1 ОСНОВНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Актуальність проблеми захисту інформації

Комп’ютерні інформаційні технології охоплюють методи збору, обробки,

зберігання і передачі інформації по каналах зв’язку. Поряд із ефективним опрацюванням і передачею інформації актуальною є проблема забезпечення її безпеки. Це пояснюється особливою інформаційних ресурсів, зростанням вартості інформації в умовах ринку та її значними втратами в результаті несанкціонованого використання.

Створення сучасної технології зв'язків між організаціями і інформаційними системами приводить до виникнення наступних проблем.

- Укладання угод і встановлення стандартів для комп’ютерного зв’язку;
- Організація доступу до стратегічної інформації;
- Організація захисту і безпеки інформації.

Великі втрати приносить порушення безпеки передачі даних. Втрати від несанкціонованого проникнення в інформаційні системи оцінюються дорого і приводять до фінансових втрат. Для боротьби з порушеннями інформаційної безпеки користувач повинен знати всі канали витоку інформації.

Оскільки комп’ютер стає інструментом користувача, а інформаційні системи – засобом підтримки прийняття рішень, то важливою умовою безпеки є безпека в комп’ютерних мережах. Основними проблемами при передачі інформації в комп’ютерних мережах є:

- Читання чужої інформації (порушення конфіденційності).
- Порушення цілісності інформації;
- Блокування доступу до інформаційних ресурсів в мережах.

В комп’ютерних мережах є велике число способів для несанкціонованого доступу до інформації. Суть захисту інформації полягає в забезпеченні та запобіганні несанкціонованого доступу до неї. Надійний захист здійснюється

комплексним забезпеченням безпеки засобів опрацювання інформації. Окремо взятий спосіб захисту не забезпечить повноцінну безпеку передачі інформації. Методи захисту даних можна поділити на:

– Методи маскування або стеганографії, які приховують факт наявності

повідомлення;

– Методи тайнопису або криптографії;

– Методи орієнтовані на спеціальні технічні пристрої для засекречування інформації.

Секретна інформація містить державну й іншу передбачену законом таємницю, розголошення якої може завдати шкоди державі і людині. Доступ громадян до інформації, що складає державну таємницю, здійснюється відповідно до закону про цю інформацію.

Важливе місце в системі безпеки даних займають спеціальні служби, основною задачею яких є організація робіт, що попереджають витік інформації. Ці служби здійснюють методичне керівництво розробкою вимог по захисту інформації від несанкціонованого доступу.

Основною характеристикою діяльності служб, пов'язаних з захистом інформації, є забезпечення функціонування системи захисту як комплексу організаційних і програмно-технічних засобів, що передбачає:

- Збереження і видача користувачам паролів і ключів;
- Ведення службової документації служби захисту інформації, яка включає генерацію паролів, ключів та правил доступу до даних;
- Контроль за функціонуванням служби захисту інформації; і за процесом опрацювання і передачі інформації.

Правове забезпечення організації і проведення заходів захисту інформації є сукупність законів, нормативних актів і правил, які регламентують загальну організацію робіт. Для забезпечення системи безпеки інформації необхідно розв'язати такі задачі:

- Розробити правові основи системи безпеки інформації, що

регламентує відношення і розмежування сфери повноважень всіх учасників інформаційних відношень;

- Розробити законодавчі акти і правові норми, що охоплюють усі

проблеми захисту інформації;

- Стандартизувати вимоги по захисту інформації в обчислювальній техніці, в автоматизованих системах, інформаційних мережах та засобах телекомунікації.

Засоби захисту інформації діляться на технічні, програмні, законодавчі та організаційні. Технічні засоби захисту інформації діляться на фізичні й апаратні. Фізичні засоби виконують функції загального захисту об'єктів, на яких опрацьовується інформація. Вони реалізуються у виді автономних пристроїв і систем. Апаратні засоби це – вбудовані пристрої безпосередньо в обчислювальну техніку та телекомунікаційну апаратуру передачі інформації. До відомих апаратних засобів відносяться схеми контролю інформації на парність, схеми захисту масивів пам'яті по ключу і т. д.

Програмні засоби призначені для перетворення відкритих текстів до незрозумілого вигляду, шляхом розробки відповідного програмного забезпечення. Зміна вигляду відкритого тексту для захования його змісту називається шифруванням. Відкритим текстом може бути текстовий файл або бітове зображення. Зашифроване повідомлення називається шифротекстом. Операція перетворення зашифровано тексту у початковий називається дешифруванням або розшифруванням. Шифруванням і дешифруванням текстів займається криптографія Розшифруванням шифротекстів називається криптоаналізом. Галузь, що охоплює криптографію і криптоаналіз, називається криптологією. а люди, які нею займаються, називаються криптологами.

Організаційні засоби включають організаційно-технічні й організаційно-правові заходи.

Морально-етичний захист включає норми, що традиційно склалися в даній країні. Хоча ці норми не є обов'язковими для виконання, їх недотримання веде до

втрати авторитету та іміджу розголошувача конфіденційної інформації.

Законодавчі засоби захисту визначаються законами, постановами та актами, які регламентують правила використання та опрацювання секретної інформації. Порушення цих правил приводить до різного роду покарання. Схему класифікації засобів захисту інформації наведено на рис 1.1.

Рисунок 1.1 – Класифікації засобів захисту інформації

Дипломноий проєкт присвячено програмним засобам захисту інформації, тобто криптографічного перетворення вівдкритого тексту в незрозумілу форму. Розроблено програмне забезпеченя для шифрування і дешифрування даних з використанням алгоритму Плейфера.

1.2 Етапи розвитку криптографії

В людському суспільстві є потреба в секретному обміні листами та повідомленнями. Це викликало необхідність приховувати зміст письмових повідомлень від сторонніх осіб. Тому важливою є проблема шифрування текстів. У криптографії текст видимий, але зашифрований і не може бути прочитаний без розшифрування. Криптографія використовує перетворення одних символів в інші,

взяті з того або іншого алфавіту.

З ускладненням інформаційних взаємовідносин в суспільстві продовжують виникати нові завдання по захисту інформації. Багато завдань можна розв’язати в рамках криптографії, що спонукало розвитку нових підходів і методів. Історія криптографії виникла близько трьох тисяч років. Вона складається з наступних етапів:

- Примітивна криптографія;
- Формальна криптографія;
- Наукова криптографія;
- Комп'ютерна криптографія.

В примітивній криптографії використовуються будь-які методи приховування справжнього змісту інформації, зокрема кодування та стеганографії. Найпоширенішими криптографічними методами були заміни та перестановки. Шифри заміни замінюють кожну літеру відкритого тексту іншими символами, причому порядок розміщення символів не змінюється. Шифри перестановок змінюють лише порядок розташування літер у відкритому тексті.

Прикладом шифру підстановки є шифр Цезаря, шифром заміни – «магічний квадрат» грецького письменника Полібію.

Формальна криптографія пов’язана з появою формалізованих алгоритмів, які були стійкими для ручного криптоаналізу. В європейських країнах це сталося в період епохи Відродження, коли розвиток науки й торгівлі потребував надійних способів захисту інформації. На цьому етапі активно використовуються матричні шифри, перестановки з заданими одним або двома ключовими словами. Прикладом матричних шифрів є метод багатоалфавітної підстановки французького дипломата Блеза Віженера. Цей метод ґрунтується на використанні спеціальної таблиці таблиці Віженера.

До Першої світової війни широко застосовувався шифр Плейфера, що ґрунтувався на способі шифрування багатоалфавітною заміною.

15

Етап наукової криптографії

характеризується появою криптосистем, основою яких є математичні методи з високою криптостійкістю. Це пов’язано з тим, що в 30-х роках XX ст. сформувалися такі розділи математики, як теорія ймовірностей і математична статистика, загальна алгебра, теорія чисел, теорія алгоритмів, теорія інформації та кібернетика.

Теоретичні принципи криптографічного захисту інформації сформулював К. Шенноном в книзі «Теорія зв'язку в секретних системах». В ній обґрунтовано можливість створення абсолютно стійких криптосистем Матеріал був викладений в 1945 році у доповіді «Математична теорія криптографії». Цю доповідь розсекретили після закінчення Другої світової Війни.

Етап комп’ютерної криптографії характеризується появою потужних і компактних обчислювальних пристроїв, використання яких сприяло створення блокових шифрів. Був створений американський стандарт шифрування DES, призначений для апаратної реалізації. Алгоритм обробляв за один цикл лише половини тексту і працював з бітами, а не з байтами інформації, що сповільнювало його програмну реалізацію.

У 80-90-х роках минулого століття розробляються нові алгоритми в галузі криптографічного захисту інформації: квантова криптографія та ймовірнісне шифрування, які й сьогодні є актуальним в криптографічній галузі захисту інформації.

1.3 Процес шифрування і дешифрування повідомлень

Для захисту інформації при передачі по каналах зв’язку її перетворюють у незрозумілий текст. Відправник, посилаючи своє повідомлення, хоче бути переконаним, що його не зможе ніхто перехопити і прочитати. Для цього текст повідомлення необхідно зашифрувати. Одержувач повідомлення повинен розшифрувати одержаний текст.

Структурну схему шифрування і дешифрування даних наведено на рис. 1.2.

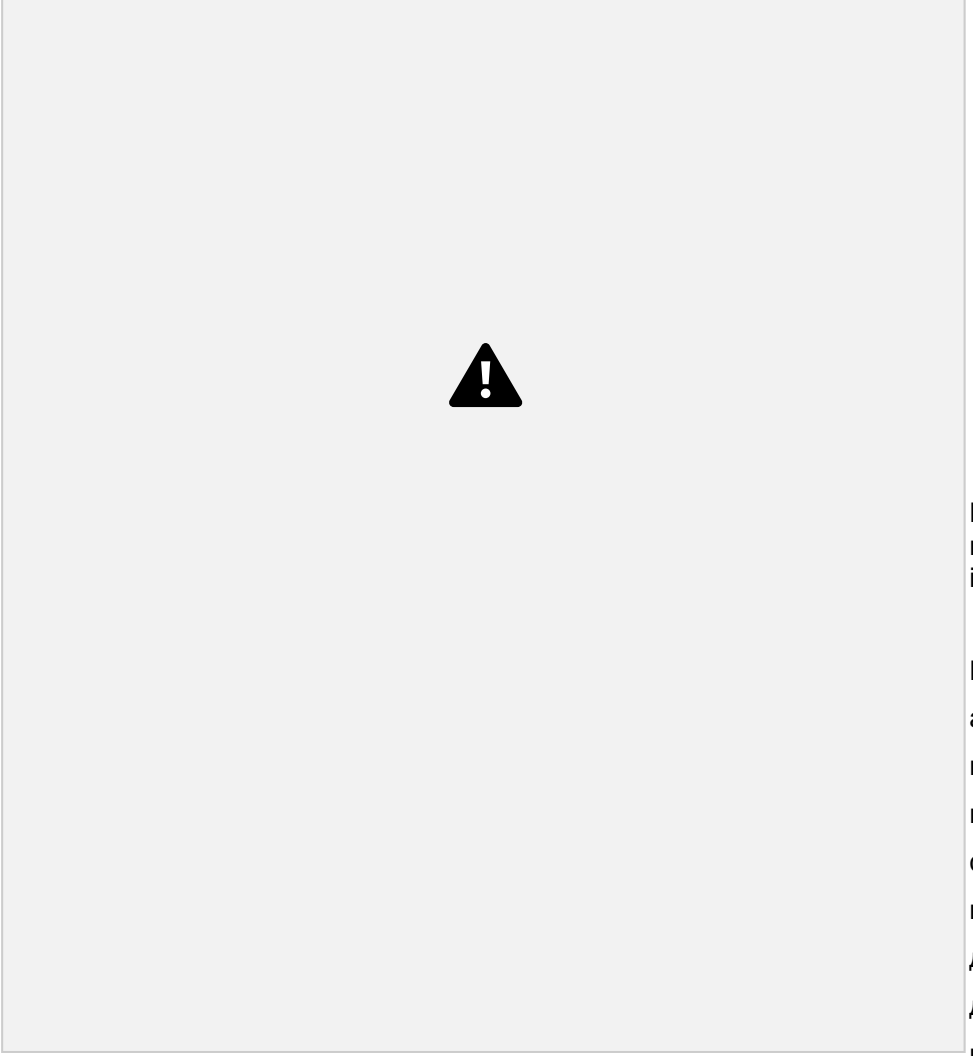


Рисунок 1.2 – Структурна схема шифрування і дешифрування інформації

Криптографічний алгоритм або шифр є математичною функцією, яка використовується для шифрування і дешифрування повідомлень.

Функції шифрування і дешифрування пов'язані між собою.

Якщо відкритий текст позначити через T, зашифроване повідомлення – через S, функцію шифрування початкового тексту – через C, функцію дешифрування шифротексту – через C_{-1}, то функція шифрування C, діючи на текст T, утворює шифротекст S. Математично цей процес можна записати формулою :

$$S=C(T). \quad (1.1)$$

При дешифруванні функція C_{-1} діє на шифротекст S, відновлюючи початковий текст T. Математично процес дешифрування виражається формулою:

$$T=C^{-1}(S). \quad (1.2)$$

Оскільки метою шифрування і дешифрування тексту є його початкове відновлення, то виконується рівність:

$$T=C^{-1}(C(T)). \quad (1.3)$$

Якщо шифрування супроводжується стисненням вхідного тексту, то послідовність S є меншою за послідовність T. Якщо шифрування супроводжується розширенням вхідного тексту, то послідовність S є більшою за послідовність T. Якщо шифрування не змінює розміру початкового тексту, то довжини послідовностей S і T є однаковими.

На передавальній стороні виконується шифрування відкритого повідомлення T за допомогою функції шифрування (1.1). В результаті отримуємо криптограму S, яка передається відкритим каналом зв'язку. На приймальній стороні до отриманого зашифрованого повідомлення S застосовується обернене перетворення (1.2). Одержано відкрите повідомлення T.

Розшифрування буде вірним, якщо повідомлення не було змінено при його передачі замовнику.

Процес шифрування інформації може забезпечити її конфіденційність при передачі. Він може бути використаний у самостійних механізмах безпеки або доповнювати існуючі.

1.4 Класифікація систем шифрування і дешифрування інформації

Для підвищення безпеки шифрування інформації використовуються ключі. В ролі ключа може бути будь-який об’єкт, що належить множині можливих ключів. Тоді процеси шифрування і дешифрування залежать від ключа. Якщо позначити функцію шифрування відкритого повідомлення T на ключі KS через $C_{KS}(T)$, то функція (1.1) матиме вигляд:

$$S=C_{KS}(T). \quad (1.4)$$

Процес дешифрування криптограми S за допомогою відомого ключа KD, можна записати за допомогою формули:

$$T=C^{-1KD(S)}. \quad (1.5)$$

На основі формул (1.4)-(1.5) одержуємо

формулу для одержання символів відкритого тексту:

$$T=C_{KD}^{-1}(C_{KS}(T)). \quad (1.6)$$

По способу використання ключа криптографічні методи діляться на:

- Симетричні з однаковими ключами шифрування і дешифрування, тобто $KS=KD=K$;
- Асиметричні з різними ключами шифрування і дешифрування, тобто $KS \neq KD$.

Симетричні алгоритми характеризуються можливістю швидкого шифрування великих потоків інформації. Вони забезпечують високу ступінь секретності. Симетричні алгоритми дають змогу використовувати одні і ті програмні засоби для шифрування і дешифрування інформації.

Схематично процес шифрування і дешифрування повідомлень з однаковими ключами показано на рис. 1.3.

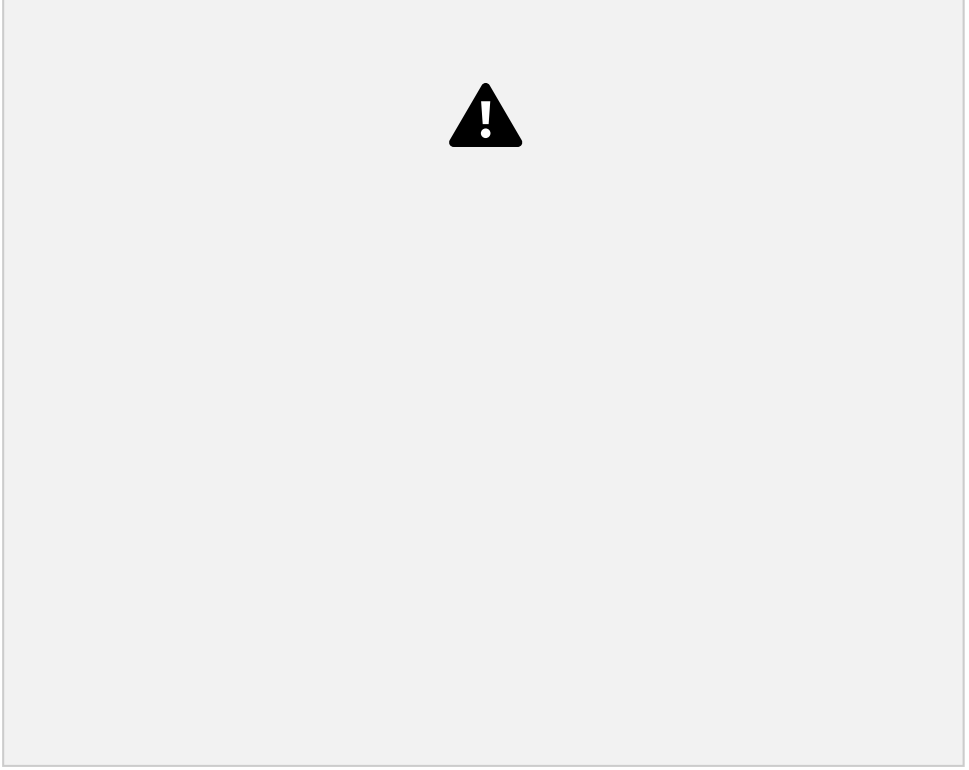


Рисунок 1.3

Симетричний метод шифрування і дешифрування інформації На передавальній стороні виконується шифрування відкритого повідомлення T за допомогою функції шифрування $C_{KS}(T)$ на ключі $KS=K$. В результаті отримуємо криптограму S, яка передається відкритим каналом зв'язку. На приймальній стороні до отриманого зашифрованого повідомлення S застосовується обернене перетворення $C_{-1KD}(S)$. Одержуємо відкрите повідомлення T при використанні того самого ключа $KD=K$, що і на передавальній стороні.

Проблемою використання симетричних алгоритмів є зберігання і передача ключа для розшифрування повідомлення, так як він є секретною частиною криптосистеми на приймальній стороні. Також потрібна велика кількість ключів для кожного одержувача секретного повідомлення.

Процес шифрування і дешифрування в асиметричних системах з двома різними ключами зображено на рис. 1.4.

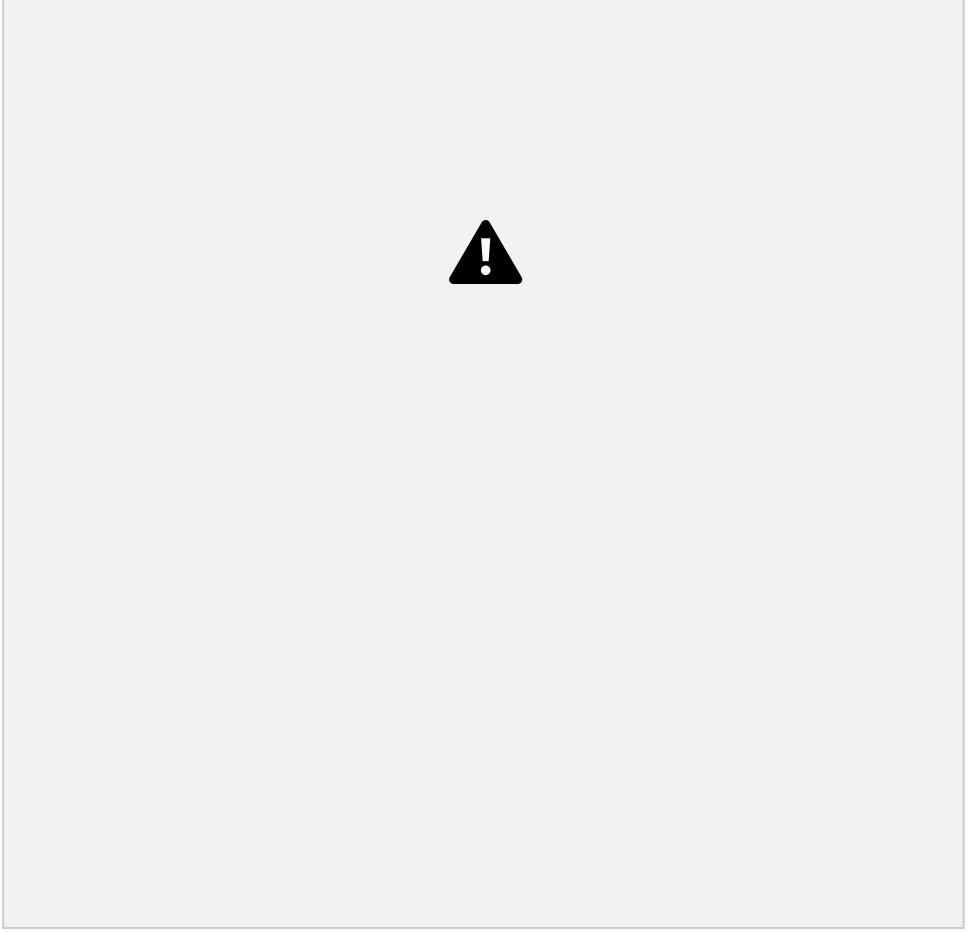
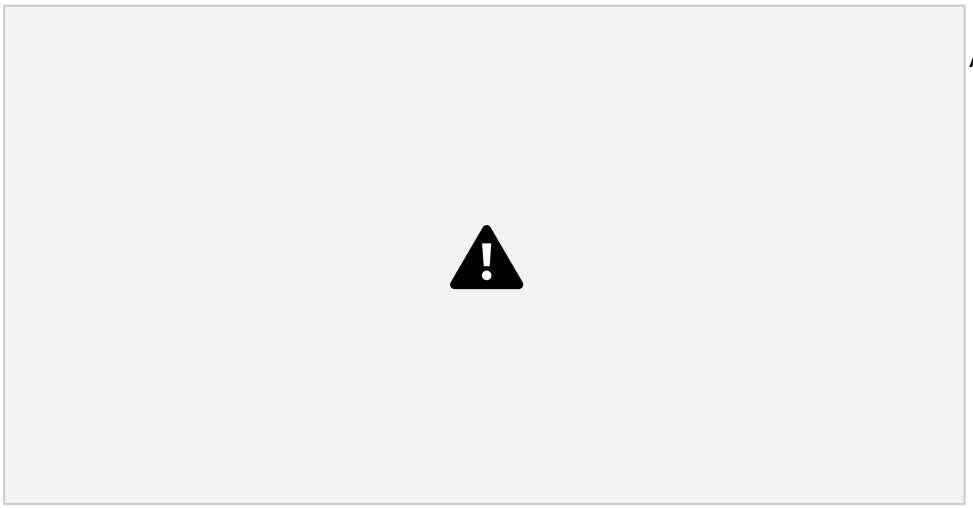


Рисунок 1.4

Асиметричний метод шифрування і дешифрування інформації В асиметричних системах використовуються різні ключі. Ключ для шифрування KS це відкритий ключ, який не є секретним. Цей ключ суттєво відрізняється від ключа дешифрування KD , який є секретним. Безпека асиметричних алгоритмів залежить від використаних ключів. Якщо ключ не відомий, то ніхто не зможе прочитати секретне повідомлення.

Асиметричні криптосистеми розв'язали основну проблему симетричних криптосистем, пов'язану з розповсюдженням ключів. Адже для шифрування інформації багатьма користувачами потрібно мати лише одну пару ключів: відкритий для шифрування і секретний для розшифрування.

Перевагою асиметричних методів є те, що для створення багатокористувацької системи обміну зашифрованою інформацією не потрібно великої кількості ключів. Недоліком асиметричних методів шифрування є мала швидкодія порівняно з симетричними, оскільки математичні перетворення є досить складними.



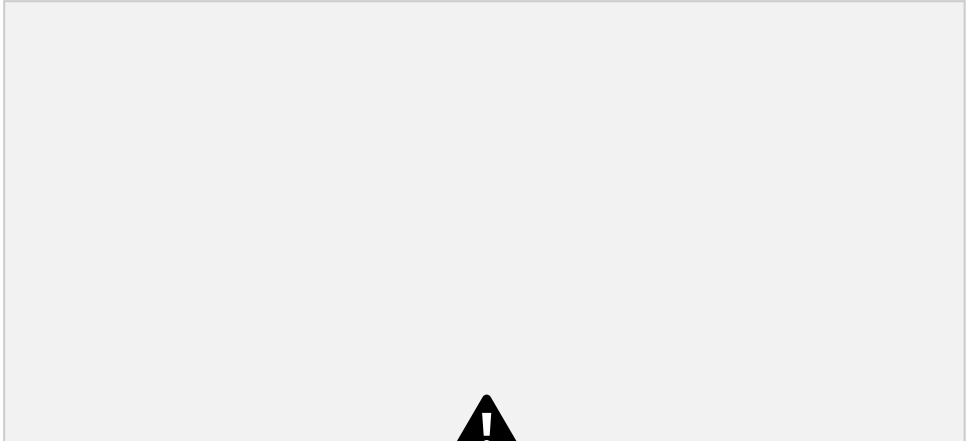
Але асиметричний метод шифрування можна використати там, де симетричні алгоритми працювати не будуть, наприклад, для створення електронного цифрового підпису.

Симетричні алгоритми завдяки високій швидкодії найкраще підходять для захисту комп'ютерної інформації. Асиметричні алгоритми внаслідок малої швидкодії недоцільно застосовувати для шифрування великих потоків інформації. Асиметричну систему можна використати для обміну інформацією малих об'ємів, тобто можна нею шифрувати ключі для симетричних систем.

Для успішної роботи учасники інформаційного секретного обміну повинні заздалегідь домовитися про алгоритм шифрування і розшифрування. Важливим фактором також є передача криптографічного ключа.

2 ВИКОРИСТАННЯ ШИФРУ ПЛЕЙФЕРА ДЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ

2.1 Поняття про шифрувальну таблицю Трісемуса



Історія шифрувальних таблиць Трісемуса дуже давня. Вона має початком

15-е століття. Абат з Німеччини Іоганн Трісемус у 1508 році опублікував роботу «Поліграфія» з криптології. У цій публікації він вперше висвітлив схему застосування шифрувальних таблиць, заповнених випадково буквами алфавіту [2].

Шифр Трісемуса відноситься до шифрів заміни. Для отримання такого шифру використовувалася таблиця для запису букв алфавіту і ключового слово або фрази. Якщо в ключовому слові або фразі були літери, що повторювалися, то вони записувалися тільки один раз. У таблицю спочатку вписувалося рядками

ключове слово. Далі ця таблиця доповнювалася буквами алфавіту, котрі були відсутні в ключовому слові. Буква алфавіту вписувалися в таблицю за порядком. Оскільки ключове слово або фразу можна було легко було запам'ятати, то тим самим спрощувався підхід до процесів шифрування та дешифрування.

Метод шифрування Трісемуса проілюстровано прикладом. В ролі ключа вибрано ключове слова «кібернетика», яке після відкидання однакових букв буде мати вигляд, показаний в табл. 2.1.

Таблиця 2.1 – Вигляд ключового слова після відкидання однакових букв

0	1	2	3	4	5	6	7	8	9	10
к	і	б	е	р	н	е	т	и	к	а

1	2	3	4	5	6	7	8	9
к	і	б	е	р	н	т	и	а

Ключове слово «кібернетика» після відкидання однакових букв матиме вигляд: «кібернтиа».

Використання шифрувальної таблиці Трісемуса розглянуто на прикладі українського алфавіту. Алфавіт має 32 букви, додано також символи: пропуск, крапка, кома, апостроф. Тому таблиця має 36 символів і розмір її буде 6 ×6 .

Звідси, при m=36 та ключовим словом «кібернтиа» отримано наступну таблицю підставляння. Процес заповнення цих таблиць підстановки з використанням ключового слова «кібернетика» проілюстровано на рис. 2.1.

а б в г д е к і б

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

Рисунок 2.1 УПроцес заповнення таблиць підстановки з використанням ключового слова «кібернетика»

Спочатку таблиці Трісемуса записуються літери ключа без повторюваних букв. Далі за порядком записуються букви алфавіту, що залишилися після вилучення літер ключа.

При шифруванні відкритого тексту в цій таблиці знаходимо черговий символ початкового тексту і записуємо в шифротекст символ, котрий розташований нижче за цей символ. Символи повинні бути в одному і тому ж самому стовпці. Якщо буква початкового тексту знаходиться в останньому рядку таблиці, то для зашифрованого тексту береться верхній символ з того ж стовпця.

Для зашифрування вхідного текст методом Трісемуса фрази «дипломний проєкт» складемо таблицю, кількість стовпців яких рівна кількості символів в початковому тексті. Для наведеного прикладу початковий текст містить 16 символів. В кожній клітинці таблиці пишемо символи початкового тексту. Під символами початкового тексту записуються символи шифротексту згідно таблиці

Трісемуса (рис. 2.1). Результати такого шифрування матимуть такий вигляд, наведений в табл. 2.2.

Таблиця 2.2 – Процес шифрування методом Трісемуса

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

24

д и п л о м н и й _ п р о є к т л ж ч ф ц х д ж у б ч г ц м т є

В результаті шифрування фрази «дипломний проєкт» одержимо наступний зашифрований текст:

лжчфцхджубчгцмтє

Такі табличні шифри називаються монограмними, так як шифрування здійснюється по одному символу. Але Трісемус першим зауважив, що подібні шифрувальні таблиці можна використати для шифрування одночасно двох символів. Такі шифри називаються біграмними. Метод біграмного шифрування вперше запропонував Плейфер.

2.2 Особливості біграмного шифру Плейфера

Біграмний шифр Плейфера вперше було розроблено в 1854 році. Він належить до найвідоміших біграмних шифрів заміни. Шифр передбачає шифрування пар символів (біграм) замість одиночних символів. Він відноситься до симетричного шифрування, в якому вперше використана заміна не одиночних символів, а біграм. Заміна біграм була винайдена Чарльзом Уїтстоном, але Лайон Плейфер запровадив цей шифр в державні служби Великобританії. Тому його названо іменем Лайона Плейфера. Цей шифр Великобританія застосовувала ще під час Першої світової війни.

В основі шифру Плейфера лежить шифрувальна таблиця, в якій випадково розташовані символи алфавіту, на котрому написані початкові тексти для шифрування. В загальному структура таблиці шифрувальної системи Плейфера аналогічна структурі шифрувальної таблиці Трісемуса. В шифрувальній системі Плейфера використовуються також ключові слова або фрази, символами яких заповнюються початкові клітини таблиці. Однакові літери ключових фраз вилучаються.

В залежності від використовуваного алфавіту, на якому написаний початковий текст, таблиця або матриця Плейфера має різну розмірність. Шифр Плейфера для латинського алфавіту використовує матрицю розміром 5x5, а для кириличного алфавіту – матрицю розміром 4x8. Кожна матриця містить ключове слово або фразу. При заповненні матриці використовуються такі

правила:

– Заповнення початкових елементів матриці літерами ключового слова без повторювані символів;

– Заповнення решту клітинок матриці літерами алфавіту, які відсутні в ключовому слові.

Ключове слово можна записувати, починаючи з верхнього рядка матриці, з лівого або з правого стовпців, а також по діагоналі з лівого верхнього кута до правого нижнього. Ключове слово, доповнене алфавітом без повторювані символів, становить матрицю 5x5 і є ключем шифру.

2.3 Опис процедури шифрування відкритих текстів

Оскільки система шифрування та дешифрування Плейфера використовує шифрувальну таблицю Трісемуса, то використаємо цю таблицю з ключовим словом «кібернетика» для опису шифрувальної процедури Плейфера.

Для шифрування відкритого тексту його необхідно розбити на біграми, тобто групи із двох символів. Якщо текст містить непарну кількість символів, то в кінці тексту додаємо пропуск. Біграми не повинні містити однакових літер. Якщо два символи біграми співпадають, то необхідно додати після першого символу інший символ, наприклад «*», або при подвоєнні символів один можна опустити, що не приведе до втрати змісту шифрованого повідомлення.

Потім ці біграми шукаємо в шифрувальній таблиці Плейфера. Два символи біграми відповідають кутам прямокутника в цій таблиці. Положення кутів в прямокутнику може бути різним відносно один до одного. Для зашифрування пари символів початкового тексту використовуються такі правила:

1. Якщо обидва символи біграми початкового тексту зустрічаються в одному рядку таблиці, то ці символи замінюються на символи, що розміщені в стовпці праворуч від них. Якщо символ є останнім у рядку, то для шифру береться відповідний символ з лівого (першого) стовпця цього ж рядка. Цю

схему шифрування показано на рис. 2.2.

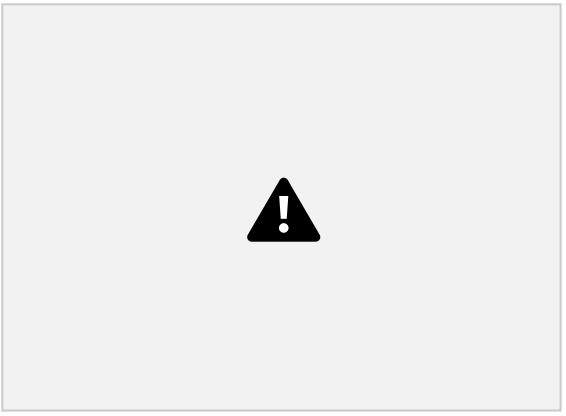


Рисунок 2.2 YСхема шифрування біграм, символи яких розміщені в одному рядку

Використовуючи шифрувальну таблицю на рис. 2.2, одержимо, що біграма «аг» дає біграму зашифрованого тексту «вд», а біграма «оф» дає біграму зашифрованого тексту «пм».

2. Якщо обидва символи біграми початкового тексту зустрічаються в одному стовпці таблиці, то вони зашифровуються символами того ж стовпця, які знаходяться під ними. Якщо при цьому символ початкового тексту є нижнім у стовпці, то він замінюється на символ з верхнього рядка цього ж стовпця. Схему шифрування біграм, символи яких розміщені в одному стовпці, показано на рис. 2.3.

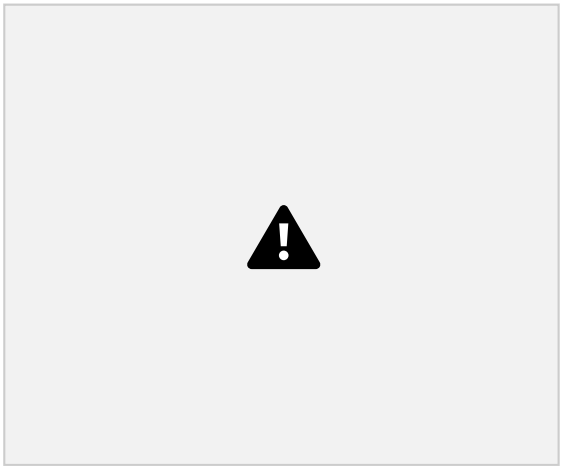


Рисунок 2.3 YCхема шифрування біграм, символи яких розміщені в одному стовпці

Використовуючи шифрувальну таблицю на рис. 2.3, одержимо, що біграма «вс» дає біграму зашифрованого тексту «їш», а біграма «мя» дає біграму зашифрованого тексту «хк».

3. Якщо обидва символи біграми початкового тексту розміщені у різних стовпцях і різних рядках, тоді вони знаходяться в кутах прямокутника, що визначається даною парою символів. Відповідно, ці символи замінюються на символи, що перебувають у тих же рядках, але відповідають іншим кутам прямокутника. Це означає, що послідовність символів біграми зашифрованого тексту є дзеркально розташованою по відношенню до послідовності символів біграми початкового тексту.

Схему шифрування біграм, символи яких розміщені в протилежних кутах прямокутника, показано на рис. 2.4.

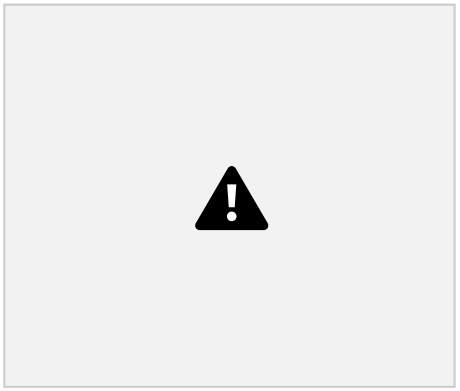


Рисунок 2.4 YCхема шифрування біграм, символи яких розміщені в протилежних кутах прямокутника

З рис. 2.4 одержимо, що пара символів «кс» відображається в біграму зашифрованого тексту «ем», а пара символів «рю» замінюється біграмою «нщ».

2.4 Опис процедури дешифрування шифротекстів

Для розшифрування зашифрованого тексту необхідно використати ці три правила в зворотному порядку, тобто застосувати обернену процедуру відображення біграм шифротексту в початковий текст.

Для дешифрування шифротексту методом Плейфера використовується та сама шифрувальна таблиця, що і для шифрування (рис. 2.1) з ключовим словом «кібернетика». Шифротекст необхідно розбити на біграми, із двох символів. Так як шифрований текст містив парну кількість символів, то і шифротекст має парну кількість символів. Згідно алгоритму шифрування Плейфера біграми шифротексту не містять однакових літер.

Далі ці біграми шукаємо в шифрувальній таблиці Плейфера (рис. 2.1). Два символи біграми завжди відповідають кутам прямокутника в цій таблиці. Розміщення кутів в прямокутнику може бути різним. Для розшифрування пари символів шифротексту використовуються наступні правила:

1. Якщо обидва символи біграми шифротексту розміщені в одному рядку шифрувальної таблиці Плейфера, то ці символи замінюються на символи, що розміщені в стовпці ліворуч від них. Якщо символ є першим у рядку, то для розшифрування береться відповідний символ з правого (останнього) стовпця цього ж рядка. .Дану схему розшифрування показано на рис. 2.5.

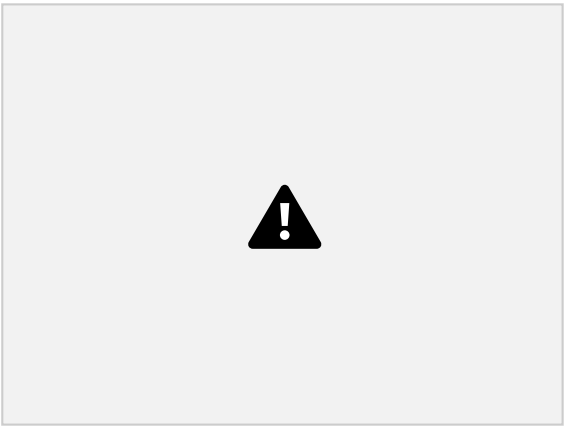


Рисунок 2.5 YСхема розшифрування біграм, розміщених в одному рядку

Використовуючи шифрувальну таблицю (рис. 2.2), одержимо, що біграма зашифрованого тексту «вд» дає біграму «аг» початкового тексту, а біграма зашифрованого тексту «пм» дає біграму «оф».

2. Якщо обидва символи біграми шифротексту зустрічаються в одному стовпці таблиці, то вони розшифровуються символами того ж стовпця, які знаходяться над ними. Якщо символ шифротексту є верхнім у стовпці, то він замінюється на символ з нижнього рядка цього ж стовпця.

Використовуючи шифрувальну таблицю на рис. 2.3, одержимо, що біграма зашифрованого тексту «їш» дає біграму початкового тексту «вс». Біграма зашифрованого тексту «хк» дає біграму відкритого тексту «мя».

Схему розшифрування біграм, символи яких розміщені в одному стовпці, показано на рис. 2.6.

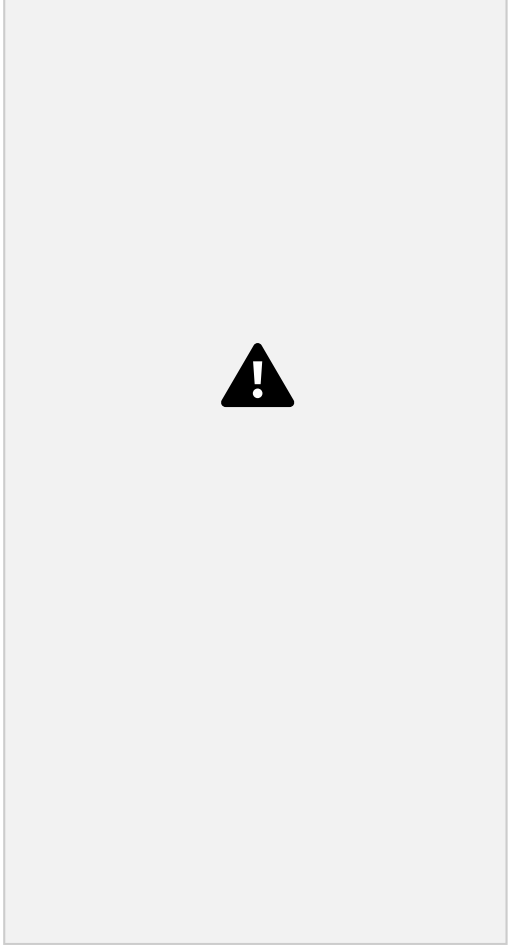


Рисунок 2.6 YCхема розшифрування біграм, розміщених в одному стовпці

3. Якщо обидва символи біграми шифротексту розміщені у різних стовпцях і різних рядках, тоді вони знаходяться в кутах прямокутника, що визначається даною парою символів. Відповідно, ці символи замінюються на символи, що перебувають у тих же рядках, але відповідають іншим кутам прямокутника. Схему розшифрування біграм, символи яких розміщені в протилежних кутах прямокутника, показано на рис. 2.7.

Рисунок 2.7 YCхема розшифрування біграм, символи яких розміщені в протилежних кутах прямокутника

З рис. 2.7 одержимо, що пара символів «ем» відображається в біграму «кс», а пара символів «нщ» зашифрованого тексту замінюється біграмою «рю».

2.5 Криптоаналіз шифру Плейфера

Якість методів шифрування визначається криптостійкістю використовуваних шифрів. Криптостійкість шифру характеризує його стійкість до дешифрування. Ця характеристика визначається періодом часу, що необхідний для розшифрування шифротексту.

Шифр Плейфера набагато стійкіший до криптоаналізу порівняно з шифрами простої заміни. Тому шифрування біграмами підвищує стійкість шифру Плейфера до злому. Частотний аналіз може бути проведений для 1024 можливих комбінацій біграм (32×32=1024). Аналіз частоти біграм є можливим, але він вимагає великого об'єму зашифрованого тексту.

Але якщо відомі зашифрований і початковий тексти і є достатній об'єм тексту, то шифр Плейфера може бути розкритий. Складною проблемою є одержання ключа. Якщо відомий тільки зашифрований текст, то криптоаналітики повинні аналізувати відповідність між частотою появи біграм у шифрованому тексті та відомій частоті появи біграм у мові, на якій написане повідомлення.

Існує інший підхід до криптоанализу шифру Плейфера, який називається en:Random-restart hill climbing. Він ґрунтується на матриці випадкових символів. За допомогою найпростіших ітерацій матриця випадкових символів максимально наближається до оригінальної матриці. цей метод занадто складний для людини, але комп'ютери за допомогою даного алгоритму можуть зламати даний шифр, навіть маючи невеликий об'єм тексту. Ніколи не зустрічаються біграми з повторюваними символами (наприклад ЇЇ). Якщо в шифрованому тексті відсутні біграми з повторюваними символами і його довжина досить велика, то можна припустити, що вихідний текст зашифрований шифром Плейфера.

3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ДАНИХ ЗА ДОПОМОГОЮ ШИФРУ ПЛЕЙФЕРА

3.1 Алгоритм для шифрування текстів на основі шифру Плейфера

В дипломному проекті розроблено алгоритм і програмне забезпечення для шифрування і дешифрування відкритих текстів за допомогою шифру Плейфера. Особливістю цього шифру є використання однакових ключів для шифрування і дешифрування текстів.

Процес шифрування відкритих

текстів складається з наступних кроків:

- Формування шифрувальної таблиці Плейфера з використанням ключової послідовності;
- Розбиття відкритого тексту на біграми (пари символів);
- Перетворення біграм тексту у шифробіграми з використанням сформованої шифрувальної таблиці Плейфера на основі заданого ключа;
- Передача шифротексту замовнику.

Алгоритм розробки криптографічної системи, яка використовує шифр Плейфера, виконує наступні функції:

- Запис у файл TABL_PLEJ.txt послідовності літер ключового слова або фрази без їх повторення та доповнення її літерами українського алфавіту за порядком, котрі відсутні в ключовому слові;
- Запис відкритого тексту в файл file_input.txt;
- Формування з символів файлу TABL_PLEJ.txt шифрувальної таблиці Плейфера розміром 6×6 з додаванням символів: риски підкреслювання, коми, крапки і апострофа та запис її у файл TABL_PLEJ_w.txt;
- Читання пари символів (біграм) відкритого тексту з файлу file_input.txt;
- Перетворення прочитаних символів в шифробіграми згідно шифрувальної таблиці Плейфера і їх запис у файл file_text.txt/

Схематично процес шифрування відкритих текстів шифром Плейфера показано на рис. 3.1.

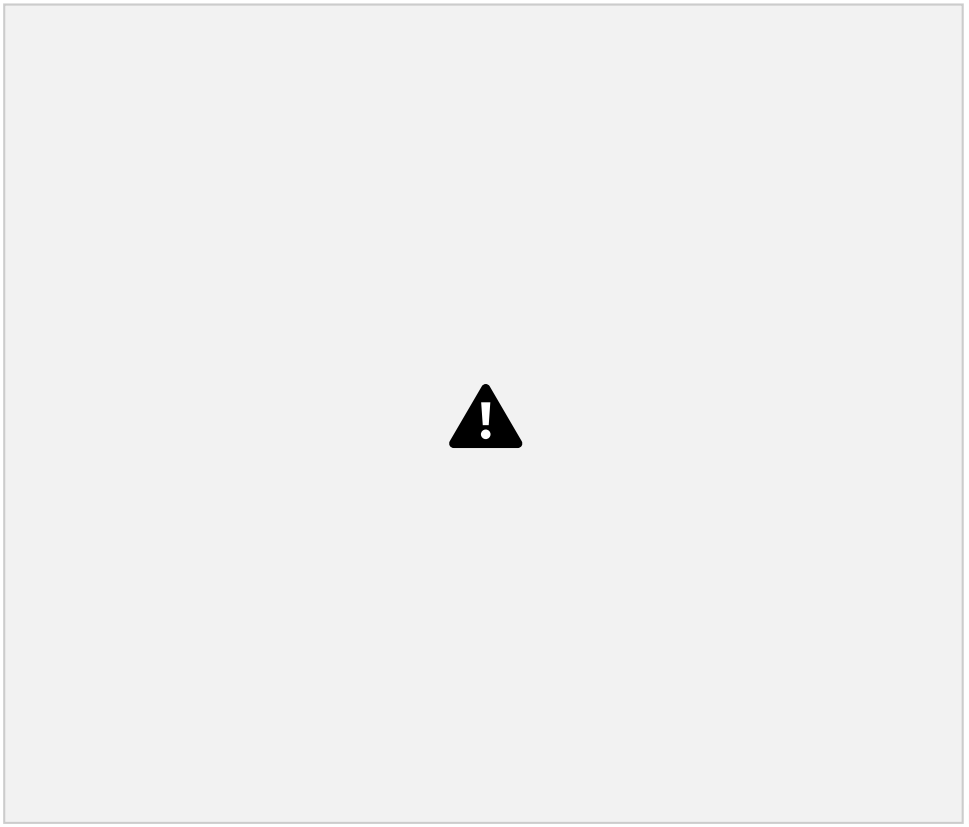


Рисунок 3.1 – Схема шифрування відкритих текстів шифром Плейфера

При шифруванні пари символів відкритого тексту замінюються парами символів того ж алфавіту, яким написано текст. Шифрування здійснюється шляхом заміни біграм відкритого тексту на біграми шифротексту на основі шифрувальної таблиці Плейфера за правилами, описаними в параграфі 2.3.

На рис. 3.2 наведено структурну схему алгоритму шифрування відкритих текстів на основі шифру Плейфера.

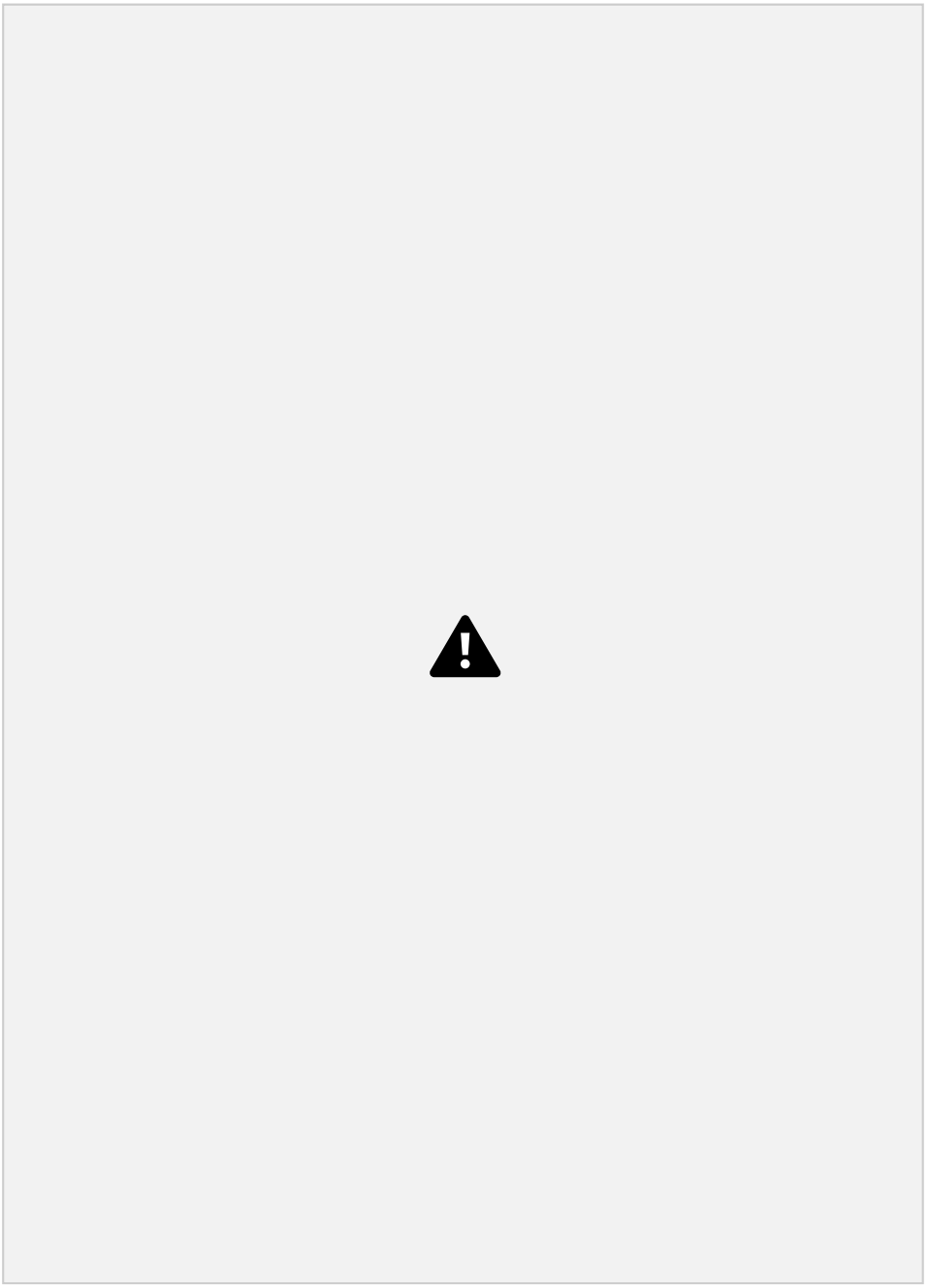


Рисунок 3.2 – Схема алгоритму шифрування текстів на основі шифру Плейфера

Шифрувальна таблиця Плейфера складається з 32-х букв українського алфавіту. Використовуються також символи: пропуск, крапка, кома, апостроф. Відповідно таблиця має 36 символів, її розмір буде 6 ×6 . В ролі ключа використано ключове слово «кібернетика». Після виключення повторюваних літер ключ матиме вигляд «кібернтиа». Літери, присутні в ключі, виключені з алфавіту при заповненні таблиці. В результаті отримано шифрувальну таблицю, наведено на рис. 2.1. Вигляд шифрувальної таблиці залежить від ключової послідовності. Тому при зміні ключа міняється розміщення символів у таблиці, що робить шифр Плейфера стійкішим до криптоаналізу.

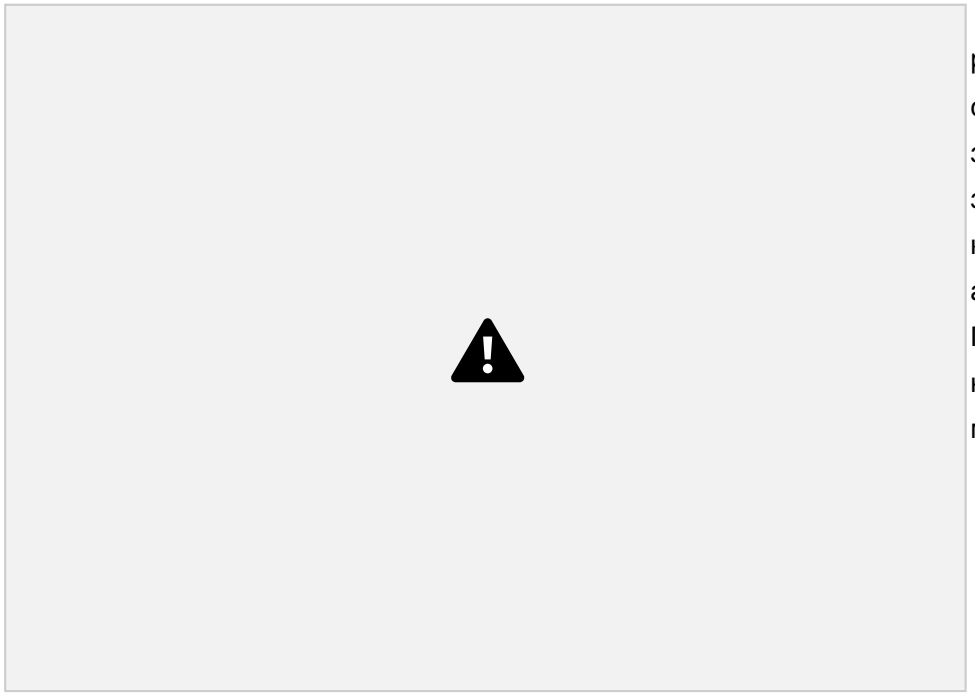
Після читання пари символів відкритого тексту шукаємо їх індекси в шифрувальній таблиці (рис. 2.1). Індекси першого символу біграми – (m1; n1), індекси другого символу біграми – (m2; n2). В залежності від розміщення елементів біграми визначаються індекси зашифрованих символів біграми згідно правил, описаних в параграфі 2.3. Індекси першого символу шифробіграми – (sm1; sn1), індекси другого символу біграми – (sm2; sn2). Кожний символ біграми початкового тексту шифрується і записується у файл file_text.txt, який призначений для зберігання шифротексту.

Розробка алгоритму ґрунтується на принципі розділення його на окремі функціональні компоненти. В процесі роботи програми ці компоненти взаємодіють між собою. Таким підхід використовується для розробки багатофункціонального програмного забезпечення і дозволяє структурувати

3.2 Опис програмного коду для шифрування текстів

На основі описаного алгоритму розроблено програмне забезпечення для шифрування відкритих текстів на основі шифру Плейфера. При шифруванні бліаграми відкритого тексту перетворюються в біграми шифротексту. Шифрування здійснюється за допомогою шифрувальної таблиці Плейфера,

36



розміщення символів якої залежить від заданого ключа (слова або фрази). Програму написано на мові програмування С. Головною особливістю мови є компактність тексту програмного коду, порівняно з іншими мовами програмування та мінімізація часу розробки. Мінімізація часу розробки великих за обсягом програм є однією з актуальних проблем, з якою стикаються фахівці при шифровані і розшифрування текстів. Програма має функціональну структуру , що полегшує процес її розробки. В процесі роботи окремі компоненти програми виконують конкретні функції і взаємодіють між собою.

Перетворення відкритого тексту в криптограму і запис криптограми в файл здійснюється програмним модулем Zaxuct_PLAYJFER_Project.c. Відкритий текст для шифрування розміщений в текстовому файлі file_input.txt в символьному форматі. Шифрувальна таблиця сформована на основі ключового слова «кібернетика» та українського алфавіту записана в файлі TABL_PLEJ_w.txt.

Програма Zaxuct_PLAYJFER_Project.c для шифрування текстів на основі шифру Плейфера складається з наступних елементів:

1 Підключення бібліотечних файлів, які містять прототипи стандартних функцій файлового вводу-виводу, функцій обробки символьної інформації та функцій роботи операційної системи:

2 Опис і задання функції для формування масиву букв алфавіту, якими задається і шифрується текст:.

```
void kkk (char unsigned x);
```

Аргумент x – це поточний символ, який опрацьовується.

3 Опис потоків вводу-виводу на структурний тип FILE для асоціації фізичних файлів на диску:

```
FILE *STP, *TP;
FILE *fp1,*fp2;
```

Потік STP зв'язаний з файлом TABL_PLEJ.txt, призначеним для зберігання ключової послідовності і символів алфавіту. Потік TP асоціюється з файлом TABL_PLEJ_w.txt, що містить шифрувальну таблицю. Потік fp1 зв'язаний з

файлом file_input.txt, призначеного для зберігання відкритого тексту. Потік fp2 зв'язаний з файлом file_text.txt, що містить шифротекст, в який перетворено початковий текст.

4 Опис констант, змінних і масивів, задання. початкових значень.

5 Відкриття використовуваних файлів для читання та запису. Для кожного файлу виводяться повідомлення про відкриття або про неможливість його відкрити. В цьому випадку програма закінчує роботу, так як неможливий процес читання чи запису даних у файл.

6 Читання з файлу TABL_PLEJ.txt ключової послідовності і символів алфавіту, формування шифрувальної таблиці і запис її у файл TABL_PLEJ_w.txt. 7 Читання з файлу file_input.txt біграм відкритого тексту, які необхідно зашифрувати, і перевірка кінця файлу.

8 Шифрування прочитаних біграм шляхом обчислення індексів шифрованих символів на основі таблиці Плейфера в залежності від індексів

початкових символів. При цьому розглядаються варіанти, наведені в табл. 3.1.

Таблиця 3.1 YВаріанти розміщення символів біграми в таблиці Плейфера

Індекси символів початкової ; n2)		Індекси символів шифробіграми (sm1; sn1) і (sm2; sn2)	
Додаткова умова	1-й символ	2-й символ	
1 m1= m2 n1<5 & n2<5	2 m1= m2 n1<5 & n2=5	sm1=m1 sn1=n1+1	
	3 m1= m2 n1=5 & n2<5	sm1=m1 sn1=0	
	4 n1=n2 m1<5 & m2<5	sm1=m1+1 sn1=n1	
	5 n1=n2 m1<5 & m2=5	sm1=m1+1 sn1=n1	
	6 n1=n2 m1=5 & m2<5	sm1=m1 sn1=n1	sm2=m2 sn2=n2+1
		sm2=m2 sn2=n2+1	sm2=m2+1 sn2=n2
		sm2=m2 sn2=0	sm2=0
		sm2=m2+1 sn2=n2	
7 m1 ≠ m2 n1 ≠ n2		sm1=m1 sn1=n2	sm2=m2 sn2=n1

9 Запис зашифрованих біграм в файл file_text.txt.

10 Закриття файлів TABL_PLEJ.txt, TABL_PLEJ_w.txt, file_input.txt і file_text.txt після закінчення роботи програми.

Результатом роботи програми Zaxuct_PLAYJFER_Project.c є створення файлу file_text.txt, в якому знаходиться зашифрований текст. Повний текст програми на мові С для шифрування відкритих текстів на основі шифру Плейфера наведено в додатку А.

3.3 Результати роботи програми шифрування текстів

Програма Zaxuct_PLAYJFER_Project.c формує числові коди шифрувальної таблиці Плейфера на основі заданої послідовності символів ключа

щена в файлі TABL_PLEJ.txt,

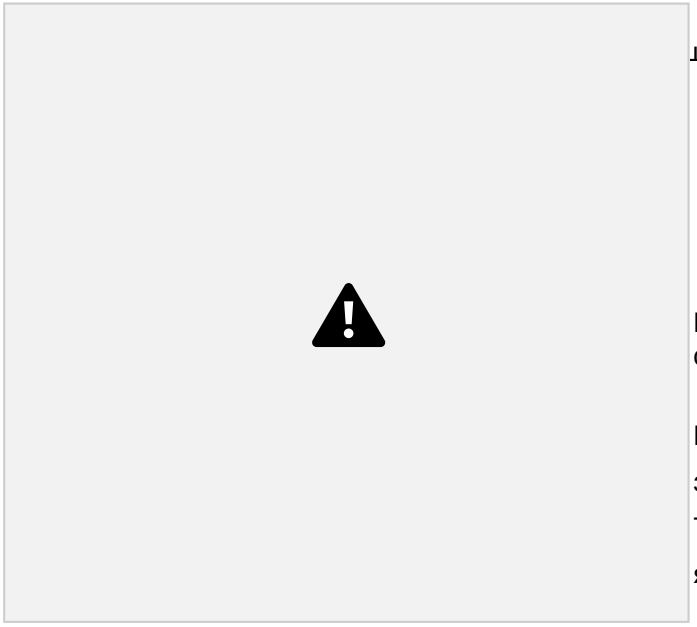


Рисунок 3.3 – Послідовність символів для формування таблиці Плейфера

Коди шифрувальної таблиці записуються в файл TABL_PLEJ_w.txt. вмістиме якого наведено на рис. 3.4.

Рисунок 3.4 – Відкритий текст для шифрування на основі шифру Плейфера

Вхідними даними для програми Zaxuct_PLAYJFER_Project.c є відкритий текст для шифрування (файлі file_input.txt). Текст наведено на рис. 3.5.

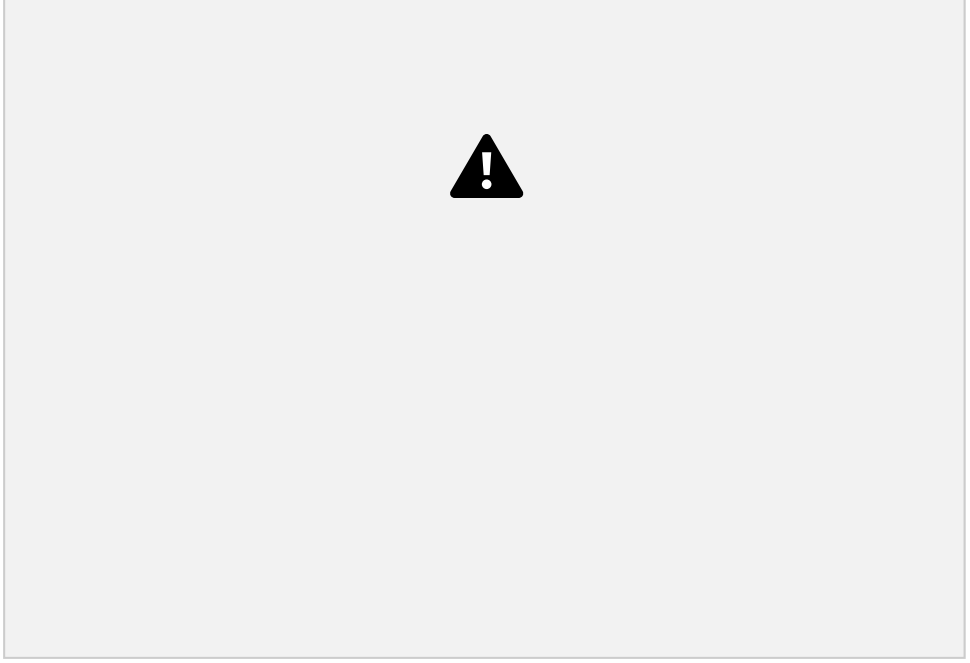


Рисунок 3.5 – Відкритий текст для шифрування на основі шифру Плейфера

Результатом роботи програми є шифротекст, який записується у файл file_text.txt. На рис. 3.6 наведено шифротекст зашифрованого відкритого тексту.

Рисунок 3.6 – Шифротекст перетвореного відкритого тексту

3.4 Опис алгоритму дешифрування

шифротексту методом Плейфера

Оскільки алгоритм шифрування Плейфера є симетричний, то використовується той же ключ, що і для шифрування текстів, тобто слово «кібернетика». Тому розшифрування шифротекстів проводиться на основі таблиці Плейфера (рис. 2.2) і переліку правил, описаних в п. 2.4.

Така структура шифрування має ряд переваг:

- Основні положення алгоритмів шифрування і дешифрування текстів збігаються;
- Для дешифрування шифротекстів можна використати ряд програмних модулів, що були використані для шифрування.

Алгоритм дешифрування повідомлень, зашифрованих за допомогою шифру Плейфера з використанням ключа, складається з таких кроків:

- Запис у файл TABL_PLEJ.txt послідовності літер ключового слова або фрази без їх повторення та доповнення її літерами українського алфавіту за порядком, котрі відсутні в ключовому слові. Ключове слово отримувачу повідомлення відоме, як елюя до розшифрування одержаного шифротексту.
- Запис одержаного шифротексту в файл file_tex.txt;
- Формування з символів файлу TABL_PLEJ.txt шифрувальної таблиці Плейфера розміром 6×6 з додаванням символів: риски підкреслювання, коми, крапки і апострофа та запис її у файл TABL_PLEJ_w.txt;
- Читання пари символів (біграм) шифротексту з файлу file_tex.txt;;
- Перетворення прочитаних символів в біграми відкритого тексту згідно шифрувальної таблиці Плейфера і їх запис у файл file_output.txt; На рис. 3.7 показано схему розшифрування криптограми на приймальній стороні з використанням ключа. Результатом розшифрування є одержання відкритого тексту.

Рисунок 3.7 – Схема розшифрування шифротекстів на основі алгоритму Плейфера

При розшифруванні пари символів шифротексту замінюються парами символів того ж алфавіту відкритого тексту. Дешифрування проводиться шляхом заміни біграм зашифрованого тексту на біграми відкритого тексту на основі шифрувальної таблиці Плейфера за правилами, описаними в параграфі 2.4.

3.5 Опис програмного коду для розшифрування шифротекстів

Програмний код написано на мові С. Мову вибрано тому, що вона порівняно з іншими мовами програмування характеризується мінімальним часом розробки. А мінімізація часу розробки програм є важливою проблемою, з якою стикаються фахівці при шифровані і розшифрування повідомлень.

В результаті виконання операції дешифрування кожний символ шифротексту замінюється символом початкового тексту.

Програма Zaxuct_PLAYFER_DEKOD_Project.c для розшифрування шифротекстів, зашифрованих шифром Плейфера, складається з наступних кроків: 1 Підключення бібліотечних файлів, які містять прототипи стандартних функцій файлового вводу-виводу, функцій обробки символьної інформації та функцій роботи операційної системи:

2 Опис і задання функції для формування масиву букв алфавіту, якими задається і розшифровується текст:.

```
void kkk (char unsigned x);
```

3 Опис потоків вводу-виводу на структурний тип FILE для асоціації фізичних файлів на диску:

```
FILE *STP, *TP;
FILE *fp1,*fp2;
```

Потік STP зв’язаний з файлом TABL_PLEJ.txt, призначеним для зберігання ключової послідовності і символів алфавіту. Потік TP асоціюється з файлом TABL_PLEJ_w.txt, що містить шифрувальну таблицю. Потік fp1 зв’язаний з файлом file_txt.txt, в якому зберігається зашифрований текст. Потік fp2 зв’язаний з файлом file_output.txt, що містить розшифрований текст.

4 Відкриття файлів для читання та запису, вивід повідомлення про відкриття або про не відкриття файлів. При не відкритих файлах програма припиняє роботу, так як неможливий процес читання чи запису даних у файл.

5 Читання з файлу TABL_PLEJ.txt ключової послідовності і символів алфавіту, формування шифрувальної таблиці і запис її у файл TABL_PLEJ_w.txt. 6 Читання з файлу file_txt.txt біграм шифротексту для розшифрування та перевірка кінця файлу.

7 Розшифрування прочитаних біграм шляхом обчислення індексів розшифрованих символів на основі таблиці Плейфера в залежності від індексів шифрованих символів. Розшифрування проводиться з використанням варіантів, наведених в табл. 3.2.

Таблиця 3.2 YВаріанти розміщення символів шифробіграми в таблиці Плейфера

Індекси символів початкової	Додаткова умова	Індекси символів шифробіграми (sm1; sn1) і (sm2; sn2)	
		1-й символ	2-й символ
m1= m2 n1>0 & n2>0	1 m1= m2 n1>0 & n2=0	sm1=m1 sn1=n1-1	
	2 m1= m2 n1=0 & n2>0	sm1=m1 sn1=5	
	3 n1=n2 m1>0 & m2>0	sm1=m1-1 sn1=n1	
	4 n1=n2 m1>0 & m2=0	sm1=m1-1 sn1=n1	
	5 n1=n2 m1=0 & m2>0	sm1=5 sn1=n1	
	6 m1≠ m2 n1=n2	sm2=m2 sn2=n2-1	sm2=m2 sn2=5
	7 m1 ≠ m2 n1 ≠ n2	sm1=m1 sn1=n2	sm2=m2 sn2=n1
	8 m1≠ m2 n1=n2	sm2=m2 sn2=n2-1	sm2=m2-1 sn2=n2
	9 m1≠ m2 n1=n2	sm1=m1 sn1=n1-1	sm2=m2-1 sn2=n2

8 Запис розшифрованих біграм в файл file_output.txt.

9 Закриття файлів TABL_PLEJ.txt, TABL_PLEJ_w.txt, file_text.txt і file_output.txt після закінчення роботи програми.

Результатом роботи програми Zaxuct_PLAYFER_DEKOD_Project.c є формування файлу file_output.txt, в який записується відкритий текст. Повний текст програми на мові С для розшифрування шифротекстів, зашифрованих шифром Плейфера, наведено в додатку Б.

3.6 Результати роботи програми дешифрування шифротекстів

Програма Zaxuct_PLAYFER_DEKOD_Project.c формує числові коди шифрувальної таблиці Плейфера на основі заданого алфавіту і ключа (слово «кібернетика»). Коди шифрувальної таблиці наведено на рис. 3.4.

Вхідними даними для програми Zaxuct_PLAYFER_DEKOD_Project.c є зашифрований текст для розшифрування (файлі file_text.txt), текст якого наведено на рис. 3.6.

Результатом роботи програми є розшифрований текст, який записується у файл file_output.txt. На рис. 3.8 наведено початковий текст.

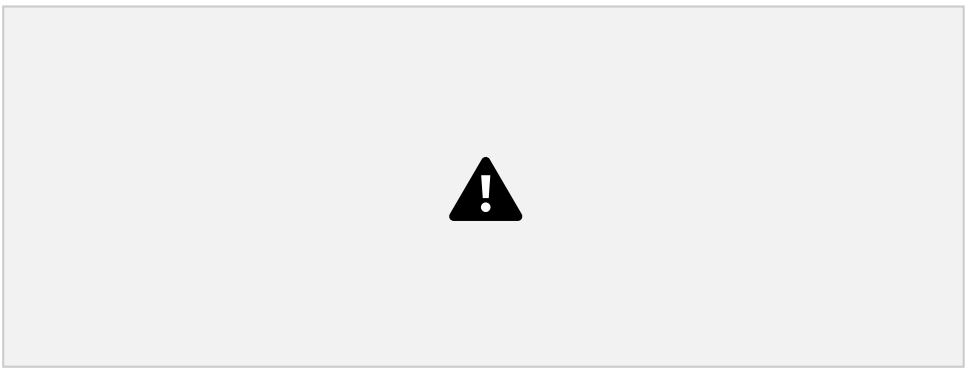


Рисунок 3.8 – Початковий текст розшифрованого шифротексту

Аналіз одержаних результатів показує, що після проведеної операції шифрування відкритого тексту, наведеного на рис. 3.5, та операції розшифрування зашифрованого тексту, одержано початковий текст, представлений на рис. 3.8.

Схожість

Схожість Цитати Посилання Вилучений

текст Підміна символів Коментарі

Назва документа: Яремко_Назар_ОК_41 **ID файлу:** 1014968858

Схожість

1 **Студентська робота** ID файлу: **1000097208** Навчальний заклад: **Lviv Polytechnic National University** 1.6%

63 Джерело

2 **Студентська робота** ID файлу: **1000042772** Навчальний заклад: **Lviv Polytechnic National University** 0.42%

30 Джерело

3 **Студентська робота** ID файлу: **1000083956** Навчальний заклад: **Lviv Polytechnic National University** 0.33%

4 Джерело

4 **Студентська робота** ID файлу: **1014265719** Навчальний заклад: **National University Ostroh Academy** 0.22% 5 **Студентська робота**

ID файлу: **1009545755** Навчальний заклад: **Uzhhorod National University** 0.2%

6 Джерело

6 **Студентська робота** ID файлу: **2078908** Навчальний заклад: **National University of Water Management and N...** 0.2% 7

Студентська робота ID файлу: **1006761187** Навчальний заклад: **National Aviation University** 0.2%

2 Джерело

8 **Студентська робота** ID файлу: **1010110939** Навчальний заклад: **Ternopil Volodymyr Hnatiuk National Pedagog...** 0.15%

16 Джерело

9 **Студентська робота** ID файлу: **3561920** Навчальний заклад: **National University of Water Management and N...** 0.13%

5 Джерело