**Лабораторна робота №1. КЛАСИЧНІ ШИФРИ. КЛАСИЧНІ ШИФРИ ПЕРЕСТАНОВКИ. КЛАСИЧНІ ШИФРИ ЗАМІНИ.**

**І КЛАСИЧНІ ШИФРИ ПЕРЕСТАНОВКИ.**

**Загальна характеристика шифрів перестановки**

*Шифр перестановки полягає в тому, що окремі знаки або певні групи знаків за певними правилами переставляються місцями безпосередньо у відкритому тексті.*

У найпростішому випадку шифр перестановки використовується як блоковий. Це означає, що в процесі шифрування знаки відкритого тексту переставляють в межах деяких блоків фіксованого розміру.

Стійкість шифру перестановки залежить від розміру блоку, а також від рівня складності порядку перестановки.

**1. Звичайна перестановка**

Розглянемо блок відкритого тексту Т=(Т1,Т2,Т3,...,ТN) довжиною N і відповідний блок попарно різних індексів σ=σ(К1,К2,К3,...,KN), де для всіх . Тут блок індексів σ є ключем шифрування.

*Звичайною перестановкою знаків даного тексту Т називається його перевпорядкування таким чином, що знак з позиції σ(і)=Кi у відкритому тексті переміщується у позицію і у криптограмі.*

*Приклад 1.* Зашифруйте відкритий текст "ШИФРУВАННЯ ПЕРЕСТАНОВКОЮ". Для шифрування використайте ключ   
 для блоку довжиною N=8.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Текст | Ш | И | Ф | Р | У | В | А | Н |
|  | 3 – Ф | 8 – Н | 1 – Ш | 5 – У | 2 – И | 7 – А | 6 – В | 4 – Р |

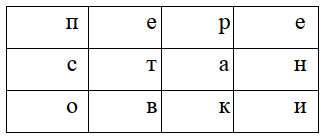
В результаті маємо криптограму

"ФНШУИАВР\_СНЕЯЕРПНЮТВАОКО".

Загальна можлива кількість перестановок заданого тексту Т із N знаків рівна N!, значення якого швидко зростає зі збільшенням N.

**2. Звичайні рядково-стовпчикові табличні перестановки**

Це перестановки, коли даний текст записується у прямокутну таблицю певного розміру по рядках (послідовне заповнення її рядків зліва направо), а зашифрований текст отримують шляхом прочитування її послідовних стовпчиків згори вниз.

*Приклад 2.* Для повідомлення «ПЕРЕСТАНОВКИ» за допомогою шифрувальної таблиці розміром 3х4 буде отримано криптограму «псоетвракени».

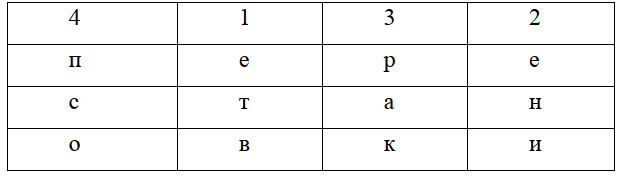
Ключем шифру є розмір таблиці (для наведеного прикладу 3х4).

Для отримання вихідного повідомлення, слід вписати криптограму в таблицю того ж самого розміру по стовпчиках, а прочитати по рядках.

Таку перестановку називают *звичайною стовпчиково-рядковою.*

**3. Рядково-стовпчикові табличні перестановки із застосуванням ключа стовпчиків**

Процес шифрування полягає в тому, що над верхнім рядком таблиці записують ключ – вектор індексів перестановок стовпчиків. Після цього здійснюють вписування відкритого тексту у таблицю по рядках звичайним способом.

*Приклад 3.* Для повідомлення «ПЕРЕСТАНОВКИ» та ключа (4, 1, 3, 2) криптограма утворюється шляхом прочитування по стовпчиках, які беруться у порядку, визначеному ключем. Таким чином отримуємо криптограму «етвениракпсо».

*Аналогічна процедура для шифрування з ключем рядків.*

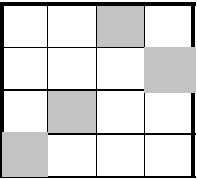
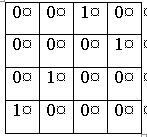
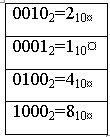
**4. Табличні перестановки з використанням трафарету**

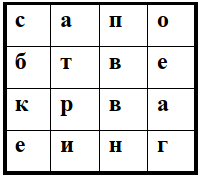
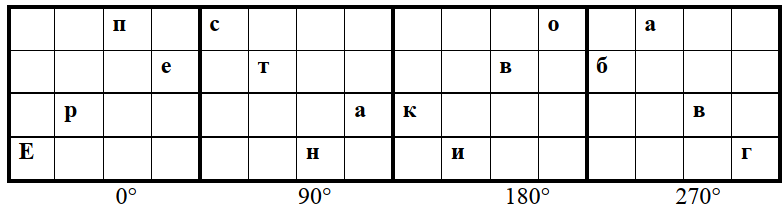
Квадратним трафаретом називають нанесену на планшет квадратну матрицю з прорізаними віконцями, кількість яких не повинна перевищувати чверті від загальної кількості клітинок трафарету.

Планшет, як маску, накладають на папір того ж розміру, і у віконця вписують знаки повідомлення по порядку слідування рядків зліва направо. Після першого заповнення планшет, повертають на 90° за годинниковою стрілкою і процедуру вписування повторюють. Таким способом вписування знаків повідомлення у віконця може бути здійснене чотири рази. При цьому віконця квадратного трафарету після кожного повороту опиняються над незаповненими клітинками паперу. З цією метою розташування віконець на трафареті підбирають спеціально .

Щоб описати трафарет, застосовують позначення: нуль – віконце відсутнє, одиниця – віконце є. Таким чином, весь трафарет можна представити у вигляді сукупності двійкових чисел, кожне з яких відповідає його рядку. Ці числа доцільно представити у десятковій системі числення. Зрозуміло, що сукупність цих чисел являє собою ключ шифру.

Якщо кількість віконець трафарету більше кількості знаків повідомлення, то порожні віконця заповнюються випадковими знаками.

*Приклад 4.* Перетворити повідомлення «перестановки» за допомогою квадратного трафарета розміром 4х4, що має чотири віконця. Ключ (2, 1, 4, 8).



На останньому четвертому повороті трафарету знаки повідомлення вже вичерпались, і тому порожні віконця були заповнені додатковими випадковими знаками «абвг». Отримана криптограма «сапобтвекрваеинг».

Для дешифрування криптограми потрібний такий же самий квадратний трафарет.

**5 Застосування магічних квадратів**

Магічними квадратами називають квадратні таблиці, в кожну клітинку яких вписано послідовні натуральні числа починаючи з 1, які дають у сумі по кожному стовпцю, кожному рядку і кожній діагоналі те саме число.

Існує тільки один магічний квадрат розміром 3×3 (якщо не враховувати його повороти). Кількість магічних квадратів 4×4 становить уже 880, а кількість магічних квадратів 5×5 – близько 250000.

Текст, що шифрується, вписується в магічні квадрати відповідно до нумерації їх клітинок. Якщо потім виписати вміст такої таблиці по рядках, то вийде шифротекст, сформований завдяки перестановці букв вихідного повідомлення.

Наприклад, методом магічного квадрата виконати шифрування тексту «ВІРТУАЛЬНИЙ КАНАЛ» .

Шифрування тексту зробимо з використанням магічного квадрата розміром 4×4 (рис. 5) .

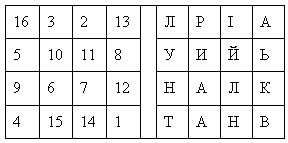
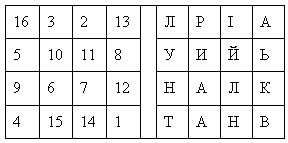
 

Рисунок 5 – Приклад магічного квадрата 4×4 і його заповнення

Шифротекст, який одержали при зчитуванні вмісту правої таблиці по рядках групами по чотири букви, має такий вигляд:

ЛРІА УИЙЬ НАЛК ТАНВ або ЛРІАУИЙЬНАЛКТАНВ.

**І І КЛАСИЧНІ ШИФРИ ЗАМІНИ.**

**Загальна характеристика шифрів заміни**

У загальному випадку шифр заміни здійснює перетворення, при якому літери або якісь інші фрагменти відкритого тексту замінюються відповідними фрагментами шифрованого тексту.

Найпростіший випадок шифрування заміною полягає в тому, що знаки відкритого тексту, записані в одному (первинному) алфавіті, заміняють знаками, що взято із іншого (вторинного) алфавіту, у відповідності з наперед установленим правилом.

Якщо використовується один і той же вторинний алфавіт, то шифр заміни називають моноалфавітним. Якщо вторинних алфавітів декілька, то шифр називають багатоалфавітним.

tableSZНехай шифруються повідомлення за допомогою первинного алфавіту. Тоді кожній букві вихідного алфавіту зіставляється деяка множина символів (шифрозаміни), наприклад для українського алфавіту А ↔ М1=МА, Б ↔ М2=МБ, ..., Я ↔ М33=МЯ.

Шифрозаміни обираються таким чином, щоб будь-які дві множини не містили однакових елементів .

Наведена таблиця є ключем шифру заміни, за допомогою якої можна здійснити як шифрування, так і розшифрування.

Наприклад, [таблиця](http://ua-referat.com/%D0%A2%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D1%96) простої заміни (кожна множина складається тількі з одного елемента) може [мати](http://ua-referat.com/%D0%9C%D0%B0%D1%82%D0%B8) наступний вигляд:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Символи первинного алфавіту | а | б | в | г | д | е | ж | з | і | ї | л | м | н | о | п | р | с | ... |
| Символи вторинного алфавіту (заміна) | s | р | x | l | r | z | i | m | a | y | e | d | w | t | b | g | v | ... |

Шифрограма для тексту «перемога» буде наступною – «bzgzdtls».

Одним із перших моноалфавітних шифрів заміни вважається полібіанський квадрат. У II столітті до н.е. грецький письменник та історик Полібій винайшов з метою шифрування квадратну таблицю розміром 5х5, заповнену літерами грецького алфавіту у випадковому порядку.

При шифруванні чергову літеру відкритого тексту знаходили у цьому квадраті, а у криптограму записували літеру, розташовану рядком нижче в тому ж стовпчику. Якщо літера знаходилась у нижньому рядку таблиці, то для криптограми брали саму верхню літеру з того ж стовпчика.

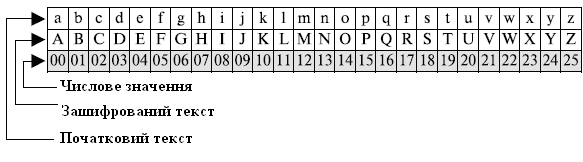
Таким чином, основним для будь-якого шифру заміни є поняття алфавіту, який являє собою фіксовану послідовність всіх використовуваних знаків. При цьому фіксується як порядок слідування знаків, так і їх загальна кількість. Знаки алфавіту нумеруються по порядку, починаючи з нуля, тобто *0 ≤ j < m*. Таким чином, *m* являє собою загальну кількість знаків в алфавіті і називається його обсягом.

Знаки відкритого тексту теж доцільно нумерувати, починаючи з нуля, тобто *0 ≤ i < n*. Тут *n* являє собою загальну кількість знаків у повідомленні.

**1 Моноалфавітна звичайна заміна Цезаря (шифр Цезаря)**

Римський імператор Гай Юлій Цезар використовував у своєму військовому та особистому листуванні шифр, суть якого полягала у заміні кожної літери повідомлення на одну з інших літер того ж самого алфавіту 26-значного латинського алфавіту.

Принцип дії полягає в тому, щоб циклічно зсунити алфавіт, а ключ — це кількість літер, на які робиться зсув.

Припустимо, що початковий текст складається з маленьких букв (від а до z ) і зашифрований текст складається із заголовних букв (від A до Z ). Щоб забезпечити застосування математичних операцій до початкового і зашифрованого текстів, ми привласнимо кожній букві числове значення (для нижнього і верхнього регістра), як це показано на малюнку.  
[](https://teteryakv12.files.wordpress.com/2014/10/imagehandler-1.png)

Якщо зіставити кожному символу алфавіту його порядковий номер (нумеруючи з 0), то шифрування й дешифрування можна виразити формулами:  
Y= (Х + k )mod n   і     X = (У – k) mod n, де:

X — символ відкритого тексту,

Y — символ шифрованого тексту,

n — потужність алфавіту,

k — ключ.

Припустимо, що, використовуючи шифр Цезаря, з ключем, який дорівнює 3, необхідно зашифрувати словосполучення «ШИФР ЦЕЗАРЯ».

Для цього зрушимо алфавіт так, щоб він починався з четвертої букви (Г). Отже, беручи вихідний алфавіт

АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ,

і зміщуючи всі літери вліво на 3, отримуємо відповідність:  
А Б В Г Ґ 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  
Г Ґ 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,  
де Г=А, Ґ=Б, Д=В, і т. д.

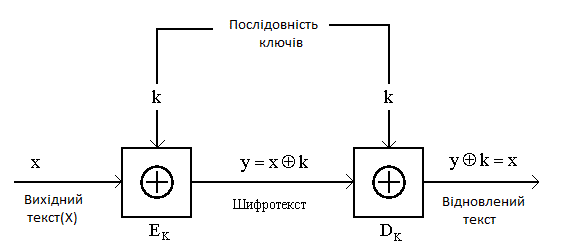
Використовуючи цю схему, відкритий текст «ШИФР ЦЕЗАРЯ» перетворюється на «ЮЙЧУ ЩЗЇГУВ». Для того, щоб одержувач повідомлення міг відновити вихідний текст, необхідно повідомити йому, що ключ — 3.

Шифр Цезаря має замало ключів — на одиницю менше, ніж літер в абетці. Тому перебрати усі ключі не складає особливої роботи. Дешифрування з одним з ключів дасть нам вірний відкритий текст.

**2 Шифр Вернама**

Ідеальна таємність, за Шеноном може бути досягнута, якщо символи вихідного тексту зашифровані за допомогою ключа, обраного випадково з деякої області ключів. Ця ідея реалізована в використовується в шифрі Вернама, який називається одноразовим блокнотом. У цьому шифрі ключ має ту ж саму довжину, що й вихідний текст, і обраний зовсім випадково.

Кожен символ вихідного відкритого текcту із англійського алфавіту {A,B,C,…,Z}, що розширений 5 допоміжними знаками (пробіл і т. д), спочатку кодувався в 5-бітовий  блок телеграфного коду Бодо. Далі випадкова послідовність ключів k0, k1 ,… наперед записувалась на паперовій стрічці. Схема передачі з використанням шифру Вернама показана на рис 6.

[](https://teteryakv12.files.wordpress.com/2014/10/image138.gif)

* – операція додавання за модулем 2.

Приклад шифрування: Текст 11001110101 – Х, Ключ 10101010101 – К, Сума за модулем 2 01100100000 – .

Дешифрування: Шифр 01100100000 – У, Ключ 10101010101 – К, Сума за модулем 2 11001110101 – Х

**3 Шифр Віженера**

Шифр Віженера — поліалфавітний шифр, який у якості ключа використовує слово. Був створений Блезом де Віженером, французьким математиком шістнадцятого сторіччя. Шифр Віженера використовує стратегію створення потоку ключів. Потік ключів – повторення початкового потоку ключа засекречування довжини m, де ми маємо 1 < m < 26. Шифр може бути описаний у такий спосіб: (k1, k2, …., km) – первісний ключ засекречування.

Якщо пронумерувати літери алфавіту від 0 до 32 (а → 0, б → 1, в → 2, …), то шифрування Віженера можна представити формулою

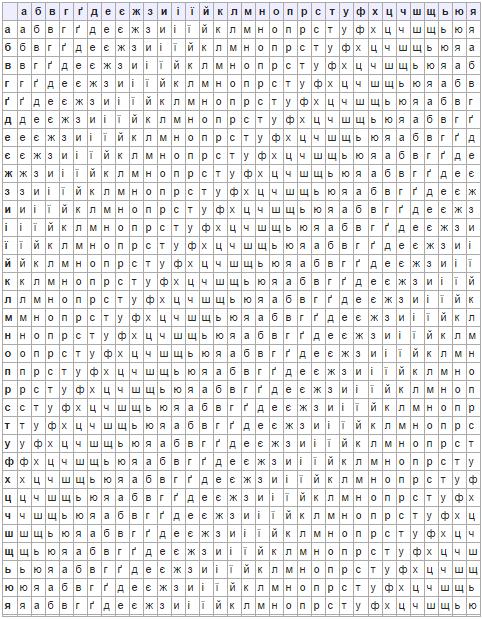
Ci = (Pi + Kj) mod 33, де Kj — j-та літера ключового слова.

P = P1,P2,P3….. C = C1,C2,C3….. k = [(k1,k2), (k3,k4),…..]

Шифрування Ci = ki Дешифрування Pi = ki

Ключове слово повторюється, поки не отримано гаму, довжина якої дорівнює довжині повідомлення.

Таблиця для шифрування

[](https://teteryakv12.files.wordpress.com/2014/10/d0b2d0bfd0b0d0bfd0b0d0bf.jpg)

По вертикалі вибираємо літери відкритого тексту, а по горизонталі — ключа, на перетині цих значень отримуємо знаки шифротексту.

Приклад

Відкритий текст: «полі/алфа/вітн/ий ши/фр»

Ключ: «ключ/ключ/ключ/кл юч/кл»

Шифротекст: «аайд/кьтч/мцрі/фш цґ/дв».

У разі, якщо ключове слово рівне довжині повідомлення і використовується лише один раз, такий варіант шифра Віженера практично еквівалентний Шифрові Вернама.

**3. Шифр Цезаря з ключовим словом**

Шифр Цезаря з ключовим словом теж є моноалфавітним. Він має ту особливість, що порядок знаків у вторинному алфавіті у порівнянні з первинним є дещо іншим завдяки використанню ключового слова. Крім того, практично необмеженою стає кількість ключів.

Для шифрування як ключ вибирається деяке число *0 ≤ K < m*, а також ключове слово. Всі знаки ключового слова мають бути різні.

Ключове слово записують під знаками алфавіту, починаючи зі знаку, числовий код якого співпадає з числом *K*. Знаки алфавіту, що залишились, записують за ключовим словом в алфавітному порядку.

Припустимо, що для алфавіту “АБВГДЕЖЗИК” обсягом *m=10* ключем вибрано число K = 3 і ключове слово БЕДА. Отримуємо шифрувальну

таблицю:

Номер (код) Знак відкритого тексту Ключове слово

Знак криптограми

0 1 2 3 4 5 6 7 8 9

А Б В Г Д Е Ж З И К

Б Е Д А

З И К

В Г Ж

32

В цій таблиці первинний алфавіт (для відкритого тексту) вказано в другому рядку, вторинний (для криптограми) – в третьому та четвертому. У відповідності з цією таблицею відкритий текст ЖАЖДА шифрується як АЗАЕЗ. Вимога про відмінність всіх знаків ключового слова не є обов’язковою. В цьому випадку просто записують ключове слово без повторення однакових

знаків. Наприклад, ключове слово ЖАЖДА записують як ЖАД.

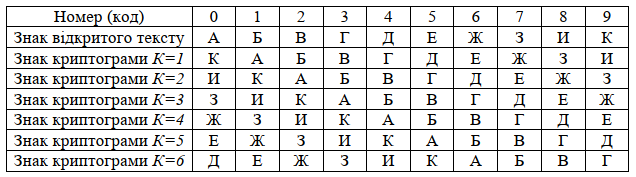
В шифрі Цезаря з ключовим словом недолік моноалфавітної звичайної заміни Цезаря, пов’язаний з відсутністю маскування частот появи різних знаків відкритого тексту, зберігається. [8]

**4. Шифр Гронсфельда**

Шифр Гронсфельда являє собою модифікацію моноалфавітної звичайної заміни Цезаря більш складним ключем, який являє собою послідовність чисел. Кожне з чисел ключа має бути меншим обсягу алфавіту *m*. Цей ключ записують під відкритим текстом. Якщо ключ коротший відкритого тексту, то його повторюють циклічно. Кріптограму отримують як і в шифрі Цезаря, але здійснюють відлік такої кількості літер, яка указана відповідним числом ключа.

Таким чином, шифр Гронсфельда є багатоалфавітним, оскільки використовує декілька вторинних алфавітів (по кількості різних чисел у складі ключа).

Наприклад, для алфавіту “АБВГДЕЖЗИК” обсягом *m=10* шифрувальна таблиця для чисел ключа в межах від *K=1* до *K=6* має наступний вигляд:



Для прикладу зашифруємо відкритий текст “ЗАДВИЖКА”, використовуючи ключ (5, 1, 3). Розмістимо ключ під відкритим текстом:

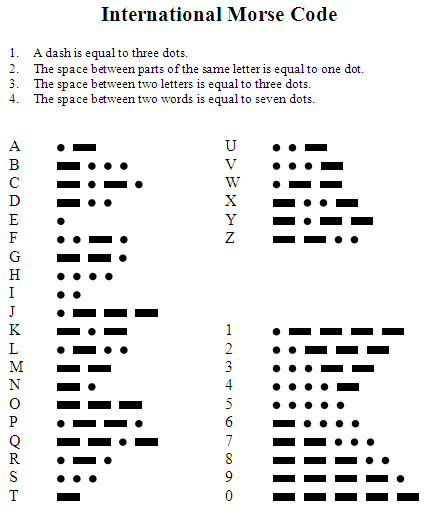
33

З А Д В И Ж К А 5 1 3 5 1 3 5 1

Щоб зашифрувати першу літеру відкритого тексту З, треба використати перше число ключа 5. Це означає, що відповідний знак криптограми треба взяти із того рядка шифрувальної таблиці, для якого K=5. Отримуємо першу літеру криптограми В. Щоб зашифрувати другу літеру відкритого тексту А, треба використати друге число ключа 1. Це означає, що відповідний знак криптограми треба взяти із того рядка шифрувальної таблиці, для якого K=1. Отримуємо другу літеру криптограми К. Остаточно отримуємо криптограму ВКБЗЗГДК. [8]

**Азбука Морзе**

Всі телеграфи використовують так званий телеграфний код - прийняту умовну систему позначень, в якій кожній літері (або знаку) відповідає своя комбінація елементарних посилок електричного струму. Елементарна посилка (елемент коду) - найліпша, з них складаються всі інші. Кількість елементарних посилок для позначення кожного знака в коді може бути різним (нерівномірні коди, наприклад, код Морзе) або однаковим (рівномірні коди, наприклад, код Бодо). Число значень, яке може набувати елементарна посилка в процесі передачі, називається підставою коду - за цією ознакою коди діляться на бінарні (двійкові), потрійні і якісь ще. Залежно від числа елементарних посилок для передачі знаків розрізняють рівномірні коди 5- елементні, 6-елементні і так далі. «Код Морзе» (він же «морзянка») - ні що інше, як нерівномірний телеграфний код, в якому знаки позначаються комбінаціями з посилок струму різної тривалості (рис. 3.2). За одиницю тривалості приймається тривалість точки, а тривалість «тире» дорівнює тривалості трьох крапок. Пауза між знаками в букві - одна точка, а між буквами в слові - 3 точки. Пауза між словами становить 7 точок. Всі знаки в коді Морзе утворюють так звану азбуку Морзе:



**5. Гомофонічна заміна**

Гомофонічна заміна одному знакові відкритого тексту ставить у відповідність декілька різних символів криптограми. Цей метод застосовується для спотворення статистичних властивостей криптограм. Наприклад, для алфавіту “АБВГДЕЖЗИК” обсягом m=10 шифрувальна таблиця для кожного знаку алфавіту може містити набори по три різні символи у вигляді довільних двозначних чисел, вибраних випадковим способом:

Номер (код) Знак відкритого тексту

Символи криптограми

0 1 2 3 4 5 6 7 8 9

А Б В Г Д Е Ж З И К

17 23 14 55 37 97 47 76 27 77 31 44 89 52 88 51 67 19 64 38 48 63 42 11 25 15 33 59 73 45

Для прикладу зашифруємо відкритий текст “ЖАДАЖА”. Для шифрування першої літери відкритого тексту Ж застосовуємо відповідний перший символ криптограми 47. Аналогічно для літер відкритого тексту А і Д, які теж зустрічаються перший раз, використовуються відповідні перші символи криптограми 17 і 37. Четверта і п’ята літери криптограми А і Ж зустрічаються вдруге, тому для них відповідними символами криптограми будуть 31 і 67.

34

Остання шоста літера криптограми А зустрічається втретє, тому вона буде шифруватись символом 48. Остаточно криптограма має вигляд 471737316748. Бачимо, що при використанні шифру гомофонічної заміни кожний знак відкритого тексту замінюється відповідними символами криптограми по черзі. Після того, як весь набір символів для даного знаку вичерпався, здійснюється його повторне використання з початку. [8]

**6. Шифруюча таблиця Трисемуса**

Багато хто з істориків вважають Іоганна Трисемуса, аббата з Німеччини, одним із засновників сучасної криптології. У 1508 році Трисемус написав свій твір “Поліграфія” – перший друкований твір з криптології. В ньому він вперше описав свій шифр, відомий під назвою шифруюча таблиця Трисемуса. В цьому шифрі використовується прямокутна таблиця певного розміру (по можливості, якнайближча до квадратної) для запису знаків алфавіту і ключове слово, записане без повторення однакових знаків. Для заповнення шифрувальної таблиці використовується підхід, запозичений із шифру Цезаря з ключовим словом. Спочатку в таблицю по рядкам вписується ключове слово. Далі таблиця доповнюється рештою знаків в алфавітному порядку. Наприклад, для алфавіту “АБВГДЕЖЗИКЛМ” обсягом *m =12* шифрувальна таблиця може мати розмір 3х4. Виберемо ключове слово ЖАД. За таких умов шифрувальна таблиця має такий вигляд:

Ж А Д Б В Г Е З И К Л М

Спосіб шифрування запозичений із полібіанського квадрата. При шифруванні чергову літеру відкритого тексту знаходили у шифрувальній таблиці, а у криптограму записували літеру, розташовану рядком нижче в тому ж стовпчику. Якщо літера знаходилась у нижньому рядку таблиці, то для криптограми брали саму верхню літеру з того ж стовпчика. Наприклад, ГЛАЗ шифрується як КДГМ. [8]

35

**7. Біграмний шифр Плейфера**

Даний шифр називається біграмним тому, що шифруються одночасно не один, а два сусідні знаки відкритого тексту. Шифрувальна таблиця Плейфера являє собою прямокутну матрицю (по можливості, якнайближчу до квадратної). Її розміри мають бути достатніми для розміщення всіх знаків алфавіту відкритого тексту. Матриця заповнюється знаками алфавіту випадковим способом. Наприклад, для алфавіту “АБВГДЕЖЗИКЛМ” обсягом *m=12* шифрувальна таблиця може мати наступний вигляд:

Ж А Д Б В Г Е З И К Л М

*Процес шифрування складається з таких кроків.*

1. Відкритий текст розбивається на пари знаків (біграми). В тексті повинна бути парна кількість знаків і не повинно бути біграм з однаковими знаками. Якщо ці умови не виконуються, то текст модифікують з утворенням незначних орфографічних помилок. *Наприклад*, можна замінити один із цих знаків іншим, вставити між ними дефіс або виключити один із них взагалі. Після цього кожна дана біграма відкритого тексту за допомогою шифрувальної таблиці перетворюється в результуючу біграму криптограми.

2. Якщо обидва знаки даної біграми відкритого тексту знаходяться в різних рядках та стовпчиках матриці, то вони вважаються протилежними кінцями діагоналі відповідного прямокутника. Результуючу біграму криптограми знаходять на кінцях другої діагоналі цього ж прямокутника. Знак, який знаходиться на лівому кінці першої діагоналі, замінюється знаком який знаходиться на лівому кінці другої діагоналі. Знак, який знаходиться на правому кінці першої діагоналі, замінюється знаком, який знаходиться на правому кінці другої діагоналі. Наприклад, даним біграмам відкритого тексту АЛ, МА, ДИ і КЕ відповідають результуючі криптограми КД, БК, ЛЖ і ГЛ.

3. Якщо знаки даної біграми знаходяться в одному й тому ж рядку, то кожний із знаків замінюється тим, що стоїть справа від нього (за останнім

36

знаком у рядку йде перший). Наприклад, даним біграмам ЖБ і ЛИ відповідають результуючі біграми АЖ і МК.

4. Якщо знаки даної біграми знаходяться в одному й тому ж стовпчику, то кожний із знаків замінюється тим, що стоїть нижче його (за останнім нижнім знаком йде самий верхній). Наприклад, даним біграмам ЖВ, ЛД і МЗ відповідають результуючі біграми ВИ, ДЕ і БМ. Наприклад, відкритий текст БАЗА перетворюється на криптограму ЖДБГ. [8]

**8. Біграмний двотабличний шифр**

Цей шифр винайдений у 1854 році англійцем Чарльзом Уитстоном. Такий метод використовує дві прямокутні таблиці однакового розміру *(по можливості, якнайближчі до квадрату)*, в кожній з яких випадковим способом розміщено один і той же алфавіт. Відкритий текст розбивають на пари знаків – біграми. Перший знак біграми відкритого тексту фіксується у першій таблиці, другий знак біграми – у другій. Між зафіксованими знаками вибудовується уявний прямокутник. Одна діагональ цього прямокутника з’єднує знаки біграми відкритого тексту, друга діагональ дає результуючу біграму до криптограми. Перший знак результуючої біграми теж прочитується із першої таблиці, другий знак біграми – із другої таблиці. Якщо знаки відкритого тексту потрапили в один і той же рядок, то і біграма криптограми береться з того ж рядка. Перший знак біграми криптограми береться із першої таблиці у стовпчику, номер якого такий же, як і номер стовпчика другого знаку біграми відкритого тексту. Другий знак біграми криптограми береться із другої таблиці у стовпчику, номер якого такий же, як і номер стовпчика першого знаку біграми відкритого тексту. При використанні алфавіту, який складається із десяти цифр, крапки та пропуску, шифрувальна таблиця може бути такою:

Таблиця 1

2 7 .

Таблиця 2

0 2 7

6 0 3 \_ . 4

1 4 9 6 8 5

\_ 5 8 3 1 9

37

У відповідності з цією таблицею біграму «78» буде зашифровано як «42», біграму «42» – як «78», біграму «59» – як «81» і т.д. А для повідомлення «2.718\_3.14» одержимо криптограму «6252330465». Перевагою біграмного двотабличного шифру у порівнянні з біграмним шифром Плейфейра є можливість використання біграм з однаковими знаками. [8]

**9. Координатні заміни**

В координатних замінах знаки алфавіту використовуються для позначень координат шифрувальної таблиці. Якщо алфавіт має *N* знаків і мова йде про двохкоординатну заміну, то шифрувальна таблиця має форму квадрата розміром *N\*N*. В окремих комірках таблиці випадковим способом розміщують всі *N* можливих пар знаків, а вертикалі та горизонаталі таблиці позначають знаками, розташованими в алфавітному порядку. Відкритий текст розбивають на пари знаків – біграми. Перший знак біграми відкритого тексту використовується як індекс рядка, другий знак біграми – як індекс стовпчика. На їх перетині знаходиться результуюча біграма до криптограми. *Наприклад,* при використанні алфавіту «0, 1, 2» шифрувальна таблиця може мати такий вигляд:

0 1 2 0 10 21 01 1 00 20 11 2 12 02 22

Для такої шифрувальної таблиці повідомлення «1020110221» перетворюється на криптограму «0012200102».

Суть ускладненого координатного методу, полягає в тому, що таблиці з числами ставиться у відповідність таблиця з алфавітом, тоді кожній літері у відповідність ставляють числа, приклад:

0 1 2 0 1 2 0 10 21 01 0 А Б В

1 00 20 11 1 Г Д Е 2 12 02 22 2 Ж Й К

Тоді, наприклад, слово ДАВАЙ перетвориться на «2010011002».

**Завдання до лабораторної роботи.**

І Зашифрувати своє прізвище ім‘я та по-батькові за допомогою зазначених алгоритмів (за необхідності перетворити ПІБ в транслітерований текст Сідоренко –Sidorenko):

- звичайної перестановки (ключ сформувати самостійно);

- магічного квадрату , та (квадрат обрати самостійно та навести у відповіді);

- трафарету;

- рядково-стовпчикової табличної перестановки із застосуванням ключа стовпчиків (ключ обрати самостійно);

- шифру Цезаря;

- Полібіанського квадрата;

- шифруючої системи Трисемус;

- шифру Playfair;

- азбуки Морзе;

- системи омофонів (допускається для кожної літери алфавіту навести всього по дві шифрозаміни, тобто прийняти, що всі літери мають однакову ймовірність появи в текстах);

- шифру Віженера.

ІІ Дешифрувати отримані в (І) зашифровані тексти.

При оформленні звіту необхідно навести вихідне повідомлення, таблицю шифрозамін, ключ (якщо таблиця шифрозамін не є ключем) та зашифроване повідомлення.