKUHUAUEKCAR

NGHIJLMNQUVWXZKRYPTOSABCDEFGHIJL  
OHIJLMNQUVWXZKRYPTOSABCDEFGHIJL  
PIJLMNQUVWXZKRYPTOSABCDEFGHIJLM  
QJLMNQUVWXZKRYPTOSABCDEFGHIJLMN  
RLMNQUVWXZKRYPTOSABCDEFGHIJLMNQ  
SMNQUVWXZKRYPTOSABCDEFGHIJLMNQ  
TNQUVWXZKRYPTOSABCDEFGHIJLMNQ  
UQUVWXZKRYPTOSABCDEFGHIJLMNQ  
VUVWXZKRYPTOSABCDEFGHIJLMNQ  
WVWXZKRYPTOSABCDEFGHIJLMNQ  
XWXZKRYPTOSABCDEFGHIJLMNQ  
YXZKRYPTOSABCDEFGHIJLMNQ  
ZZKRYPTOSABCDEFGHIJLMNQ  
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD

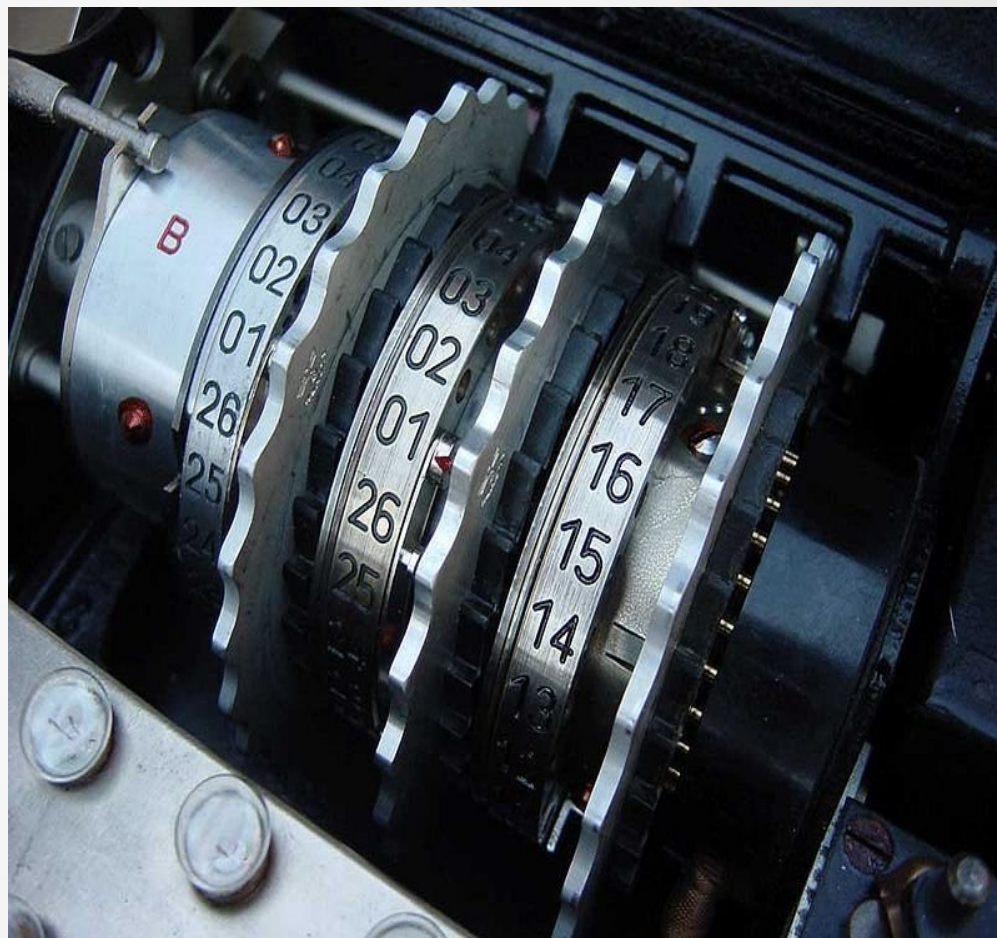


# Артур Шербіус



Артур Шербиус — винахідник  
роторної шифрувальної  
машини

# Шифрувальні машини



Шифрувальна машина «Енігма» та її ротори



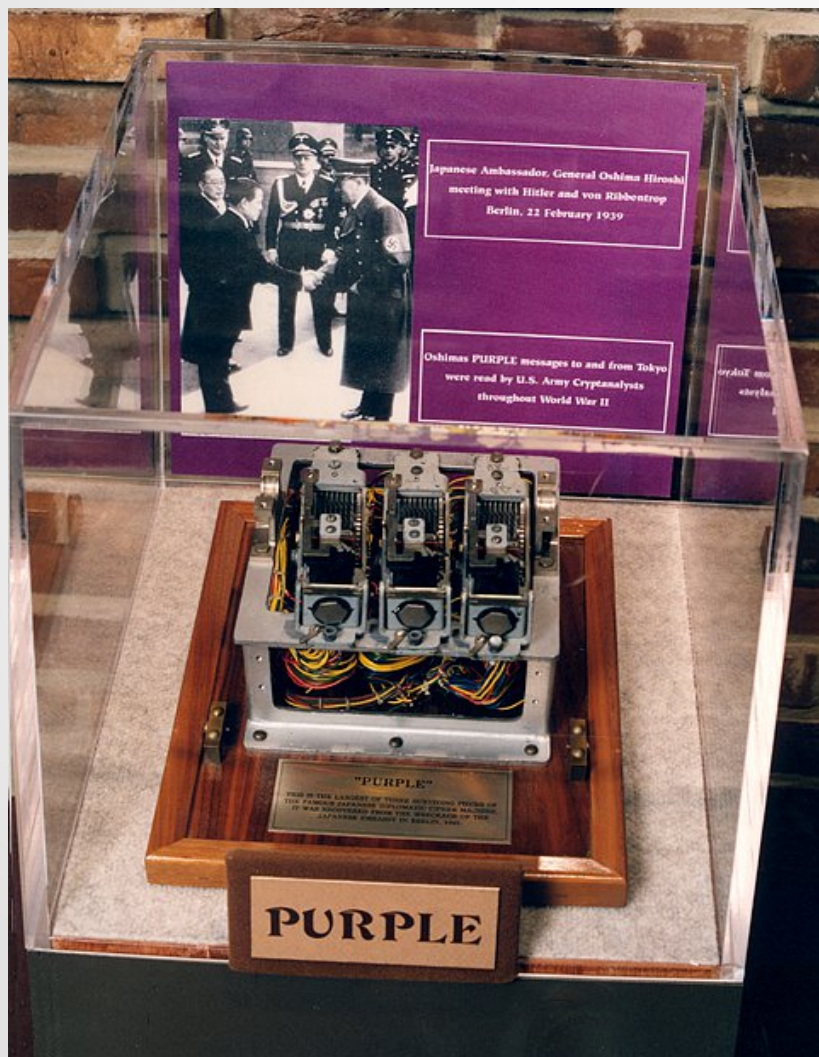
# Шифрувальні машини



Російська  
шифрувальна  
машина М-125,  
«Фиалка»



# Шифрувальні машини



Японська шифрувальна  
машина Purple

# Шифрувальні машини



Американська шифрувальна  
машина М-209

# Симулятор машины “Еніґма”

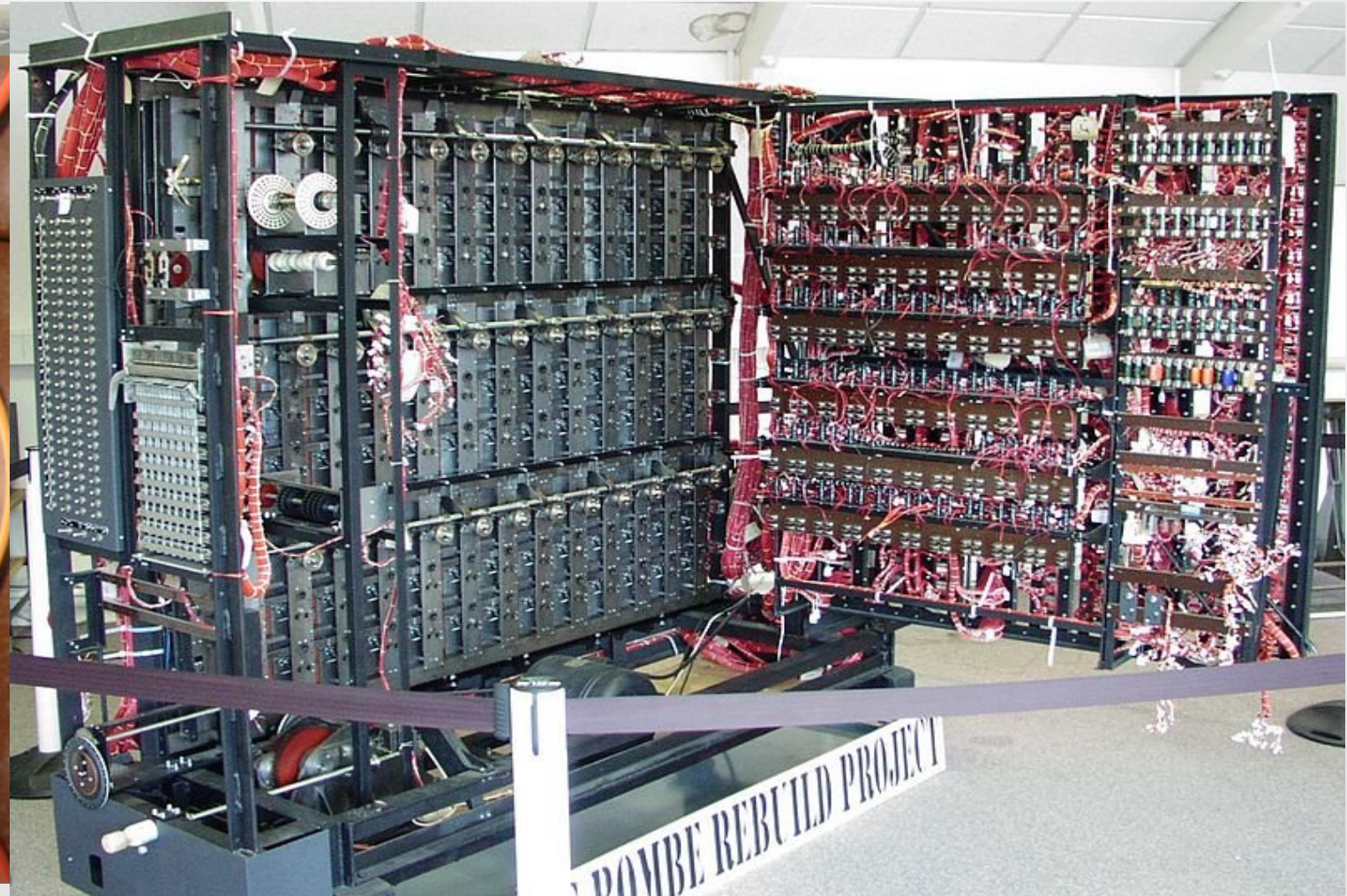


Програмний симулятор шифромашини “Еніґма” для усіх операційних систем  
Можна скачати за адресою:

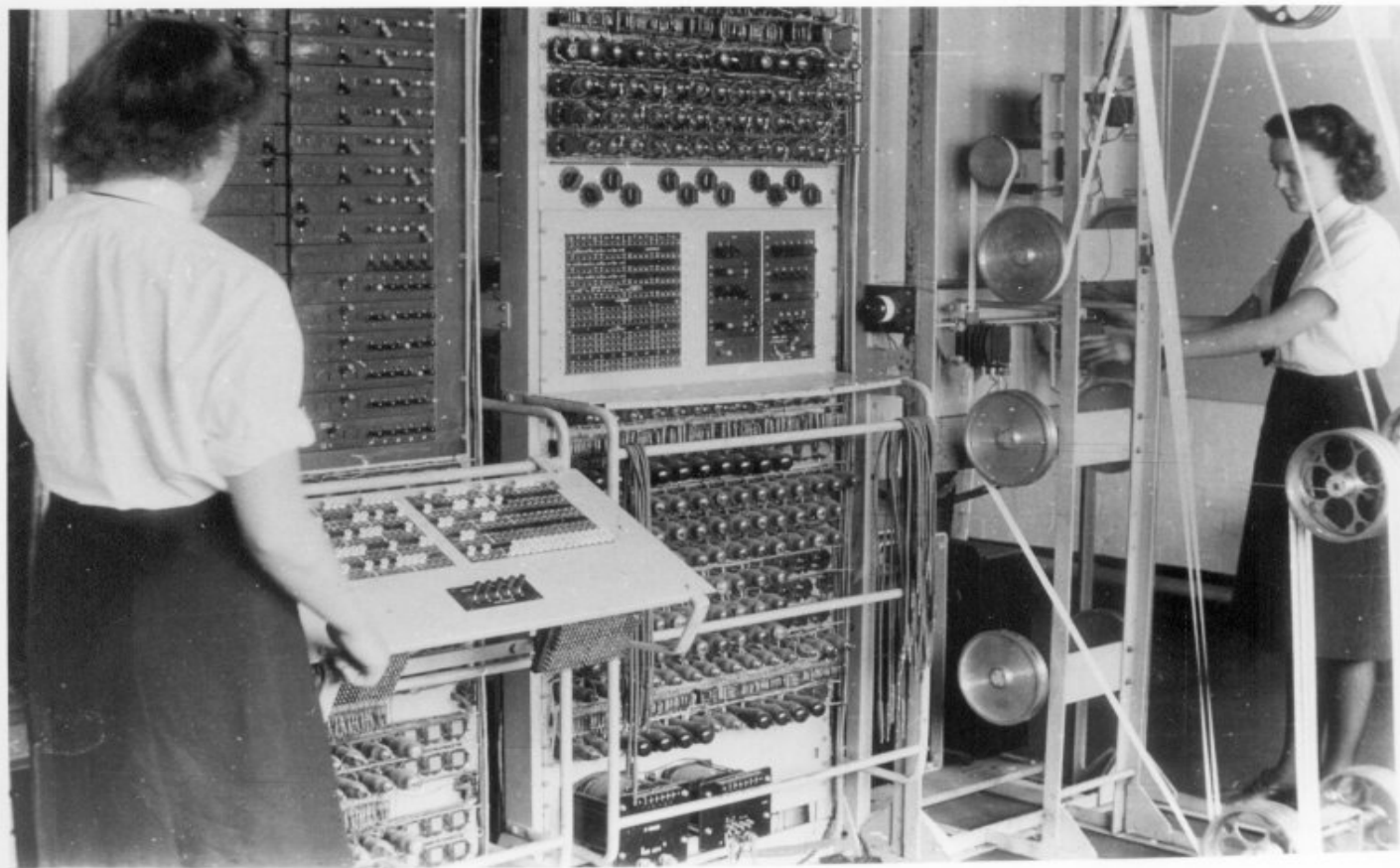
**<http://www.radioscanner.ru/files/miscsoftware/file15849/>**



# Криптоаналіз “Енігми”



# Криптоаналіз машини “Лоренц”



Дешифрувальна машина “Колосс”



# Класичні техніки шифрування

Усі прості класичні шифри поділяються на:

- **шифри перестановки**, коли змінюється порядок літер в повідомленні;
- **шифри заміни (підстановки)**, коли літери повідомлення замінюються іншими символами. Підстановки бувають одноалфавітними та багатоалфавітними, коли використовуються літери з кількох різних алфавітів.

Усі сучасні шифри – комбінації з перестановок та замін.

# Шифри перестановок

Нагадаємо, що шифри перестановок лише змінюють порядок слідування літер у повідомленні, не змінюючи власне літер.

Найпростіші з шифрів перестановок:

- Шифр сцитала;
- Шифр частоголу;
- Матричний шифр.

# Шифри перестановки

## Шифр сцитала (сцитали, скітали):





# Шифри перестановки

## До шифрів перестановок можна віднести:

# Шифр частотолу

Відкритий текст записується по «стовпчиках», кількість яких визначається «висотою частотолу». Якщо «висота частотолу» = 2, маємо 2 стовпчики, якщо 3 — 3 стовпчики і т. д. Шифротекст читається по рядках.

Наприклад, зашифруємо слово «**криптографія**»:

криптографія → р п о р ф я → рпорфя китгаї  
к и т г а і

криптографія → и о а я → иоая ртрі кпгф  
р т р і  
к п г ф

Розшифровують навпаки, записуючи шифротекст по рядках, відкритий текст зчитують по стовпчиках.

# Шифри перестановки

## Матричний шифр

Вибирається розмір матриці для заповнення. Відкритий текст записується по рядках матриці, зашифрований читається по стовпчиках. Наприклад, зашифруємо текст: «**програмне забезпечення**» в матриці з 6 стовпчиків:

п	р	о	г	р	а
м	н	е	з	а	б
е	з	п	е	ч	е
н	н	я			

Зашифрований текст: «**пмен рнзн оепя гзе рач абе**»

Для розшифрування все роблять навпаки: шифротекст записують в матрицю по стовпчиках, а зчитують відкритий — по рядках матриці.

# Шифри перестановки

## Матричний шифр

Можна ускладнити шифр, увівши ключове слово. Нехай, наприклад, ключове слово «**крипто**». Запишемо його у заголовку стовпчиків, а потім переставимо їх в алфавітному порядку літер ключового слова.

<b>к</b>	<b>р</b>	<b>и</b>	<b>п</b>	<b>т</b>	<b>о</b>
п	р	о	г	р	а
м	н	е	з	а	б
е	з	п	е	ч	е
н	н	я			



<b>и</b>	<b>к</b>	<b>о</b>	<b>п</b>	<b>р</b>	<b>т</b>
о	п	а	г	р	р
е	м	б	з	н	а
п	е	е	е	з	ч
я	н			н	

Тепер зашифрований текст буде мати вигляд: «**оеля пмен абе гзе рнзн рач**»

# Шифри перестановки

## Матричний шифр

Можна ще покращити стійкість цього шифру, увівши ще одне ключове слово, розташоване по рядках. Нехай таке слово «**шифр**». Додамо його зліва від матриці:

	<i>и</i>	<i>к</i>	<i>о</i>	<i>п</i>	<i>р</i>	<i>т</i>
<i>ш</i>	о	п	а	г	р	р
<i>и</i>	е	м	б	з	н	а
<i>ф</i>	п	е	е	е	з	ч
<i>р</i>	я	н			н	



	<i>и</i>	<i>к</i>	<i>о</i>	<i>п</i>	<i>р</i>	<i>т</i>
<i>и</i>	е	м	б	з	н	а
<i>р</i>	я	н			н	
<i>ф</i>	п	е	е	е	з	ч
<i>ш</i>	о	п	а	г	р	р

Отримаємо такий шифротекст: «**еяпо мнєп б еа з ег ннзр а чр**»

Сьогодні шифри перестановок занадто прості, щоби застосовувати їх безпосередньо для шифрування. Самостійного значення вони не мають, лише історичне. Ідеї, закладені в них, використовуються як елементарна складова сучасних шифрів.

# Шифри заміни (підстановки)

Тепер розглянемо шифри заміни.

Нагадаємо, що в цих шифрах літери одного алфавіту замінюються на літери іншого або інших. В першому випадку шифр називається одноалфавітною заміною, в другому — багатоалфавітною.

# Шифри заміни

## Шифр «атбаш»

Таблиця заміни будується так, як показано нижче. Шифрування відбувається заміною літери верхнього рядка літерою нижнього («**а**» - «**я**», «**к**» - «**п**», «**ш**» - «**д**» тощо).

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
я	ю	ь	щ	ш	ч	ц	х	ф	у	т	с	р	п	о	н	м	л	к	й	ї	і	и	з	ж	є	е	д	г	в	б	а

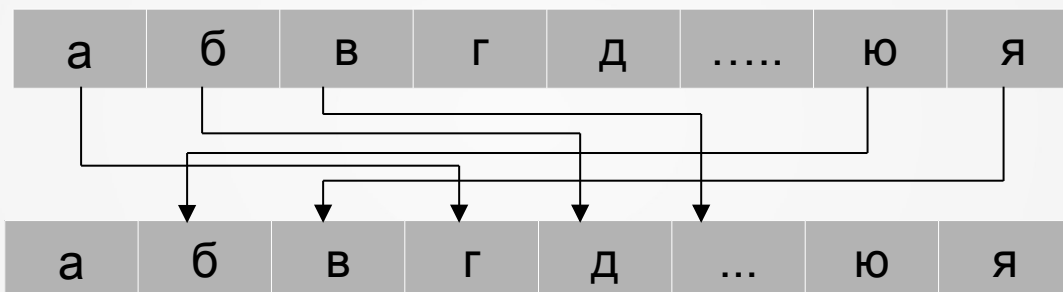
Зашифруємо повідомлення: «**Місце зустрічі змінити не можна**»

Зашифроване повідомлення: «**Нтієч фіїїйте фнтмуіу мч  
НЛХМЯ**»

# Шифри заміни

## Шифр Цезаря

Одним з найвідоміших класичних шифрів заміни вважається шифр Цезаря. Процес шифрування зводиться до заміни літери відкритого тексту такою, що знаходиться від неї на три позиції праворуч. Розшифрування виконується заміною літери шифротексту такою, що знаходиться від неї на три позиції ліворуч.



Ми бачимо, що алфавіт замкнений в «кільце», після літери «**я**» знову використовуються літери з самого початку: «**а**», «**б**» і т.д.

Математично такий спосіб шифрування можна записати наступним чином:  $c_i = (m_i + 3) \bmod 32$ , оскільки потужність алфавіту в нашому випадку становить 32 символи. Розшифрувати можна так:  $m_i = (c_i - 3) \bmod 32$ . Тут  $m_i$  та  $c_i$  — порядкові номери літер відкритого тексту та шифротексту в алфавіті. Нумерація починається з нуля.

# Шифри заміни

Спробуємо зашифрувати шифром Цезаря повідомлення: «**Зустрічайте літак завтра опівночі**». Ключ (тобто зсув) візьмемо +3.

Зашифрований текст буде мати вигляд: «**Їцфчукьгмхз окхгн їгехуг сткерськ**».

Існують численні вдосконалення шифру Цезаря. Найпопулярнішим є афінна система Цезаря. Тут таблиця заміни будується з використанням ключа, що складається з двох чисел **a**, **b**.

Ключ підставляється у формулу:  $c_i = (am_i + b) \bmod 32$ , за якою обчислюється заміна поточної літери (тут  $m_i$  — порядковий номер в алфавіті літери відкритого тексту,  $c_i$  — зашифрованого тексту).

Вимоги до ключа: для того, щоби таблиця заміни була взаємно однозначною, необхідно, щоби  $\text{НСД}(a, n) = 1$ , тобто щоби **a** та потужність алфавіту **n** були взаємно простими числами.

Оскільки у нас потужність алфавіту = 32, то, наприклад, число 3 буде з ним взаємно простим. Отже, ми можемо вибрати ключ  $a=3$ ;  $b=5$ .



# Шифри заміни

Таблиця заміни для такого ключа буде мати вигляд ( $c_i = (3m_i + 5) \bmod 32$ ):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
Е	З	Ї	Л	О	С	Ф	Ч	Ь	А	Г	Є	И	Й	М	П	Т	Х	Ш	Ю	Б	Д	Ж	І	К	Н	Р	У	Ц	Щ	Я	В

Тепер можна шифрувати повідомлення. Зашифруємо повідомлення: «**Афінний шифр Цезаря**». Для цього шукаємо літери повідомлення у верхньому рядочку та замінюємо їх на літери, які стоять у тому ж стовпчику нижнього рядочка (тобто «білу» літеру замінюємо на «чорну»).

Шифротекст буде мати вигляд: «**Еігттаи уажю Нсьеюв**».

Розшифровується шифротекст аналогічно: шукаємо літери в нижньому рядочку та замінюємо їх на відповідні, що стоять у в тому ж стовпчику верхнього рядочка (тобто «чорну» літеру міняємо на «білу»).

Наприклад, розшифруємо криптограму: «**ВКХРЖ ШВДЩЬ ІЮАШД ХЛЮЕІ ГЄ**». Шукаючи літери криптограми в нижньому рядочку і замінюючи їх на ті, що стоять у верхньому, отримаємо: «**Я хочу п'ять з криптографії**».

# Шифри заміни

## Шифр пар

Для створення таблиці заміни використовують ключову фразу, яка містить щонайменше 16 різних літер. Наприклад: «*Рече та стогне Дніпр широкий*». До таблиці заміни вписують 16 літер в тому порядку, як вони зустрічаються у фразі. Літери, що повторюються, пропускаємо. Решту літер, які не входять до фрази, записуємо в нижній рядок в алфавітному порядку. В результаті отримаємо таку таблицю заміни.

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

Зашифруємо повідомлення: «**Передайте дані каналом номер два**»

Для цього шукаємо літеру відкритого тексту в таблиці й замінюємо її тією, що стоїть в тому ж стовпчику («**П**» - «**Ч**»; «**е**» - «**є**»; «**л**» - «**с**» тощо).

Результат шифрування: «**Чєбєхїязє хїфц юїфісмо фмоєб хжї**»

# Шифри заміни

## Квадрат Полібія

Існує кілька варіантів цього старовинного шифру. Ми розглянемо два з них. Перший варіант такий. Усі літери абетки записуються у випадковому порядку в квадратну матрицю. Власне, розміщення цих літер і буде ключем до шифру. Для української мови вибирають матрицю 6х6.

<i>ж</i>	<i>л</i>	<i>т</i>	<i>і</i>	<i>о</i>	<i>б</i>
<i>р</i>	<i>д</i>	<i>я</i>	<i>к</i>	<i>.</i>	<i>с</i>
<i>ш</i>	<i>ф</i>	<i>п</i>	<i>а</i>	<i>ї</i>	<i>н</i>
<i>є</i>	<i>и</i>	<i>ь</i>	<i>ч</i>	<i>,</i>	<i>г</i>
<i>м</i>	<i>х</i>	<i>–</i>	<i>у</i>	<i>щ</i>	<i>ц</i>
<i>в</i>	<i>ю</i>	<i>е</i>	<i>;</i>	<i>з</i>	<i>й</i>

# Шифри заміни

<i>ж</i>	<i>л</i>	<i>т</i>	<i>і</i>	<i>о</i>	<i>б</i>
<i>р</i>	<i>д</i>	<i>я</i>	<i>к</i>	<i>.</i>	<i>с</i>
<i>ш</i>	<i>ф</i>	<i>п</i>	<i>а</i>	<i>ї</i>	<i>н</i>
<i>є</i>	<i>и</i>	<i>ь</i>	<i>ч</i>	<i>,</i>	<i>г</i>
<i>м</i>	<i>х</i>	<i>–</i>	<i>у</i>	<i>щ</i>	<i>ц</i>
<i>в</i>	<i>ю</i>	<i>е</i>	<i>;</i>	<i>з</i>	<i>й</i>

Шифрування відбувається у такий спосіб:

кожна літера відкритого тексту замінюється тією, що стоїть у таблиці заміни нижче на одну клітинку («*ж*» - «*р*»; «*л*» - «*д*»; «*х*» - «*ю*» тощо).

Якщо літера знаходиться у нижньому рядку, вона замінюється такою, що стоїть у верхньому рядочку цього ж стовпчика («*в*» - «*ж*»; «*ю*» - «*л*» і т.д.).

Зашифруємо повідомлення «*ми вивчаємо криптографію*».

Зашифрований текст буде таким: «*вх жхжучмв. ашхья.цшчил*»



# Шифри заміни

## Другий варіант квадрату Полібія такий.

Літери абетки розміщуються в алфавітному порядку в таблиці, наприклад 6х6 (для української мови). Кожен рядок та стовпчик нумеруються як показано нижче.

	1	2	3	4	5	6
1	а	б	в	г	д	е
2	є	ж	з	и	і	ї
3	й	к	л	м	н	о
4	п	р	с	т	у	ф
5	х	ц	ч	ш	щ	ь
6	ю	я	-	-	-	-

Можна також ототожнити літери «*і*» та «*ї*»; «*ш*» та «*щ*» та розмістити літери, повністю заповнивши прямокутник 6х5.

# Шифри заміни

	1	2	3	4	5	6
1	а	б	в	г	д	е
2	є	ж	з	и	і	й
3	к	л	м	н	о	п
4	р	с	т	у	ф	х
5	ц	ч	ш	ь	ю	я

Спробуємо зашифрувати за допомогою такої таблиці слово «**заміна**». Запишемо координати відповідних літер у таку таблицю:

Літера:	з	а	м	і	н	а
Горизонтальна координата:	2	1	3	2	3	1
Вертикальна координата:	3	1	3	5	4	1

Тепер запишемо цифри по дві, читаючи по рядках: **21 32 31 31 35 41**

Далі замість цифр записуємо відповідні літери з таблиці, наприклад, **21** - «**є**», **32** - «**л**» ... Отримаємо слово: «**єлккор**». Це й буде зашифрований текст.

*Можна також заповнювати таблицю заміни літерами у випадковому порядку, як і в першому випадку.*

# Шифри заміни

## Шифр Плейфера (магічний квадрат)

Ще одним популярним шифром був так званий «магічний квадрат» або шифр Плейфера.

Він використовувався для шифрування пар літер, так званих «біграм». Для шифрування використаємо квадрат, в який у випадковому порядку вписано усі літери алфавіту, наприклад такий, як квадрат Полібія.

<b>ж</b>	<b>л</b>	<b>т</b>	<b>і</b>	<b>о</b>	<b>б</b>
<b>р</b>	<b>д</b>	<b>я</b>	<b>к</b>	<b>.</b>	<b>с</b>
<b>ш</b>	<b>ф</b>	<b>п</b>	<b>а</b>	<b>ї</b>	<b>н</b>
<b>є</b>	<b>и</b>	<b>ь</b>	<b>ч</b>	<b>,</b>	<b>г</b>
<b>м</b>	<b>х</b>	<b>—</b>	<b>у</b>	<b>щ</b>	<b>ц</b>
<b>в</b>	<b>ю</b>	<b>е</b>	<b>;</b>	<b>з</b>	<b>й</b>

Нехай нам потрібно зашифрувати повідомлення: **«зустріч відбудеться на старому місці»**. Розіб'ємо повідомлення на пари літер: **«зу ст рі чв ід бу де ть ся на ст ар ом ум іс ці»**.

# Шифри заміни

## Шифр Плейфера

Отже, «*зу ст рі чв ід бу де ть ся на ст ар ом ум іс ці*»

ж	л	т	і	о	
р	д		к	.	с
ш	ф	п	а	ї	н
є	и	ь	ч	,	г
м	х	—	у		ц
в	ю	е		з	й

Шукаємо літери першої пари в квадраті (вони підсвічені жовтим). Вважаючи ці комірки «діагоналлю» уявного прямокутника, «переходимо» на іншу його «діагональ» (в даному випадку це символи «;» та «*ц*» - заштриховано). Це й буде зашифрований текст. Друга пара («*ст*» — підсвічено зеленим) шифрується у біграму «*яб*» (заштриховано). Третя біграма («*рі*») шифрується у «*жк*».



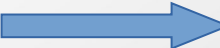
# Шифри заміни

## Шифр Плейфера

Існує кілька простих правил, яких треба дотримуватися для правильної роботи з шифром:

1. Якщо літери пари знаходяться в одному рядку, то вони замінюються на ті, що стоять праворуч у сусідніх стовпчиках.
2. Якщо літери пари знаходяться в одному стовпчику, то вони перетворюються у символи, що знаходяться безпосередньо під ними.
3. Якщо символ не має пари, тобто кількість символів у повідомленні непарна, то воно доповнюється якимось спецсимволом або літерою, що рідко зустрічається.
4. Якщо шифрується пара однакових літер, то після першої з них ставиться спецсимвол (або літера, що рідко зустрічається) і шифрується ця пара літер.

Користуючись цими правилами, отримаємо таку шифрограму:

«;щ яб жк є; лк іц тй я\_ пн чг яб шк жищ щх кб уб» 

«;щябжкє;лкїцтйя\_пнчгябшкжищщхкбуб»

# Шифри заміни

## Шифр Віженера

Шифр Віженера — мабуть, найвідоміший класичний шифр, який було названо на честь французького дипломата Блеза де Віженера. Довгий час він вважався абсолютно стійким до зламу вручну. І лише у 19 сторіччі німецький криптограф та археолог Фрідріх Касіскі повністю зламав цей шифр. Однак, за деякими повідомленнями, він був не першим: ще за кілька років до Касіскі шифр був зламаний Чарлзом Беббіджем.

Архітектурно шифр Віженера є багатоалфавітною заміною. Він використовує стільки «алфавітів», скільки літер у реальній мові, якою написано повідомлення. Якщо це англійська — 26 типів заміни, якщо українська — 32 або 33.

Математично процес зашифрування можна описати формулою:

$$C_i = (M_i + K_i) \bmod 32,$$

де  $C_i$  — номер літери шифротексту в алфавіті;  $M_i$  — номер в алфавіті літери відкритого тексту;  $K_i$  — номер літери ключа.

Розшифровка виконується за такою формулою:

$$M_i = (C_i - K_i + 32) \bmod 32.$$

Для полегшення роботи можна використати спеціальну таблицю.

## Таблиця Віженера

	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
а	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
б	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а
в	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б
г	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в
ѓ	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г
д	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ
е	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д
є	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е
ж	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є
з	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж
и	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з
і	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и
ї	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і
й	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї
к	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й
л	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к
м	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л
н	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м
о	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н
п	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о
р	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п
с	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р
т	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с
у	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т
ф	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у
х	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ч	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	ш	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	щ	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ь	ь	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ю	ю	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
я	я	а	б	в	г	ѓ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю

# Шифри заміни

## Шифр Віженера

Припустимо, нам треба зашифрувати повідомлення «**Наступаємо на світанку**» на ключі «**Віженер**».

Шифрування за допомогою таблиці відбувається у такий спосіб.

1. Записуємо відкритий текст без пробілів.
2. Підписуємо під ним ключ стільки разів, скільки треба, щоби заповнити усю довжину відкритого тексту.
3. В таблиці в першому рядку шукаємо літери відкритого тексту, а в першому стовпчику — літери ключа.
4. На перетині отриманих стовпчика і рядка отримуємо відповідну літеру зашифрованого тексту.

Наприклад: шукаємо в першому рядочку «**н**» (першу літеру повідомлення); шукаємо в першому стовпчику «**в**» - першу літеру ключа. На перетині отриманих стовпчика та рядка отримуємо літеру «**п**» - першу літеру шифротексту. Продовжуємо до кінця тексту.

Відкритий текст:	наступаємонасвітанку
Ключ:	віженервіженервіжене
Зашифрований текст:	піщшєхрзчцунчтїажующ



# Шифри заміни

## Шифр Віженера

Розшифровується криптограма так.

1. Записуємо шифротекст.
  2. Над ним записуємо ключ так, щоби заповнити усю довжину повідомлення.
  3. У першому стовпчику таблиці знаходимо літеру ключа, наприклад, «**в**».
  4. Просуваємось вправо по рядочку, поки не зустрінемо відповідну літеру шифротексту, наприклад, «**п**».
  5. Літера, що стоїть в заголовку цього стовпчика, і буде відповідною літерою відкритого тексту, наприклад, «**н**».
  6. Повторюємо до закінчення шифротексту.
- Таким чином отримуємо все повідомлення.

Ключ:

віженервіженервіжене

Зашифрований текст:

піщшєхрзчцунчтїажующ

Відкритий текст:

наступаємонасвітанку

# Класичні техніки шифрування

На цьому ми закінчимо огляд класичних технік шифрування, хоча існує ще багато шифрів, які варті згадування. Це:

- диск Енея або лінійка Енея;
- різного роду книжкові шифри;
- омофонічні шифри;
- решітка Кардано;
- шифр Першої світової війни,

і багато інших способів перетворення інформації у незрозумілу для сторонніх осіб форму.