МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ

КЛАСИЧНІ МЕТОДИ КРИПТОЛОГІЇ

методичні рекомендації для здобувачів спеціальностей
«Прикладна математика» та «Системний аналіз»

Ужгород 2020

Класичні методи криптології: методичні рекомендації для здобувачів спеціальностей «Прикладна математика» та «Системний аналіз» / М.М. Повідайчик, І.Я. Шпонтак. Ужгород: Видавництво УжНУ «Говерла», 2020. 28 с.

Упорядники:

- Повідайчик М.М., к.е.н., доцент кафедри кібернетики і прикладної математики факультету математики та цифрових технологій УжНУ;
- Шпонтак І.Я., викладач кафедри кібернетики і прикладної математики факультету математики та цифрових технологій УжНУ

Рецензенти:

- Глебена М.І., к.ф.-м.н., доцент кафедри системного аналізу і теорії оптимізації факультету математики та цифрових технологій УжНУ;
- Бортош М.Ю., к.ф.-м.н., доцент кафедри алгебри факультету математики та цифрових технологій УжНУ

Розглянуто і схвалено науково-методичною комісією
факультету математики та цифрових технологій УжНУ.
Протокол №1 від 01.09.2020 року.

Рекомендовано до друку Вченою радою
факультету математики та цифрових технологій УжНУ.
Протокол №4 від 18.12.2020 року.

ЗМІСТ

Частина І.

Силабус курсу «Основи криптографії. Технологія Blockchain»

Курс «Основи криптографії. Технологія Blockchain» – це нормативний курс освітньої програми «Системний аналіз» для першого (бакалаврського) рівня вищої освіти спеціальності 124 «Системний аналіз» факультету математики та цифрових технологій.

Мета та цілі курсу: ознайомити студентів як з класичними методами криптографії, так із методами асиметричної криптології, а також із застосуванням вказаних методів, зокрема у технології блокчейн.

Структура курсу: в рамках курсу студенти будуть вивчати теоретичні питання та виконувати лабораторні роботи.

Теоретична частина курсу

Тема 1. Докомп'ютерний захист інформації.

Основні поняття криптографії. Шифри підстановки. Шифр Цезаря. Модулярний шифр. Гомофонічне шифрування. Поліграмне шифрування. Шифр Плейфера. Багатоалфавітне підстановочне шифрування. Шифр Віженера. Шифр Вернама.

Тема 2. Арифметичні основи криптографії.

Алгоритм ділення з остачею. Найбільший спільний дільник. Взаємно прості числа. Найменше спільне кратне. Прості числа. Порівняння. Класи лишків. Функція Ейлера. Порівняння першого степеня. Первісні корені. Існування первісних коренів. Індекси за модулем pk і 2pk. Символ Лежандра. Квадратичний закон взаємності. Символ Якобі.

Тема 3. Алгебраїчні основи криптографії.

Поняття групи. Підгрупи груп. Циклічні групи. Гомоморфізм груп. Групи підстановок. Дії групи на множині. Кільця і поля. Підкільця. Гомоморфізм кілець. Евклідові кільця. Прості і максимальні ідеали. Скінченні розширення

полів. Поле розкладу. Скінченні поля. Порядки незвідних многочленів. Лінійні рекурентні послідовності. Послідовності максимального періоду.

Тема 4. Поняття про еліптичні криві.

Рівняння Вейєрштрасса, дискримінант і j-інваріант. Додавання точок еліптичної кривої. Еліптичні криві над скінченними полями.

Тема 5. Ймовірнісно-статистичні моделі повідомлень та їхні ентропійні властивості.

Джерела дискретних повідомлень та їхні ймовірнісні моделі. Функціонал ентропії та його властивості. Умовна ентропія та її властивості. Питома ентропія стаціонарної символьної послідовності. Ентропійні характеристики марківських символьних послідовностей. Джерела неперервних повідомлень і їхні ентропійні властивості. Оптимізація функціонала ентропії на класі ймовірнісних розподілів.

Тема 6. Методи теорії інформації у криптографії.

Асимптотичні властивості стаціонарного джерела дискретних повідомлень. Ентропійна стійкість випадкових символьних послідовностей. Кількість інформації за Шенноном і її властивості. Шенноновські моделі криптосистем. Теоретико-інформаційні оцінки стійкості симетричних криптосистем.

Тема 7. Статистичне тестування випадкових і псевдовипадкових послідовностей.

Рівномірно розподілена випадкова послідовність і її властивості. Універсальний алгоритм статистичного тестування випадкових і псевдовипадкових послідовностей. Тест n-серій. Тест інтервалів. Узагальнений покер-тетст. Тест «збирача купонів». Тест перестановок. Тест перетинаючихся n-грам. Тест, заснований на рангах двійкових матриць. Спектральні тести. Тест випадкового блуждання. Універсальний статистичний тест Мауера. Тест на основі прирощеної ентропії. Тест, заснований на алгоритмі стиснення Лемпеля-Зіва. Тест, заснований на лінійній складності. Тест на основі екстремальної

статистики скалярного добутку. Тест на основі екстремальної статистики дельта-добутку. Алгоритмічне визначення випадковості.

Тема 8. Алгоритми генерування випадкових і псевдовипадкових послідовностей.

Класифікація алгоритмів генерування. Лінійні і мультиплікативні конгруентні генератори. Нелінійні конгруентні генератори. Рекуренти у скінченному полі. Послідовності, породжені лінійними регістрами здвигу зі зворотнім зв'язком. Генератори Фібоначчі. Криптостійкі генератори на основі односторонніх функцій. Криптостійкі генератори, засновані на проблемах теорії чисел. Методи «покращення» псевдовипадкових послідовностей. Комбінування алгоритмів генерації методом Макларена-Марсальї. Комбінування LFSR-генераторів. Конгруентний генератор з випадковими параметрами.

Тема 9. Потокові криптосистеми.

Основні поняття. Рекурентні послідовності. Лінійні рекурентні послідовності. Оцінка параметрів і розпізнавання ЛРП. Лінійна складність. Визначення початкового стану ЛРП. Комбінування послідовностей. Кореляційний криптоаналіз.

Тема 10. Математичні моделі стандартних блочних криптосистем.

Криптосистема DES і її властивості. Криптосистема IDEA. Криптосистема ГОСТ 28147-89. Загальна структура алгоритму Rijndael. Використання алгебри поліномів у алгоритмі Rijndael.

Тема 11. Математичні методи криптоаналізу симетричних систем.

Завдання та принципи криптоаналізу. Метод «опробування» і його обчислювальна складність. Методи криптоаналізу на основі теорії статистичних рішень. Різницевий криптоаналіз. Лінійний криптоаналіз.

Тема 12. Криптосистеми з відкритим ключем.

Описання RSA–криптосистеми. Можливі атаки на криптосистему RSA. Стійкість RSA проти методу повторного шифрування. Пошук секретного ключа d і факторизації модуля N. Біти в RSA-криптосистемі. Система Рабина.

Ранцевий метод шифрування. Стійкість ранцевого шифру. Теорема Вінера про малий секретний ключ. Арифметика великих чисел. Модулярна арифметика. Ознака простоти. Алгоритми генерації простих чисел. Задача факторизації.

Тема 13. Функції хешування.

Визначення і властивості. Блочно-ітераційні функції хешування. Використання блочних криптосистем. Атака «днів народження». Криптосистеми аутетифікації. Функція хешування СТБ 1176.1-99.

Тема 14. Електронний цифровий підпис.

Узагальнена модель ЕЦП. Схема ЕЦП Рабина. Схема Діффі-Лампорта. Імовірнісна схема підпису Рабина. Стандарт ЕЦП DSS. Схема ЕЦП Ель Гамаля. Арифметичні властивості російського стандарту цифрового підпису. Еквівалентність задач фальсифікації підпису в DSS схемою Ель Гамаля. Електронний цифровий підпис СТБ 1176.1-99. Задача дискретного логарифмування.

Тема 15. Еліптичні криві у криптографії.

Цифровий підпис на еліптичних кривих. Особливості скалярного множення на еліптичних кривих. Обчислення порядку еліптичної кривої.

Тема 16. Протоколи управління криптографічними ключами.

Протоколи генерації ключів. Протоколи взаємної аутентифікації. Протоколи прямого обміну ключами. Протоколи розподілу сеансових ключів з використанням центру розподілу ключів.

Тема 17. Нові напрямки у криптографії.

Можливості квантової криптографії. Математичне розділення секрету. Стенографія і її застосування. Активний криптоаналіз.

Тема 18. Технологій блокчейн.

Історія блокчейну. Структура: блоки, децентралізація, відкритість, використання. Типи: публічні, приватні, гібридні блокчейни. Сумісність.

Лабораторні роботи.

Лабораторна робота №1. Докомп’ютерні методи криптографії.

Лабораторна робота №2. Потокові криптосистеми.

Лабораторна робота №3. Стандартні блочні криптосистеми.

Лабораторна робота №4. Криптосистеми з відкритим ключем.

Лабораторна робота №5. Електронний цифровий підпис.

Система оцінювання та вимоги

Оцінювання буде проводитися за 100-бальною шкалою. Бали будуть нараховуватися за таким співвідношенням:

− тести на лекціях: 10% оцінки;

− лабораторні роботи : 40% оцінки;

− домашні завдання: 30% оцінки;

− іспит: 20% оцінки.

Частина ІІ. Класичні криптосистеми

1. Шифр Цезаря.

Ця криптосистема зобов'язана своєю появою Юлію Цезарю. У ній кожна буква тексту зсувається циклічно на k позицій за алфавітом. Наприклад, при $k = 3$ виходить наступне шифрування слова "cleopatra":

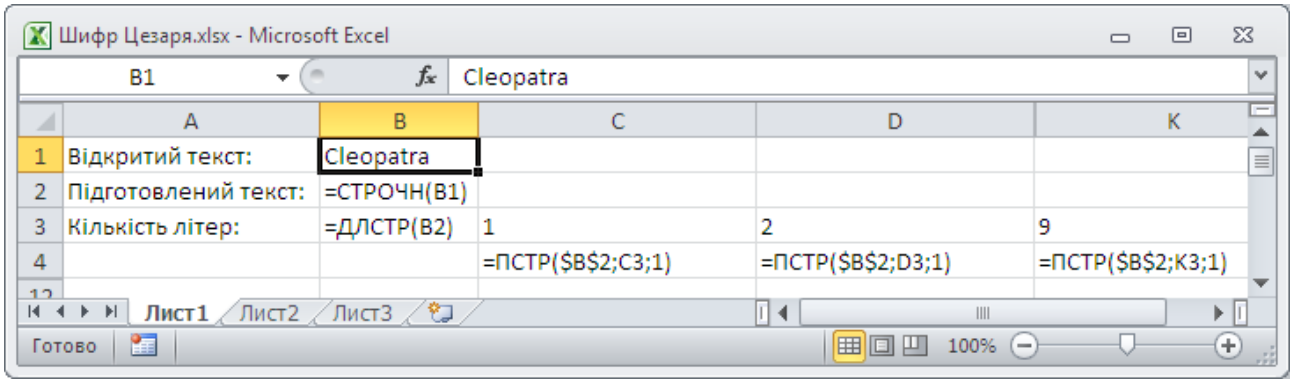
$$\text{cleopatra} \to \text{dmfpqbusb} \to \text{engqrcvtc} \to \text{fohrsdwud}$$

Більш формально *шифр Цезаря* визначається над алфавітом $\{0,1,\dots,25\}$ співвідношеннями:

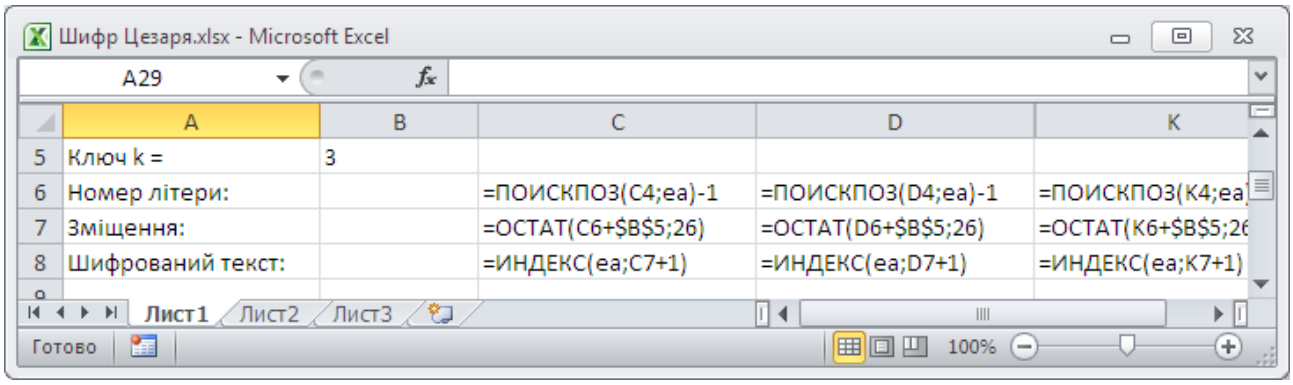
$$E_k(m) = (m + k) \bmod 26, 0 \le m < 26,$$
$$\varepsilon = \{E_k | 0 \le k < 26\}.$$

Для цієї криптосистеми простором ключів $\mathcal{K}$ є множина $\{0,1,\dots,25\}$ і $D_k = E_{26-k}$. Тому її легко зламати простим перебором всіх ключів. Такий метод називається *повним перебором ключів*.

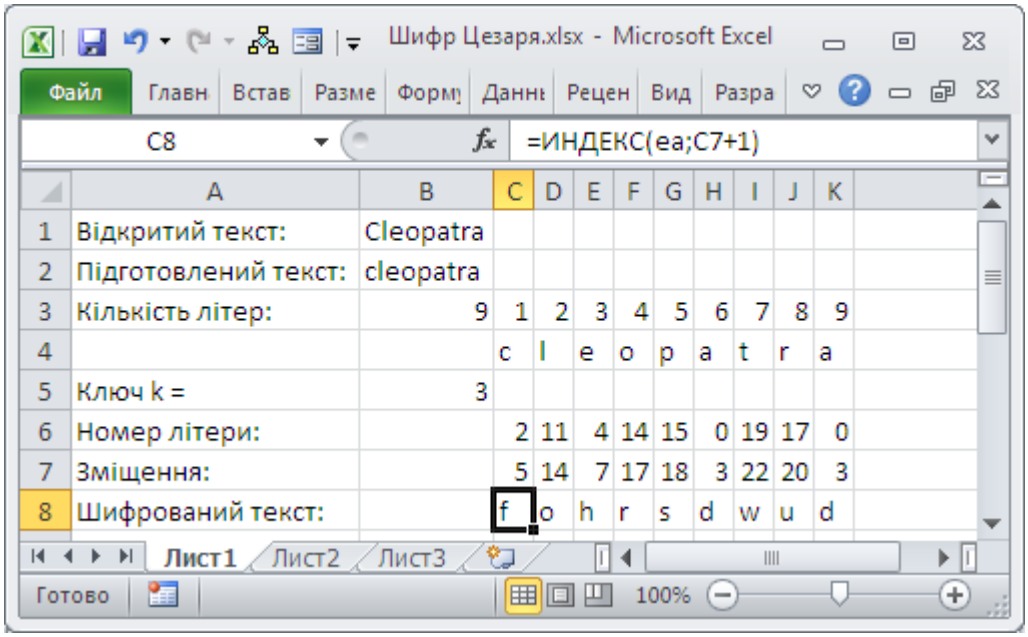
Приклад 1. У електронній таблиці MS Excel введемо початкові дані та формули:



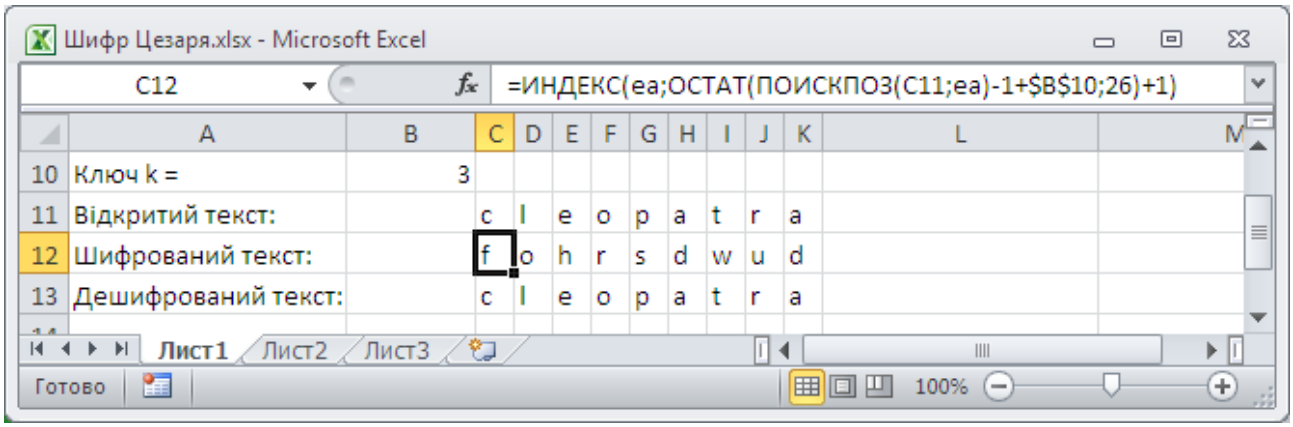
За допомогою «Диспетчера імен» задаємо константу масиву з літерами англійського алфавіту: ea={"a";"b";"c";"d";"e";"f";"g";"h";"i";"j";"k";"l";"m";"n";"o";"p";"q";"r";"s";"t";"u";"v";"w";"x";"y";"z"}. Далі задаємо ключ k та вводимо формули для шифрування:



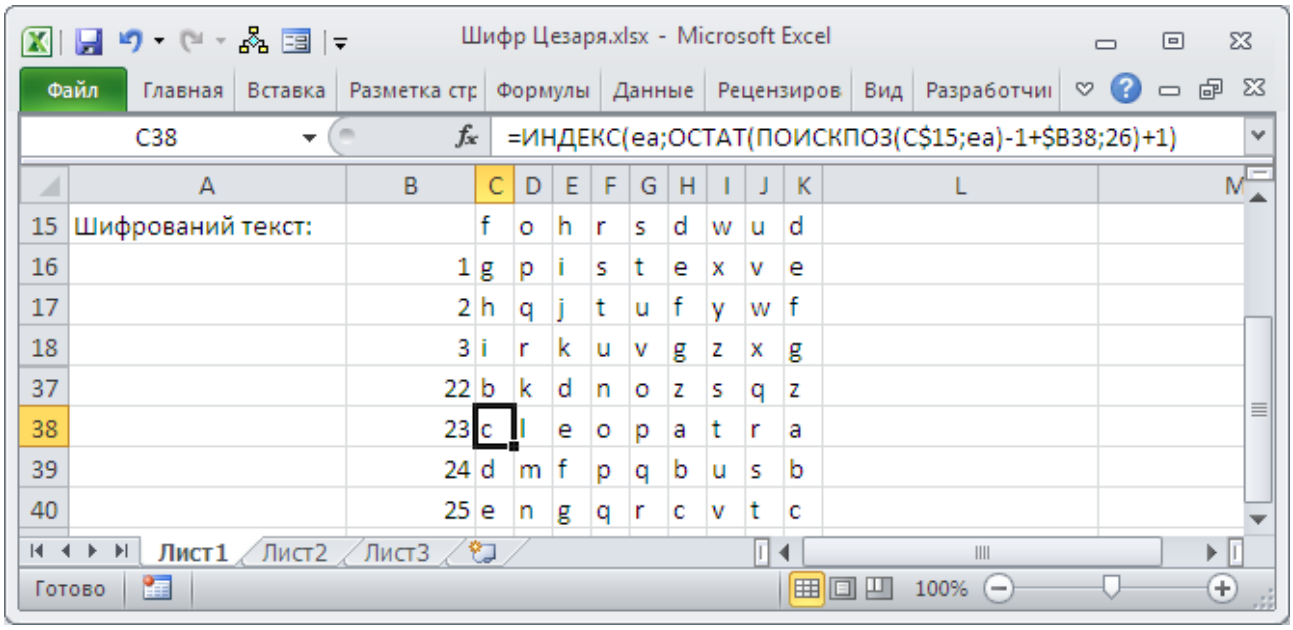
Отримуємо шифрований текст:



Використовуючи вкладені формули (мегаформули) MS Excel шифрування (і дешифрування) можна здійснити так:



Аналогічно реалізується криптоаналіз шифротексту:



2. Шифр простої заміни.

Метод простої заміни полягає у фіксації деякої перестановки π алфавіту $\{a, b, \dots, z\}$, після чого вона застосовується до кожної букви відкритого тексту. Опишемо більш формально систему простої заміни. Простором ключів $\mathcal{K}$ є множина S_q всіх перестановок на множині $\{0,1, \dots, q-1\}$, а криптосистема ε визначається так:

$$\varepsilon = \{E_\pi | \pi \in S_q\},$$

де

$$E_\pi(m) = \pi(m), 0 \le m < q.$$

Функція дешифрування D_π задається рівністю $D_\pi = E_{\pi^{-1}}$, оскільки

$$D_\pi\big(E_\pi(m)\big) = D_\pi\big(\pi(m)\big) = E_{\pi^{-1}}\big(\pi(m)\big) = \pi^{-1}\big(\pi(m)\big) = m, 0 \le m < q.$$

На відміну від шифру Цезаря, ця система не має такого недоліку, як занадто малий простір ключів. Дійсно, $|\mathcal{K}| = S_{26} = 26! \approx 4 \cdot 10^{26}$. Ця система є прикладом того, як нерозумно вірити в надійність криптосистеми, сподіваючись на її великий простір ключів. Простий підрахунок частот появи

літер в шифротексті і їхнє порівняння з частотами літер (які відомі для кожної мови, зокрема для української – див табл. 1) дозволяє швидко знайти образи перестановки π для більшості найбільш уживаних літер відкритого тексту. Справді, найбільш часто вживана літера в криптограмі англійського тексту швидше за все виявиться образом літери *e*. Наступна за частотою буде образом літери *n* і т.д. Очевидно, чим довша криптограма, тим легше її розшифрувати.

о	0,100	р	0,050	д	0,031	ч	0,012	ш	0,006
н	0,079	е	0,048	п	0,029	х	0,013	є	0,005
а	0,075	с	0,043	з	0,023	ц	0,012	ф	0,004
и	0,064	к	0,039	я	0,021	ї	0,011	щ	0,004
в	0,053	м	0,034	ь	0,018	й	0,010	ґ	0,000
і	0,052	л	0,032	б	0,015	ю	0,009		
т	0,052	у	0,032	г	0,015	ж	0,008		

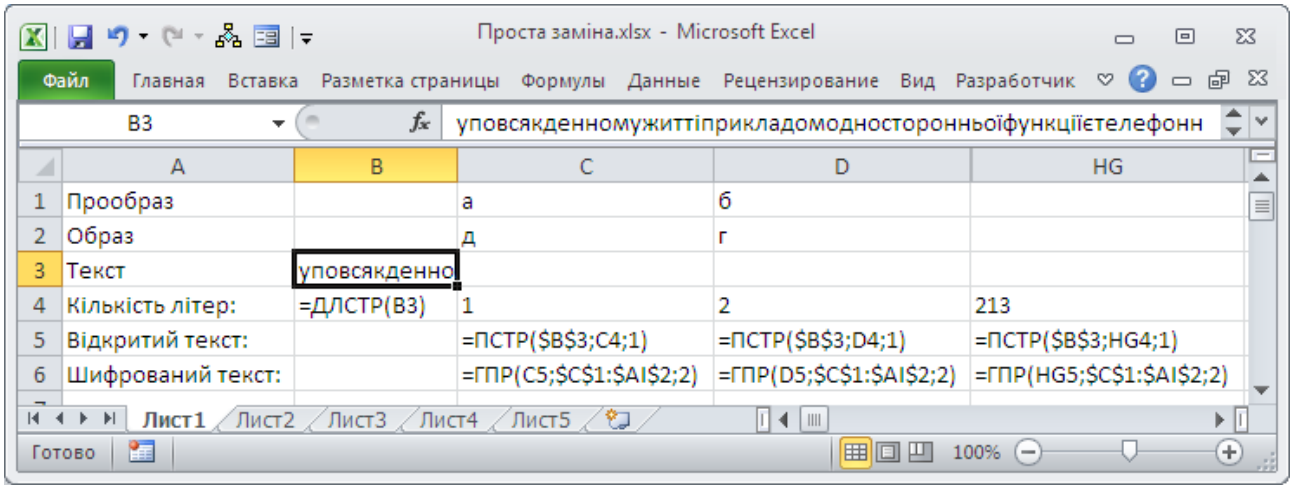
Табл. 1. Середньостатистичні частоти букв без врахування пропуску між словами в українській мові (Сушко С.О., Фомичова Л.Я., Барсуков Є.С. Частоти повторюваності букв і біграм у відкритих текстах українською мовою)

Приклад 2. Розглянемо деякий відкритий текст: «уповсякденномужиттіприкладомодносторонньоїфункціїєтелефоннакнигазазад аниміменемлюдинилегкознайтивідповіднийїйтелефоннийномераленена впакиві дшуканнятелефонногономерапевноїлюдинирівносильнезнаходженнюіменіціїп ерсони» та деяку перестановку літер українського алфавіту:

а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м
д	г	а	е	є	й	и	і	ж	б	в	к	м	з	о	ї

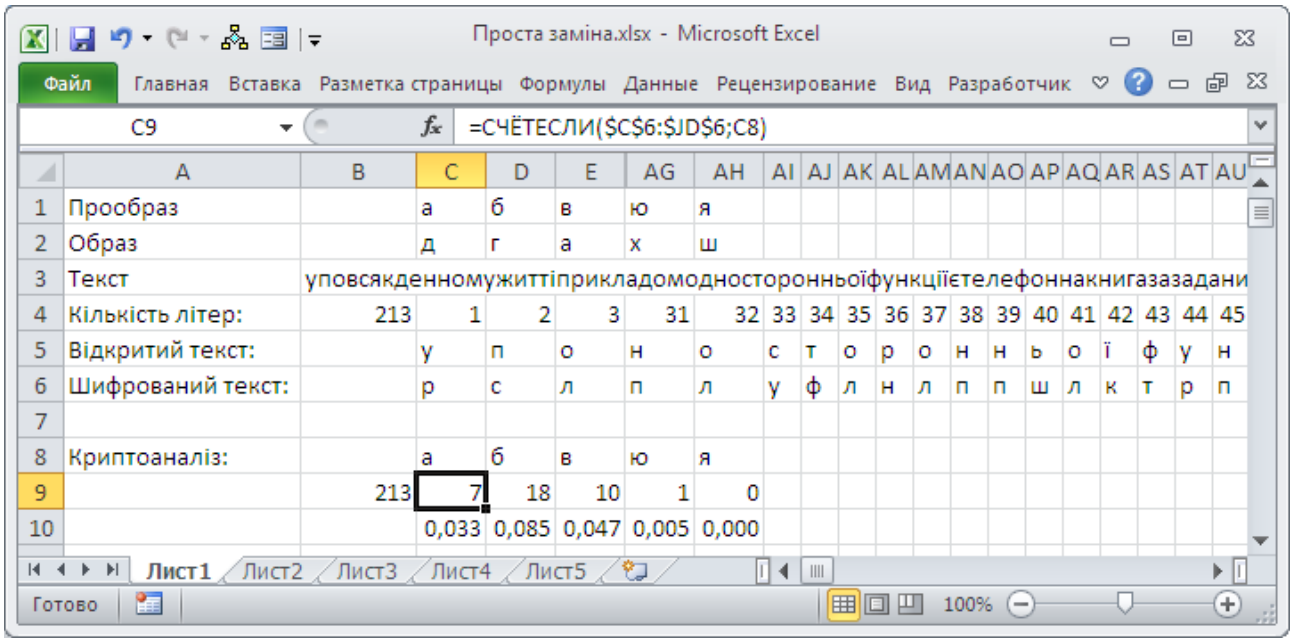
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
п	л	с	н	у	ф	р	т	ц	щ	ь	ю	ч	я	х	ш

У електронній таблиці MS Excel введемо початкові дані та формули:



Використовуючи функцію «ГПР», отримуємо шифротекст: «рслаушзєйпплїріббффвснбзодєлїлєплуфлнлппшлктрпзщвкифйойтлппдзпбеджд ждєдпбївїйпйїохєбпбойезлжпдбфбавєславєпббкббфйойтлпппббплїйндойпйпдасдз бавєюрздппшфйойтлпплелплїйндсйаплкохєбпбнваплубошпйжпдцлєійппхвїйпв щвиксйнулпб».

Підрахунок частот літер шифротексту реалізуємо за допомогою функції «СЧЁТЕСЛИ»:



Отримуємо емпіричну таблицю частот, яку можна використати для установлення відповідності літер шифротексту та літер табл. 1:

п	0,155		ї	0,038		р	0,019		щ	0,009
л	0,099		а	0,033		т	0,019		ц	0,005
й	0,089		з	0,033		у	0,019		ю	0,005
б	0,085		ф	0,033		ш	0,019		г	0,000
д	0,061		н	0,028		е	0,014		м	0,000
в	0,047		с	0,028		х	0,014		ч	0,000
є	0,047		к	0,023		и	0,009		ь	0,000
о	0,042		ж	0,019		і	0,009		я	0,000

Так, прообразами літер із найбільшими частотами є «н, о, е, и, а, д, і, л».

Приклад 3. Криптоаналіз значно спрощується, якщо про шифротекст ми знаємо додаткову інформацію. Нехай для шифротексту з прикладу 2 відомо, що у відкритому тексті зустрічається термін «одностороння функція». Зважаючи на особливості української мови, ми можемо шукати фрагмент тексту, що відповідає шаблону «х**х**х*х», де «х» – літера шифротексту. Починаючи з 29 позиції шифротексту маємо такий фрагмент: «лєплуфлнл», що дозволяє установити відповідність:

л	є	п	л	у	ф	л	н	л
↓	↓	↓	↓	↓	↓	↓	↓	↓
о	д	н	о	с	т	о	р	о

3. Криптосистема Віженера.

Криптосистема Віженера (названа в честь Блеза де Віженера, який в 1586 р. в своєму «Трактаті про шифри» описав складнішу версію подібної системи) складається з r періодично застосованих шифрів Цезаря. У наведеному нижче прикладі ключем є слово довжини $r = 7$. В цьому слові літера з номером i визначає частковий шифр Цезаря, тобто використовується для шифрування букв відкритого тексту з номерами $i, i + r, i + 2r, \ldots$

Більш формальний опис криптосистеми Віженера:

$$\varepsilon = \left\{E_{(k_0,k_1,\dots,k_{r-1})} | (k_0, k_1, \dots, k_{r-1}) \in \mathcal{K} = \mathbb{Z}_{26}^r\right\},$$
$$E_{(k_0,k_1,\dots,k_{r-1})}(m_0, m_1, m_2, \dots) = (c_0, c_1, c_2, \dots),$$

де

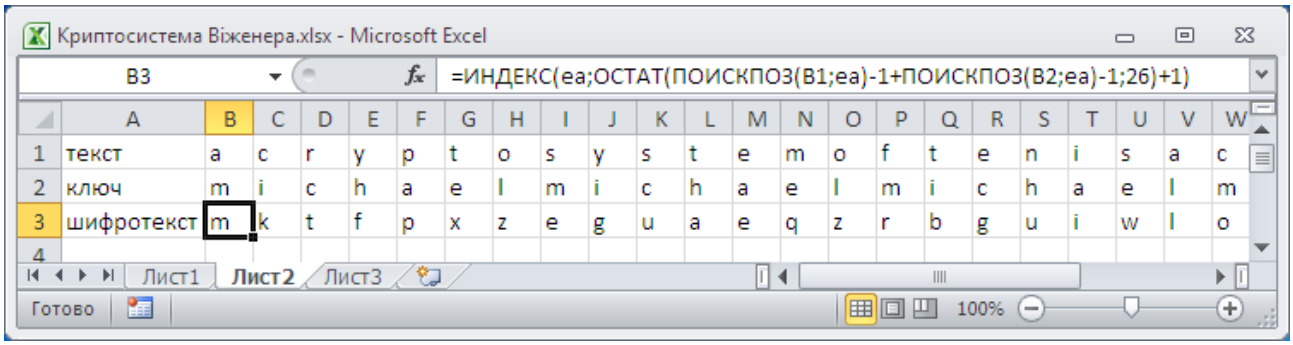
$$c_i = (m_i + k_{i \bmod r}) \bmod 26.$$

Замість періодичного використання r шифрів Цезаря в криптосистемі Віженера можна, зрозуміло, застосувати і r довільних простих замін. Така система є прикладом так званої *багато-алфавітної заміни*. Кілька століть не було ефективного способу злому цієї системи, в основному, через відсутність техніки визначення довжини ключа r. Адже, якщо вдається визначити r, то можна згрупувати літери $i, i + r, i + 2r$, ... для кожного i з інтервалу $0 \leq i < r$ і знайти (наприклад, частотним аналізом) свою заміну для кожної з цих груп окремо. У 1863 р. прусський офіцер Фрідріх В. Казіскі вказав статистичний метод знаходження довжини r ключа.

Приклад 4. Ототожнимо $\{0,1, \dots, 25\}$ з $\{a, b, \dots, z\}$. Для шифрування і дешифрування зручною є так звана таблиця Віженера (див. табл. 2). Використовуючи ключ "michael", виконуємо наступне шифрування:

текст	a	c	r	y	p	t	o	s	y	s	t	e	m	o	f	t
ключ	m	i	c	h	a	e	l	m	i	c	h	a	e	l	m	i
шифротекст	m	k	t	f	p	x	z	e	g	u	a	e	q	z	r	b

текст	e	n	i	s	a	c	o	m	p	r	o	m	i	s	e	
ключ	c	h	a	e	l	m	i	c	h	a	e	l	m	i	c	
шифротекст	g	u	i	w	l	o	w	o	w	r	s	x	u	a	g	



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	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	a	b	c	d	e	f	g	h	i	j
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u

w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Табл. 2. Таблиця Віженера.

Через надмірність природної мови ефективний розмір ключового простору істотно скоротиться, якщо в якості ключів вибирати лише осмислені слова.

4. Підрахунок числа збігів.

Розглянемо шифротекст $\mathbf{c} = c_0, c_1, \dots, c_{n-1}$, отриманий при шифруванні шифром Віженера з ключем $\mathbf{k} = k_0, k_1, \dots, k_{r-1}$ відкритого тексту $\mathbf{m} = m_0, m_1, \dots, m_{n-1}$ англійською мовою. Як уже було вияснено, основою злому криптосистеми Віженера є визначення довжини ключа r.

При проведенні аналізу будемо припускати, що джерело відкритих текстів генерує окремі літери, причому ймовірність появи кожної літери задана і не залежить від попереднього тексту. Крім того, припустимо, що букви k_i з ключа є незалежні випадкові величини, рівномірно розподілені на множині $\{a, b, \dots, z\}$ (тобто ймовірність того, що k_i виявиться деякою наперед заданою буквою, дорівнює $\frac{1}{26}$).

Позначимо через $\mathbf{c}_{left}^{(i)}$ і $\mathbf{c}_{right}^{(i)}$ підрядки рядка $\mathbf{c}$, що складаються з i крайніх лівих символів $\mathbf{c}$ і, відповідно, з i крайніх правих символів $\mathbf{c}$, тобто

$$\mathbf{c}_{left}^{(i)} = c_0, c_1, \dots, c_{i-1} \text{ і } \mathbf{c}_{right}^{(i)} = c_{n-i}, c_{n-i+1}, \dots, c_{n-1}.$$

Потім підрахуємо кількість збігів символів рядків $\mathbf{c}_{left}^{(i)}$ і $\mathbf{c}_{right}^{(i)}$, тобто таких координат j, що $\left(\mathbf{c}_{left}^{(i)}\right)_j$ і $\left(\mathbf{c}_{right}^{(i)}\right)_j$. У наступній лемі показано, що математичне сподівання частки цих збігів (тобто їх кількості, поділеної на i, – довжину рядка) дорівнює 0,06875, якщо r ділить $n-i$, і дорівнює $1/26 = 0{,}03846$, якщо r не ділить $n-i$.

Лема. Нехай шифротекст **c** отриманий при шифруванні відкритого тексту **m** шифром Віженера з ключем **k** довжини r. Нехай текст **m** породжений джерелом відкритих текстів. Інакше кажучи, букви в **m** є незалежні випадкові величини, розподіл ймовірностей $p(m)$ яких заданий. Крім того, нехай букви k_i з ключа – це незалежні випадкові величини, рівномірно розподілені на множині $\{a, b, \dots, z\}$ (тобто ймовірність того, що k_i виявиться деякою наперед заданою буквою, дорівнює $\frac{1}{26}$) . Тоді для кожної пари $(i, j), 1 \le i < j \le n$,

$$Pr[c_i = c_j] = \begin{cases} \sum_m p(m)^2 \approx 0{,}06875, \text{якщо } r \text{ ділить } j-i, \\ \frac{1}{26} \approx 0{,}03846, \text{якщо } r \text{ не ділить } j-i. \end{cases}$$

Доведення. Якщо $j-i$ ділиться на r, то $c_i = c_j$ тоді і тільки тоді, коли $m_i = m_j$. Це безпосередньо випливає з формули (2.1), оскільки $j \bmod r$ дорівнює $i \bmod r$. Таким чином,

$$Pr[c_i = c_j] = Pr[m_i = m_j] = \sum_m \Pr[m_i = m_j = m] =$$
$$= \sum_m \Pr[m_i = m] \cdot \Pr[m_j = m] = \sum_m p(m)^2 \approx 0{,}06875.$$

Якщо $j-i$ не ділиться на r, то за формулою (2.1) $c_i = c_j$ тоді і тільки тоді, коли $m_i + k_{i \bmod r} = m_j + k_{j \bmod r}$. З нерівності $i \bmod r \neq j \bmod r$ випливає, що $k_{j \bmod r}$ співпадає з $m_i + k_{i \bmod r} - m_j$ з ймовірністю $\frac{1}{26}$. Звідси

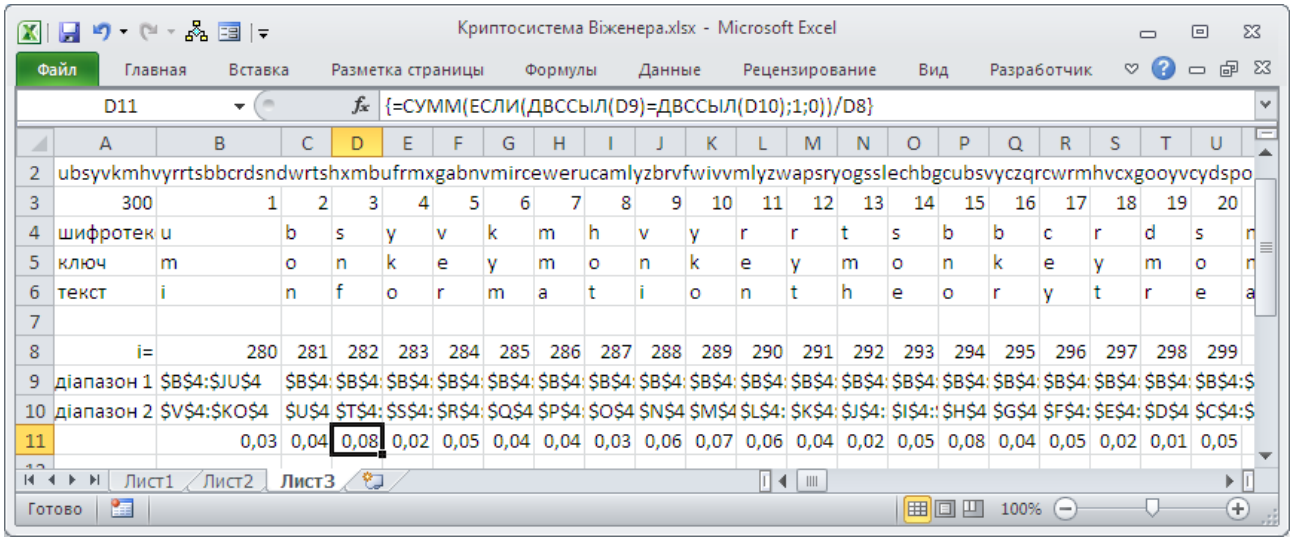
$$Pr[c_i = c_j] = \frac{1}{26} = 0{,}03846.$$

■

Зрозуміло, що чим більша довжина криптограми, тим легше визначити довжину ключа по частках збігу символів в парах рядків $\mathbf{c}_{left}^{(i)}$ і $\mathbf{c}_{right}^{(i)}$ для різних i.

Приклад 5. Розглянемо криптограму:
"ubsyvkmhvyrrtsbbcrdsndwrtshxmbufrmxgabnvmircewerucamlyzbrvfwivvmlyzwaps ryogsslechbgcubsvyczqrcwrmhvcxgooyvcydspomtqfpyqkgbcmerucadlcaflrsuqjrbhce qesfcehuoqmdstorcdoymeqqwaglgovggsmdabbigztbbqyfwbxwmgfpowgztyeilosrkgfa huovqfogswruqnvpwfvrnmpqqgsslatgrmqubsvyczqrswcjdeowqqroihqdspdibffnxwgzt bbqyfwbxus".

Використовуючи формули масиву, обчислюємо кількості збігів символів рядків $\mathbf{c}_{left}^{(i)}$ і $\mathbf{c}_{right}^{(i)}$.



Найбільші величини (0,08) виявилися в позиціях цього списку з номерами -6 і -18, а це вказує, що довжина ключа r дорівнює 6. І справді, при шифруванні був використаний шестилітерний ключ "monkey".

5. Метод Казіскі.

Криптоаналіз Казіскі криптосистеми Віженера заснований на тому факті, що якщо деяка комбінація букв (фрагмент відкритого тексту, який часто зустрічається) шифрується більш ніж один раз одним і тим же фрагментом

ключа (це відбувається через повторення ключа довжини r), то в криптограмі на відповідних місцях також виникають повторення.

Приклад 6. Розглянемо наступний відкритий текст і криптограму, отриману з нього за допомогою ключа "comet".

текст	t	h	e	r	e	i	s	a	n	o	t	h	e	r	f
ключ	c	o	m	e	t	c	o	m	e	t	c	o	m	e	t
шифротекст	v	v	q	v	x	k	g	m	r	h	v	v	q	v	y

текст	a	m	o	u	s	p	i	a	n	o	p	l	a	y
ключ	c	o	m	e	t	c	o	m	e	t	c	o	m	e
шифротекст	c	a	a	y	l	r	w	m	r	h	r	z	m	c

У криптограмі є два входження підрядка "vvqv", що починаються з 1-ї і з 11-ї позицій. Це означає, що довжина ключа r ділить 10. Крім того, два рази зустрічається і підрядок "mrh", з 8-ї і з 23-ї позицій. Таким чином, здається правдоподібним, що довжина ключа r ділить 15. Комбінуючи ці результати, можна зробити висновок, що $r = 5$. В даному випадку висновок виявляється вірним.

6. Шифр Вернама.

Одноразовий щит, іноді також кажуть *шифр Вернама* (по імені Г.С. Вернама – службовця американської компанії A.T.&T., який ввів цю систему в 1917 р.), являє собою шифр Віженера, в якому довжина ключа дорівнює довжині відкритого тексту. При цьому ключова послідовність має будуватися абсолютно випадковим чином і використовуватися тільки один раз. Інтуїтивно зрозуміло, що ця система *безумовно безпечна* (або *абсолютно стійка*). Головним недоліком такої системи є велика довжина ключа, через що система виявляється незручною в більшості додатків.

7. Шифр Плейфера.

Шифр Плейфера (1854 р., названий по імені шотландця Л. Плейфера) використовувався Британією під час Першої світової війни. Він працює з біграмами. Спершу ототожнюються букви i та j. Отримані 25 букв алфавіту розставляються по рядках матриці K розміром 5×5 наступним чином. Ключове слово виписується по рядках, починаючи з лівого верхнього кута. У ключове слово кожна буква повинна входити не більше одного разу. В іншому випадку повтори доведеться опустити. Букви, що не ввійшли в ключове, виписуються слідом за ним в алфавітному порядку. Наприклад, ключове слово "hieronymus" задає матрицю

$$\begin{Vmatrix} h & i & e & r & o \\ n & y & m & u & s \\ a & b & c & d & f \\ g & k & l & p & q \\ t & v & w & x & z \end{Vmatrix}$$

Біграма $(x, y) = (K_{i,j}, K_{m,n})$, в якій $x \neq y$, шифрується як

$$\begin{gathered} \left(K_{i,n}, K_{m,j}\right), \text{якщо } i \neq m \text{ і } j \neq n, \\ \left(K_{i,j+1}, K_{i,n+1}\right), \text{якщо } i = m \text{ і } j \neq n, \\ \left(K_{i+1,j}, K_{m+1,j}\right), \text{якщо } i \neq m \text{ і } j = n, \end{gathered}$$

де обчислення індексів проводиться за модулем 5. Якщо ж символи x, y в біграмі (x, y) співпадають, то необхідно вставити між ними букву q і продовжити шифрування тексту …*xqy*….

8. Криптосистема Хілла.

Ще одна біграмна криптосистема, яка належить Хіллу, заснована на лінійній алгебрі. Ототожнимо $\{0,1,\dots,25\}$ з $\{a,b,\dots,z\}$. Виберемо деяку квадратну матрицю K 2-го порядку, яка має обернену за модулем 26, у якості ключа. Нехай відкритий текст записаний у вигляді стовпців матриці M 2-го порядку. Тоді шифротекст отримується за формулою:

$$C = KM. \tag{1}$$

Для дешифрування використовується співвідношення:

$$M = K^{-1}C. \tag{2}$$

Приклад 7. Нехай ключ задається так:

$$K = \begin{Vmatrix} 2 & 5 \\ 3 & 3 \end{Vmatrix}$$

Відкритий текст «help» задаємо матрицею:

$$M = \begin{Vmatrix} \text{h} & \text{l} \\ \text{e} & \text{p} \end{Vmatrix} = \begin{Vmatrix} 7 & 11 \\ 4 & 15 \end{Vmatrix}$$

Тоді шифротекст отримуємо за (1):

$$C = \begin{Vmatrix} 8 & 19 \\ 7 & 0 \end{Vmatrix} = \begin{Vmatrix} \text{i} & \text{t} \\ \text{h} & \text{a} \end{Vmatrix}$$

Тобто отримуємо шифротекст «ihta».

Для дешифрування знайдемо обернену матрицю K^{-1} за модулем 26. Визначник $|K| = 17 \pmod{26}$. Для знаходження 17^{-1} необхідно знайти x із співвідношення $17x = 1 \pmod{26}$. Оскільки $\text{НСД}(17,26) = 1$, то розширений алгоритм Евкліда дає розклад $17x + 26y = 1$. Звідси $x = -3 = 23 \pmod{26}$:

26	*	1	0
17	*	0	1
9	1	1	-1
8	1	-1	2
1	1	2	-3
0	8	*	*

Далі записуємо транспоновану матрицю:

$$K' = \begin{Vmatrix} 2 & 3 \\ 5 & 3 \end{Vmatrix}$$

Приєднану матрицю:

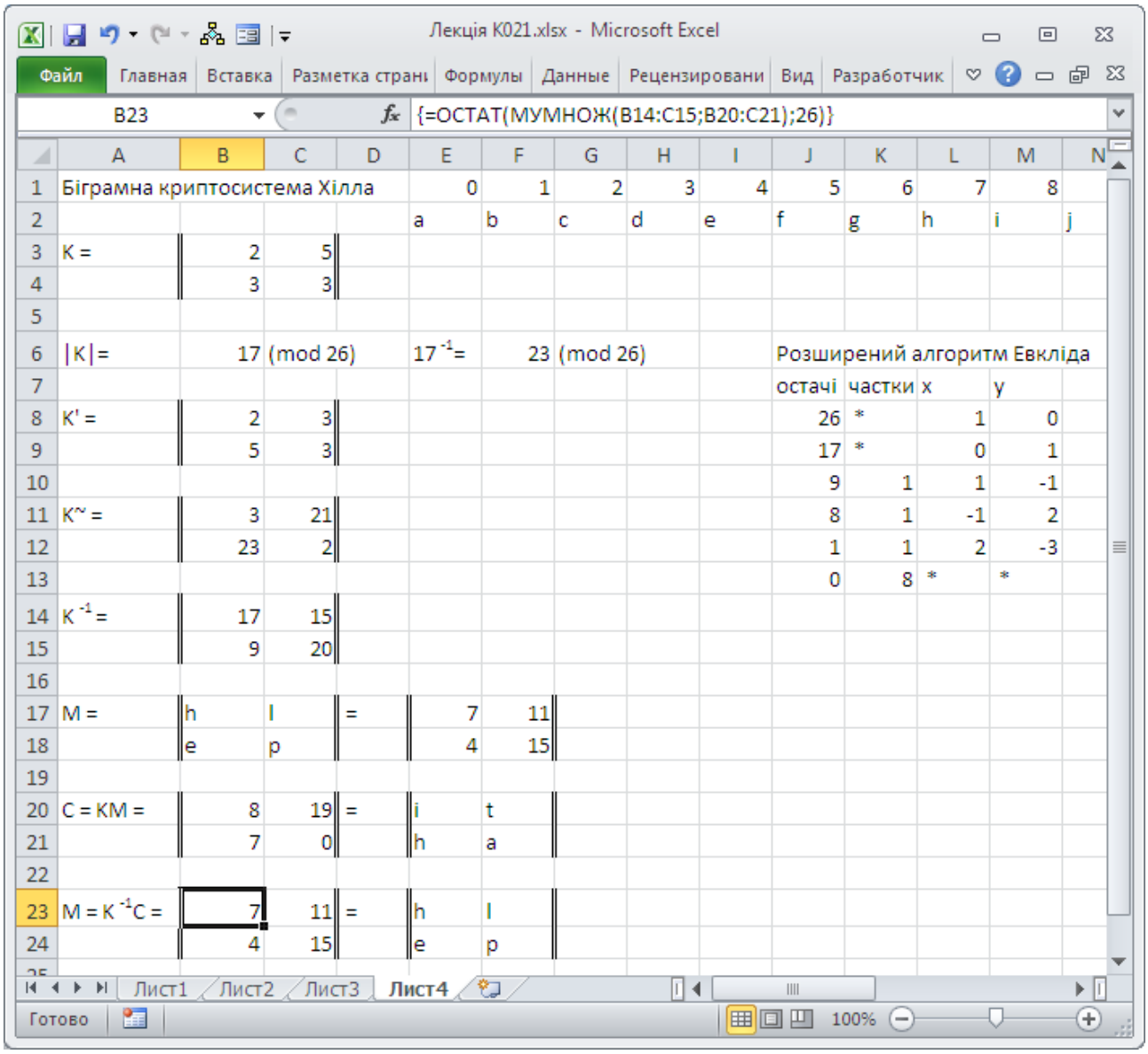
$$\widetilde{K} = \begin{Vmatrix} 3 & 21 \\ 23 & 2 \end{Vmatrix}$$

Та обернену матрицю:

$$K^{-1} = \begin{Vmatrix} 17 & 15 \\ 9 & 20 \end{Vmatrix}$$

Тоді відновлення початкового тексту реалізується за формулою (2):

$$M = \begin{Vmatrix} 7 & 11 \\ 4 & 15 \end{Vmatrix} = \begin{Vmatrix} \text{h} & \text{l} \\ \text{e} & \text{p} \end{Vmatrix}$$



9. Шифри перестановок.

Принципово інший спосіб шифрування називається *перестановкою*. Ця система розбиває текст на блоки однакової довжини, наприклад, довжини n, і застосовує до кожного такого блоку фіксовану перестановку σ координат.

Приклад 8. При $n = 5$ і $\sigma = (1,4,5,2,3)$ виходить наступне шифрування:

crypt ograp hical ... → ytrcp rpgoa cliha ...

Часто перестановка має геометричну природу, як у випадку *стовпчикової перестановки*. Відкритий текст записується по рядках в матрицю заданого

розміру, а читається по стовпцях, переставлених у порядку, визначеному ключовим словом. Наприклад, після ототожнення букв $a, b, \ldots, z$ і чисел $1,2,\ldots,26$ ключове слово "right" вказує, що першим слід читати 3-й стовпець (буква "g" розташована в алфавіті раніше інших букв слова "right"), за ним 4-й, 2-й, 1-й і нарешті 5-й. Таким чином, відкритий текст

computing science has had very little influence on computing practice

при шифруванні за допомогою матриці 5×5 і ключа "right" спочатку пишеться по рядках, як показано нижче,

4	3	1	2	5		4	3	1	2	5		4	3	1	2	5
c	o	m	p	u		y	l	i	t	t		n	g	p	r	a
t	i	n	g	s		l	e	i	n	f		c	t	i	c	e
c	i	e	n	c		l	u	e	n	c						
e	h	a	s	h		e	o	n	c	o						
a	d	v	e	r		m	p	u	t	i						

а потім читається по стовпцях в порядку нумерації, в результаті чого виходить наступний шифротекст: «mneav pgnse oiihd ctcea uschr iienu tnnct leuop yllem tfcoi …»

Перестановки не змінюють частоти букв, але руйнують взаємозв'язок між послідовними буквами відкритого тексту. Шифр Віженера та інші шифри заміни діють прямо протилежним чином. Тому часто ці системи комбінують. Такі комбіновані криптосистеми прийнято називати *добутком шифрів*. Шеннон для позначення цих факторів впливу криптоперетворень на відкритий текст вживав слова "confusion" і "diffusion" ("перемішування" і "розсіювання").

ЛІТЕРАТУРА

Базова

1. Ван Тилборг Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.
2. Венбо Мао. Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice – М.: Вильямс, 2005. – 768 с.
3. Грабарчук В., Зинович З.,Свиць А. Кибернетический подход к проектированию систем защиты информации. – Киев, 2003. – 659 с
4. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1996. – 335 с.
5. Задірака В.К., Олексюк О.С. Комп’ютерна арифметика багаторозрядних чисел. Наукове видання. – Київ, 2003. – 254 с.
6. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М: Постмаркет. – 2001. 187 с.
7. Математические и компьютерные основы криптографии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003. – 382 с.
8. Нильс Фергюсон, Брюс Шнайер Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems – М.: Диалектика, 2004. – 432 с.

Допоміжна

1. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. – М.: Гелиос АРВ, 2002. – 240 с.
2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. – М.: Горячая линия – Телеком, 2002. – 175 с.
3. Вильям Столлингс. Криптография и защита сетей: принципы и практика. – М.: Вильямс, 2001.

4. Гребенніков В.В. Історія криптології & секретного зв’язку. Ужгород. – 803 с.
5. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. – СПб.: Лань, 2000.
6. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
7. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2004.
8. Ухлинов А. М. Управление безопасностью информации в автоматизированных системах. – М.: МИФИ, 1996.
9. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.
10. Ященко В. В. Введение в криптографию. – СПб.: Питер, 2001.

Підписано до друку 21.12.2020. Формат 60х84/16.
Гарнітура Times New Roman. Ум. друк. арк. 1,8.
Наклад 100 прим. Віддруковано на різографі.

Видавництво УжНУ «Говерла»
88000, м. Ужгород, вул. Капітульна, 18.
Свідоцтво про внесення до державного реєстру видавців виготівників, і розповсюджувачів видавничої продукції
Серія Зт №32 від 31 травня 2006 року