ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД УКООПСПІЛКИ
«ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ»
ІНСТИТУТ ЕКОНОМІКИ, УПРАВЛІННЯ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ФАКУЛЬТЕТ ЕКОНОМІКИ І МЕНЕДЖМЕНТУ
ФОРМА НАВЧАННЯ ДЕННА
КАФЕДРА МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ТА СОЦІАЛЬНОЇ ІНФОРМАТИКИ

Допускається до захисту
Завідувач кафедри _____О.О. Ємець
(підпис)
«_____»_____2020 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА ДО БАКАЛАВРСЬКОЇ РОБОТИ

на тему

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ТЕМИ «КОДУВАННЯ ТЕКСТІВ ШИФРОМ PLAY FAIR»"

зі спеціальності 122 «Комп'ютерні науки»

Виконавець роботи Колінько Євгеній Андрійович
_____«_ _»__2020 р.
(підпис)
Науковий керівник проф., к.ф. – м.н. Є. М. Ємець
_____«_ _»__2020 р.
(підпис)

ПОЛТАВА 2020 р.

ВСТУП

Актуальність. Проблема захисту інформації шляхом перетворення, яке виключає можливість її зчитування сторонньою особою, хвилювала людський розум з давніх часів. Питаннями захисту інформації шляхом її перетворювання займається ***криптологія*** (kryptos – таємний, logos – наука). Криптологія поділяється на два напрямки – криптографію й криптоаналіз. Цілі цих напрямків є прямо протилежні. Взаємини криптографії й криптоаналізу є очевидні: криптографія – захист, тобто розробляння шифрів, а криптоаналіз – напад, тобто атака на шифри. Однак вони щільно пов'язані, й не буває кваліфікованих криптографів, котрі не володіли б методами криптоаналізу.

Криптографія – одноліток історії людської мови. Більш того, спочатку писемність власне сама була криптографічною системою, тому що в стародавніх суспільствах нею володіли лише обрані. В той час як у сучасному світі писемність доступна кожному, саме і тому розвиваються нові методи шифрування інформації які і вивчає наука криптологія [1, с. 6].

В наш час особливо гостро постає проблема забезпечення інформаційної безпеки в зв’язку із стрімким впровадженням комп’ютерної техніки в такі сфери, як біржова та банківська справа, страхування, медицина тощо. Необхідність вирішення проблем захисту інформації також зумовлена різким зростанням комп’ютерної злочинності, результат діяльності якої призводить до значних матеріальних втрат, незалежно від того чи це вірусна атака, чи шахрайство в електронній комерції. Все це і обумовлює актуальність обраної теми.

Об’єктом дипломної роботи є дослідження методів шифрування відомих під назвою Play Fair.

Предметом дипломної роботи є розробка програмного продукту основні задачі якого будуть шифрування та розшифровування вхідного тексту.

Метою дипломної роботи є розробка програмного продукту для шифрування та дешифрування тексту на основі аналізу шифру Плейфера.

Для досягнення мети, необхідно виконати ряд завдань:

– на основі порівняльного аналізу описати функціональність та структуру програмного продукту;

– описати проектні рішення, інструменти створення, використані технології та підходи до розробки;

– розробити програмний продукт для криптографії.

Методи дослідження. У процесі виконання дипломної роботи були використані такі методи, як: теоретичні – порівняльний аналіз провідних теорій з використання різноманітних криптографічних методів та використання мови програмування C++; системний аналіз – для деталізації і розчленування об’єкта дослідження на окремі важливіші складові елементи; аналіз і синтез – для визначення особливостей процесу візуального оформлення та функціонального наповнення програмного продукту.

Практичне значення роботи – розробка додатку наочного вивчення методу шифрування Плейфера.

Структура роботи. Дипломна робота складається зі вступу, семи розділів, висновків, списку використаних джерел та додатків. Містить 52 сторінки, 20 рисунків, список літератури з 9 найменування, 1 додаток.

1. Основні поняття та задачі інформаційної безпеки

1.1. Поняття інформаційної безпеки

Саме тому забезпечення інформаційної безпеки є досить складною задачею, але перш ніж говорити про інформаційну безпеку необхідно визначитися з поняттям “інформація”. Це поняття сьогодні вживається дуже широко і різнобічно. Важко знайти таку галузь знань, де б воно не використовувалося. Повсякденно під час здійснення різних видів діяльності користуються таким поняттям: інформація – нові дані про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього представлення.

У галузі інформаційних систем рекомендується таке означення інформації.

Інформація – це відомості, які є об’єктом зберігання, передавання і оброблення.

Відомо, що інформація може мати різну форму, зокрема, дані в комп’ютерах, листи, пам'ятні записи, досьє, формули, креслення, діаграми, моделі продукції, дисертації, судові документи й ін.

Як і всякий продукт, інформація має споживачів, що потребують її, і тому володіє певними споживчими якостями, а також має і своїх власників або виробників.

Відповідно до різноманітності поняття інформації, словосполучення “інформаційна безпека” в різних контекстах може мати різний сенс. Так, у Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” наводиться таке поняття інформаційної безпеки:

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Спеціальне законодавство в галузі безпеки інформаційної діяльності представлено низкою законів. У їхньому складі особливе місце належить базовому Закону “Про інформацію, інформатизацію і захист інформації”, що закладає основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

- інформації та інформаційних систем;
- суб’єктів – учасників інформаційних процесів;
- правовідносин виробників – споживачів інформаційної продукції;
- власників інформації – обробників і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

Інформаційна безпека (ІБ) – це стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб’єктам інформаційних відносин, зокрема, власникам і користувачам інформації та інфраструктури.

Таким чином, правильний з методологічної точки зору підхід до проблем ІБ починається з виявлення суб’єктів інформаційних відносин та інтересів цих суб'єктів, пов’язаних з використанням інформаційних систем (ІС). Загрози інформаційній безпеці – це зворотна сторона використання інформаційних технологій.

Тут необхідно зауважити, що трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно різнитися. Для ілюстрації досить зіставити режимні державні організації і навчальні заклади. У першому випадку “хай краще все зламається, ніж ворог дізнається хоч один секретний біт”, у другому – “немає у нас жодних секретів, аби все працювало”. Отже, інформаційна безпека не зводиться виключно до захисту від несанкціонованого доступу до інформації, це поняття принципово ширше.

Суб’єкт інформаційних відносин може постраждати (зазнати збитки та/або одержати моральний збиток) не тільки від несанкціонованого доступу, але й від поломки системи, що викликала перерву в роботі. Більш того, для багатьох

відкритих організацій власне захист від несанкціонованого доступу до інформації стоїть за важливістю зовсім не на першому місці.

Повертаючись до питань термінології, відзначимо, що термін “комп’ютерна безпека”(як еквівалент або замінник ІБ) є дуже вузьким. Комп'ютери – тільки одна із складових інформаційних систем, і хоч наша увага буде зосереджена в першу чергу на інформації, яка зберігається, обробляється і передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових і, в першу чергу, найслабкішою ланкою, якою в переважній більшості випадків виявляється людина.

Згідно з визначенням інформаційної безпеки, вона залежить не тільки від комп’ютерів, але й від інфраструктури, що її підтримує, до якої можна віднести системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання інформаційною системою своїх функцій.

Звернемо увагу, що у визначенні ІБ перед іменником “втрати” знаходиться прикметник “неприйнятний”. Очевидно, застрахуватися від усіх видів втрат неможливо, тим більше неможливо зробити це економічно доцільним способом, коли вартість захисних засобів і заходів не перевищує розмір очікуваних втрат. Значить, з чимось доводиться миритися і захищатися слід тільки від того, з чим змиритися ніяк не можна. Іноді такими неприпустимими витратами є нанесення шкоди здоров'ю людей або стану навколишнього середовища, але частіше поріг неприйнятності має матеріальний (грошовий) вираз, а метою захисту інформації стає зменшення розмірів втрат до припустимих значень.

1.2. Основні задачі інформаційної безпеки

Інформаційна безпека – це багатогранна галузь діяльності, в якій успіх може принести тільки систематичний, комплексний підхід.

Основними задачами інформаційної безпеки є:

- забезпечення доступності інформації;
- забезпечення цілісності інформації;
- забезпечення конфіденційності інформації;
- забезпечення вірогідності інформації;
- забезпечення юридичної значимості інформації, представленої у вигляді електронного документа;
- забезпечення невідстежуваності дій користувача.

Доступність – це властивість інформаційного об’єкта щодо одержання його користувачем за прийнятний час.

Інформаційні системи створюються для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитку всім суб’єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво основна роль доступності виявляється в різного роду системах управління виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги тощо).

Цілісність – це властивість інформаційного об’єкта зберігати свою структуру і/або зміст у процесі передавання і зберігання.

Розрізняють цілісність *статичну* (тобто незмінність інформаційних об’єктів) і *динамічну* (стосується коректного виконання складних дій (транзакцій). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Цілісність є найважливішим аспектом ІБ в тих випадках, коли інформація служить “керівництвом до дії”. Рецептура ліків, зміст медичних процедур, набір і характеристики комплектуючих виробів, хід технологічного процесу – все це

приклади інформації, порушення цілісності якої може призвести до небажаних наслідків. Неприємно і спотворення офіційної інформації, будь то текст закону або сторінка Web-сервера якої-небудь урядової організації.

Конфіденційність – це властивість інформації бути доступною тільки обмеженому колу користувачів інформаційної системи, в якій циркулює дана інформація.

Конфіденційність – найбільш опрацьований у нашій країні аспект інформаційної безпеки. На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем пов’язана із серйозними труднощами. По-перше, відомості про технічні канали витоку інформації є закритими, тому більшість користувачів позбавлено можливості мати уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії, як основного засобу забезпечення конфіденційності, стоять численні законодавчі перепони і технічні проблеми.

Вірогідність – це властивість інформації, яка полягає у строгій приналежності об’єкту, що є її джерелом, або тому об’єкту, від якого ця інформація прийнята.

Юридична значимість – це властивість інформації, представленої у вигляді електронного документа, мати юридичну силу.

З цією метою суб’єкти, що мають потребу в підтвердженні юридичної значимості переданого повідомлення, домовляються про прийняття деяких атрибутів інформації, що описують її здатність бути юридично значимою. Дана властивість інформації особливо актуальна в системах електронних платежів, де здійснюється операція з пересилання коштів.

Невідстежуваність – це здатність користувача робити деякі дії в інформаційній системі непомітно для інших об'єктів.

Актуальність даної вимоги виникла завдяки появі таких понять, як електронні гроші та Internet-banking. Так, для авторизації доступу до електронної платіжної системи користувач повинен надати деякі відомості, що однозначно його ідентифікують. У процесі розвитку даних систем може з’явитися реальна небезпека, що, наприклад, усі платіжні операції будуть контролюватися, тим самим виникнуть

умови для тотального стеження за користувачами інформаційних систем.

Існує кілька шляхів вирішення проблеми неможливості стеження:

- заборона за допомогою законодавчих актів будь-якого тотального стеження за користувачами інформаційних систем;
- застосування криптографічних методів для підтримки неможливості слідкування.

Інформаційна безпека може розглядатися не тільки стосовно деяких конфіденційних відомостей, але і стосовно здатності інформаційної системи виконувати задані функції.

Інформаційна безпека в рамках забезпечення працездатності ІС повинна забезпечувати захист від**:**

- порушення функціонування інформаційної системи шляхом впливу на інформаційні канали, канали сигналізації, керування і віддаленого завантаження баз даних, комутаційного устаткування, системне і прикладне програмне забезпечення;
- несанкціонованого доступу до інформаційних ресурсів і від намагань використання ресурсів мережі, що призводять до витоку даних, порушення цілісності мережі й інформації, зміни функціонування підсистем розподілу інформації, доступності баз даних;
- руйнування засобів захисту, що вбудовуються, і зовнішніх засобів;
- неправомірних дій користувачів і обслуговуючого персоналу мережі.

Пріоритети серед перерахованих задач інформаційної безпеки визначаються індивідуально для кожної конкретної ІС і залежать від вимог, що висуваються безпосередньо до інформаційних систем.

Якщо повернутися до аналізу інтересів різних категорій суб’єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй за важливістю цілісність – який сенс в інформаційній послузі, якщо вона містить спотворені відомості?

З погляду державних структур захисні заходи в першу чергу покликані забезпечити *конфіденційність, цілісність і доступність інформації.*

Комерційним структурам**,** ймовірно, важливіше всього *цілісність і доступність* даних і послуг. На відміну від державних, комерційні організації більш відкриті і динамічні, тому ймовірні загрози для них відрізняються не тільки кількістю, але і якістю.

Для розв'язання задач забезпечення безпеки в інформаційних системах необхідно:

- захистити інформацію під час її зберігання, оброблення і передавання мережею;
- підтвердити дійсність об'єктів даних і користувачів (автентифікація сторін, що встановлюють зв'язок);
- знайти і попередити порушення цілісності об'єктів даних;
- захистити технічні пристрої і приміщення;
- захистити конфіденційну інформацію від витоку і від вбудованих електронних пристроїв знімання інформації;
- захистити програмні засоби від під'єднання програмних закладок і вірусів;
- захистити від несанкціонованого доступу до інформаційного ресурсу і технічних засобів мережі, зокрема, до засобів керування, щоб запобігти зниженню рівня захищеності інформації і самої мережі в цілому;
- організувати заходи, що спрямовані на забезпечення збереження конфіденційних даних.

Конкретна реалізація загальних принципів забезпечення інформаційної безпеки може полягати в організаційних або технічних заходах захисту інформації [11].

2. Основні поняття криптографії

2.1. Загальні відомості

Криптографія – наука про створення безпечних методів зв'язку, про створення стійких (стійких до злому) шифрів. Вона займається пошуком математичних методів перетворення інформації.

Криптоаналіз - даний розділ присвячений дослідженню можливості читання повідомлень без знання ключів тобто пов'язаний безпосередньо зі зломом шифрів. Люди, що займаються криптоаналізом і дослідженням шифрів називаються криптоаналітиками.

Шифр - сукупність оборотних перетворень безлічі відкритих текстів (тобто вихідного повідомлення) на безліч зашифрованих текстів, що проводяться з метою їх захисту. Конкретний вид перетворення визначається за допомогою ключа шифрування.

Для кращого розуміння суті варто ввести ще декілька понять такі як: шифрування - процес застосування шифру до відкритого текст, розшифрування - процес зворотного застосування шифру до зашифрованого тексту та дешифрування - спроба прочитати зашифрований текст без знання ключа, тобто злом шифротексту або шифру. Тут слід підкреслити різницю між розшифрування і дешифруванням. Перша дія проводиться законним користувачем, які знають ключ, а друга криптоаналітиками або досить вмілими хакерами.

Сучасна криптографія також має поняття криптографічної системи - сімейство перетворень шифру і сукупність ключів (тобто алгоритм + ключі). Само по собі опис алгоритму не є криптосистемою. Тільки доповнене схемами розподілу і управління ключами воно стає системою. Приклади алгоритмів - опису DES, ГОСТ28.147-89. Доповнені алгоритмами вироблення ключів, вони перетворюються в кріптосистеми. Як правило, опис алгоритму шифрування вже включає в себе всі необхідні частини.

Сучасні криптосистеми поділяють на два типи:

1. Симетричні криптосистеми (з секретним ключем - secret key systems) – дані криптосистеми побудовані на основі збереження в таємниці ключа шифрування. Процеси шифрування і розшифрування використовують один і той же ключ. Секретність ключа є постулатом. Основна проблема при застосуванні симетричних криптосистем для зв'язку полягає в складності передачі обом сторонам секретного ключа. Однак дані системи мають високу швидкодію. Розкриття ключа зловмисником загрожує розкриттям тільки тієї інформації, що була зашифрована на цьому ключі. Американський і Російський стандарти шифрування DES і ГОСТ28.147-89, кандидати на AES - всі ці алгоритми є представниками симетричних криптосистем.

2. Асиметричні криптосистеми (системи відкритого шифрування - О.Ш., з відкритим ключем тощо - public key systems) - сенс даних криптосистем полягає в тому, що для шифрування і розшифрування використовуються різні перетворення. Одне з них - шифрування - є абсолютно відкритим для всіх. Інша ж - розшифрування - залишається секретним. Таким чином, будь-який, хто хоче що-небудь зашифрувати, користується відкритим перетворенням. Але розшифрувати і прочитати це зможе лише той, хто володіє секретним перетворенням. На даний момент у багатьох асиметричних криптосистемах вид перетворення визначається ключем. Тобто у користувача є два ключі - секретний і відкритий. Відкритий ключ публікується в загальнодоступному місці, і кожен, хто захоче послати повідомлення цьому користувачу - зашифровує текст відкритим ключем. Розшифрувати зможе тільки згаданий користувач з секретним ключем. Таким чином, пропадає проблема передачі секретного ключа (як у симетричних систем). Однак, незважаючи на всі свої переваги, ці криптосистеми досить трудомісткі і повільні. Стійкість асиметричних криптосистем базується, в основному, на алгоритмічної труднощі вирішити за прийнятне час будь-яку задачу. Якщо зловмисникові вдасться побудувати такий алгоритм, то дискредитована буде вся система і всі повідомлення, зашифровані за допомогою цієї системи. У цьому полягає головна небезпека асиметричних криптосистем на відміну від симетричних. Приклади - системи О.Ш. RSA, система О.Ш. Рабина тощо [7].

2.2. Шифр Play Fair. Криптоаналіз шифру Play Fair

2.2.1. Опис шифру

Шифр Плейфера використовує матрицю 5x5 (для латинського алфавіту, для кириличного алфавіту можливо збільшити розмір матриці до 4x8), що містить ключове слово або фразу. Для створення матриці й використання шифру досить запам'ятати ключові слова й чотири простих правила. Щоб скласти ключову матрицю, в першу чергу потрібно заповнити порожні клітинки матриці буквами ключового слова (без запису символів, які повторюються), потім заповнити пусті клітинки матриці символами алфавіту, що не зустрічаються в ключовому слові, по порядку (в англійських текстах зазвичай опускається символ «Q», щоб зменшити алфавіт, в інших версіях «I» і «J» об'єднуються в одну клітинку). Ключове слово можна записувати у верхніх рядках матриці зліва направо, або якимось іншим чином, наприклад, по спіралі з лівого верхнього кута до центру. Ключове слово, доповнене алфавітом, становить матрицю 5x5 і є ключем шифру.

1. Для того щоб зашифрувати повідомлення, необхідно розбити його на біграми (групи з двох символів), наприклад «Hello World» стає «HE LL OW OR LD», і відшукати ці біграми в таблиці. Два символи біграми відповідають протилежним кутам прямокутника в ключовий матриці. Визначаємо положення кутів цього прямокутника відносно один одного. Потім, керуючись наступними 4 правилами, зашифровуємо пари символів вихідного тексту:

2. Якщо два символи біграми збігаються (або якщо залишився один символ), додаємо після першого символу «X», зашифровуємо нову пару символів і продовжуємо. У деяких варіантах шифру Плейфера замість «X» використовується «Q».

3. Якщо символи біграми вихідного тексту зустрічаються в одному рядку, то ці символи замінюються на символи, розташовані в найближчих стовпцях

праворуч від відповідних символів. Якщо символ є останнім в рядку, то він замінюється на перший символ цього ж рядка.

4. Якщо символи біграми вихідного тексту зустрічаються в одному стовпці, то вони перетворюються в символи того ж стовпця, що знаходяться безпосередньо під ними. Якщо символ є нижнім в стовпці, то він замінюється на перший символ цього ж стовпця.

5. Якщо символи біграми вихідного тексту знаходяться в різних стовпчиках і різних рядках, то вони замінюються на символи, що знаходяться в тих же рядках, але відповідні іншим кутам прямокутника.

6. Для розшифровки необхідно використовувати інверсію цих чотирьох правил, відкидаючи символи «X» (або «Q»), якщо вони не несуть сенсу в початковому повідомленні [2].

2.1.2. Приклад шифрування

Нехай треба зашифрувати фразу “ПУСТЬ КОНСУЛЫ БУДУТ БДИТЕЛЬНЫ”.

Вихідний текст розбивається на біграми

ПУ СТ ЬК ОН СУ ЛЫ БУ ДУ ТБ ДИ ТЕ ЛЬ НЫ

За допомогою таблиці

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

отримуємо таку шифровку:

ЦТ ТН ЦВ ПО ФТ БЧ ЧЕ ФЕ ЕО ЗГ ЖЯ ЫК ЩО

Шифрування біграмами значно підвищило стійкість шифрів до зламування. Але, незважаючи на те, що “Поліграфія” І. Трисеміуса була легко доступною друкованою книжкою, ідеї, що описані в ній, отримали визнання лише через три сторіччя. Напевно це викликано тим, що І. Трисеміус був погано відомий криптографам тому що його вважали богословом, бібліофілом і засновником архівної справи.

На скільки виросла стійкість таких шифрів до зламування? Якщо алфавіт повідомлення складається з 30 літер, то кількість біграм дорівнює 900. Таким чином ймовірність успіху частотного криптоаналізу шифру “Чесна гра” є, лише коли довжина шифрованих текстів перевищує приблизно 2000 літер (сторінка друкованого тексту).

2.1.3. Криптоаналіз шифру Плейфера

Як і більшість шифрів формальної криптографії, шифр Плейфера може бути легко зламаний, якщо є достатній обсяг тексту. Якщо відомий і зашифрований, і відкритий текст, то ключ отримати дуже просто. Коли відомий тільки зашифрований текст, криптоаналітики аналізують відповідність між частотою появи біграм у зашифрованому тексті і відомою частотою появи біграм у мові, на якій написано повідомлення.

Вперше алгоритм злому шифру Плейфера був описаний в брошурі лейтенанта Джозефа О. Моуборнома в 1914 році. Пізніше, в 1939 році, криптоаналіз шифру був наведений в книзі Х. Ф. Гейнс «Cryptanalysis — a study of ciphers and their solution». Однак більш докладний посібник для знаходження ключа для шифру Плейфера можна знайти в розділі 7 «Solution to polygrafic substitution systems» керівництва Field Manual 34-40-2 Сухопутних Військ США.

Шифр Плейфера зломується подібно до шифру двох квадратів, але простіше. Для цього застосовується кілька закономірностей. Найважливіша — це те, що у зашифрованому тексті пряма і обернена біграми (AB і BA) відповідають іншій прямій і оберненій біграмі у відкритому тексті (наприклад RE і ER). В

англійській мові є багато слів, що містять такі інверсні біграми, наприклад REceivER і DEpartED — це зручна зачіпка для початку криптоаналізу. У зашифрованому тексті відшукуються близькі обернені біграми, для них шукаються відповідники зі списку відомих слів відкритого тексту. Це дозволяє відтворити частину вихідного тексту і почати конструювати ключа.

Існує інший підхід до криптоаналізу шифру Плейфера, який отримав назву Random-restart hill climbing. Він починається із матриці випадкових символів. За допомогою найпростіших ітерацій матриця випадкових символів максимально наближається до оригінальної матриці. Очевидно, що цей метод дуже складний для людини, але комп'ютери за допомогою такого алгоритму можуть зламати шифр, навіть маючи невеликий обсяг тексту [8].

Також існує інший спосіб взлому такого шифру. Так як ключ шифру Плейфера є таблицею, що містить 25 букв англійського алфавіту, можна помилково припустити, що метод пошуку сходженням до вершини - кращий спосіб злому даного шифру. На жаль, цей метод не буде працювати. Досягнувши певного рівня відповідності тексту, алгоритм застрягне в точці локального максимуму і не зможе продовжити пошук.

Щоб успішно зламати шифр Плейфера краще скористатися алгоритмом імітації відпалу.

Відмінність алгоритму імітації відпалу від пошуку сходженням до вершини полягає в тому, що останній на шляху до правильного рішення ніколи не приймає в якості можливого рішення слабші варіанти. У той час як алгоритм імітації відпалу періодично відкочується назад до менш імовірним рішенням, що збільшує шанси на кінцевий успіх.

Суть алгоритму зводиться до наступних дій:

1. Вибирається випадкова послідовність літер - основний-ключ. Шифр текст розшифровується за допомогою основного ключа. Для отриманого тексту обчислюється коефіцієнт, що характеризує ймовірність приналежності до природної мови.

2. Основний ключ піддається невеликим змінам (перестановка двох довільно вибраних букв, перестановка стовпців або рядків). Проводиться розшифровка і обчислюється коефіцієнт отриманого тексту.

3. Якщо коефіцієнт вище збереженого значення, то основний ключ замінюється на модифікований варіант.

4. В іншому випадку заміна основного ключа на модифікований відбувається з ймовірністю, яка прямо залежить від різниці коефіцієнтів основного і модифікованого ключів.

5. Кроки 2-4 повторюються близько 50 000 разів.

Алгоритм періодично заміщає основний ключ, ключем з гіршими характеристиками. При цьому ймовірність заміни залежить від різниці характеристик, що не дозволяє алгоритму приймати погані варіанти занадто часто.

Для розрахунку коефіцієнтів, що визначають приналежність тексту до природної мови найкраще використовувати частоти появи триграм.

Шифр Плейфера можна відрізнити від шифру двох квадратів за тою озанкою, що в ньому ніколи не зустрічаються біграми з повторюваними символами (наприклад ЇЇ). Якщо в зашифрованому тексті відсутні біграми з повторюваними символами і його довжина досить велика, то можна припустити, що вихідний текст зашифрований шифром Плейфера [9].

Пізніше були зроблені спроби удосконалити шифр за допомогою використання матриці 7x4 і додаванням символів «*» і «#». Незважаючи на те, що аналіз шифру ускладнився, його все одно можна зламати тими ж методами, що і початковий.

3. Програмна реалізація шифрування методом Плейфера

3.1 Відомості про розроблений програмний продукт

В результаті роботи була розроблена програма яка здійснює шифрування та дешифрування тексту шифром Плейфера на мові програмування С++.

Одразу при відкритті додатку користувач бачить головне вікно яке (див. рис. 3.1.1). Оскільки основна робота програмного продукту полягає в шифруванні тексту то його поле поділене на кілька зон, а саме: поле «Вихідний текст», поле «Результат», поле під назвою «Дія» де користувач обирає що саме він хоче зробити, та «Шифрувальна решітка» де виводиться на екран схема за якою зашифровується повідомлення.

На рисунках 3.1.2 – 3.1.3 зображена робота програмного продукту під час зашифровування та розшифровування вхідного повідомлення. Також на цих рисунках видно шифрувальну решітку яка більш детально зображена на рисунку 3.1.4. На рисунку 3.1.5 зображене вікно яке виводить на екран загальні відомості про програмний продукт.

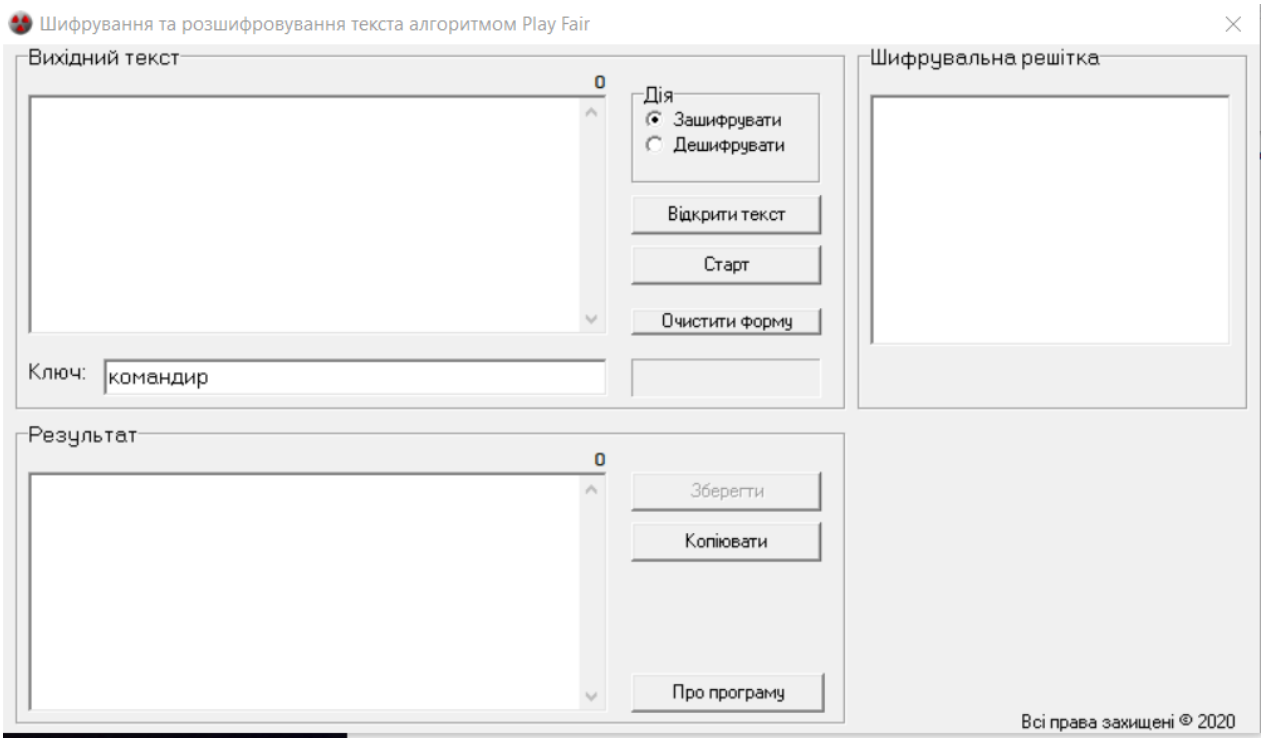

Рисунок 3.1.1 – Загальний вигляд програмного продукту

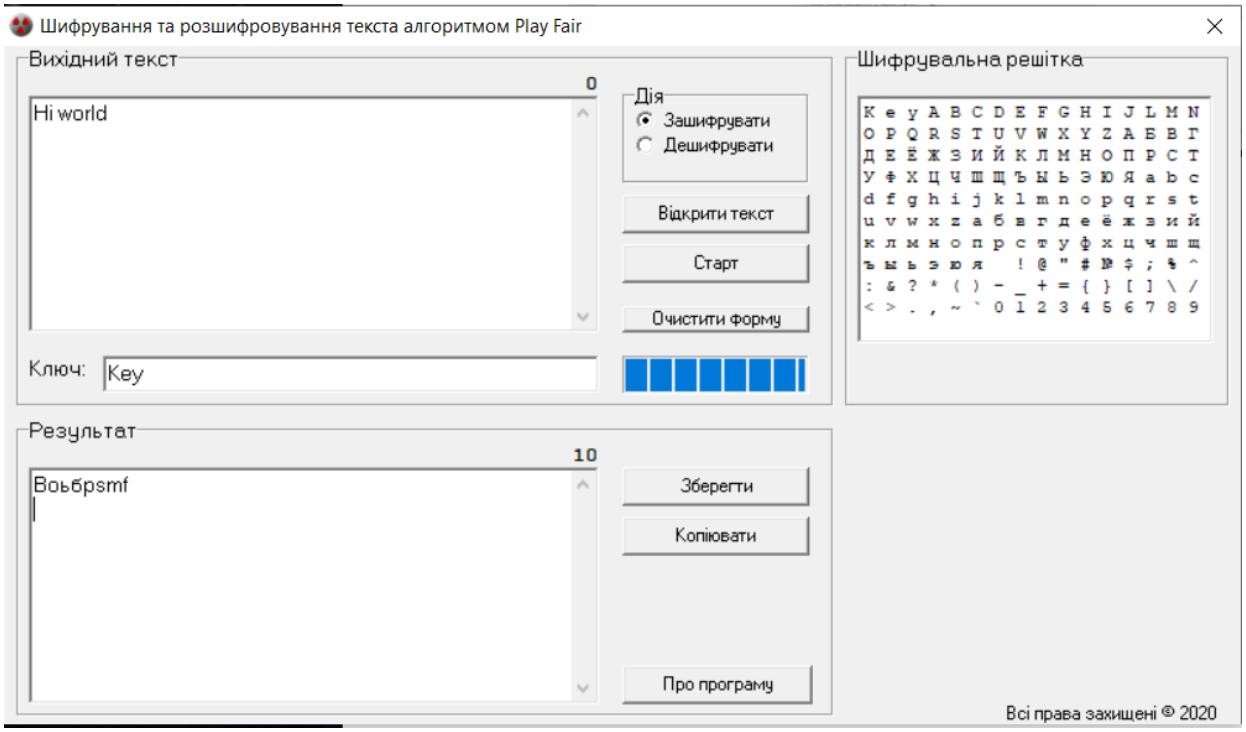

Рисунок 3.1.2 – Робота програмного забезпечення під час шифрування тексту

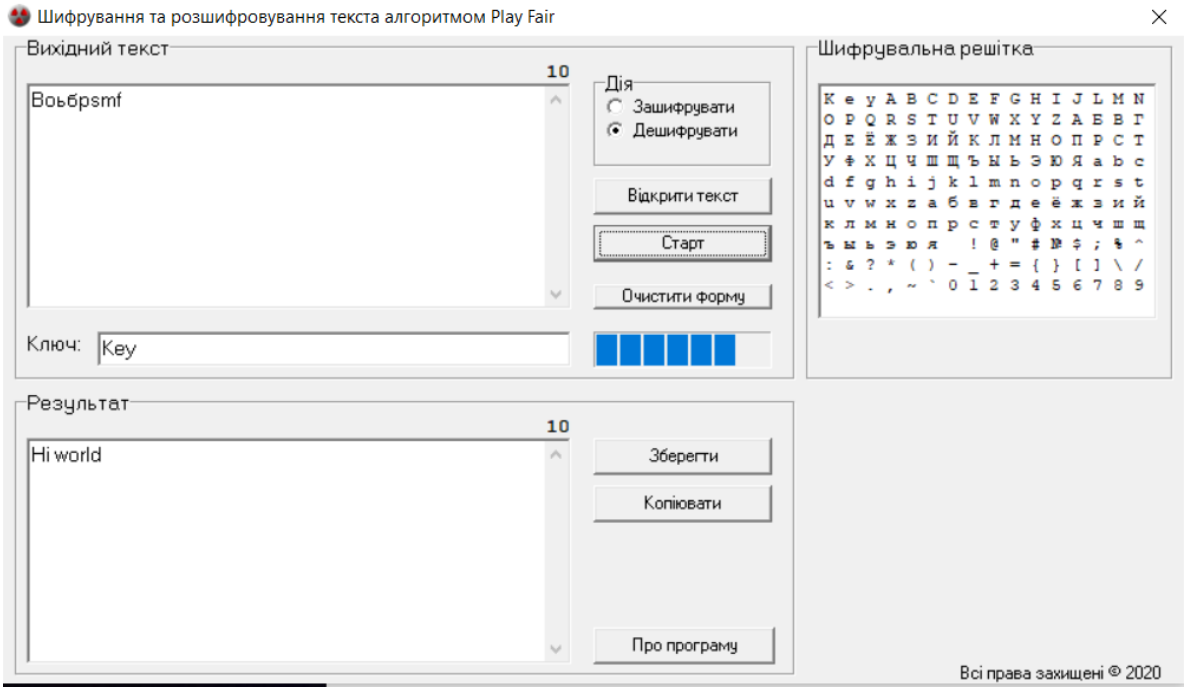

Рисунок 3.1.3 – Робота програмного забезпечення під час розшифрування тексту

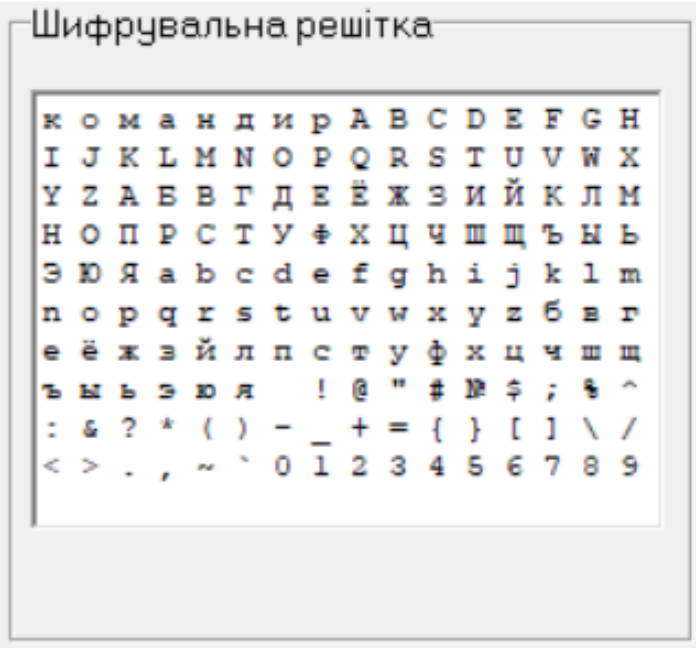

Рисунок 3.1.4 – Матриця шифрування що використовується в роботі

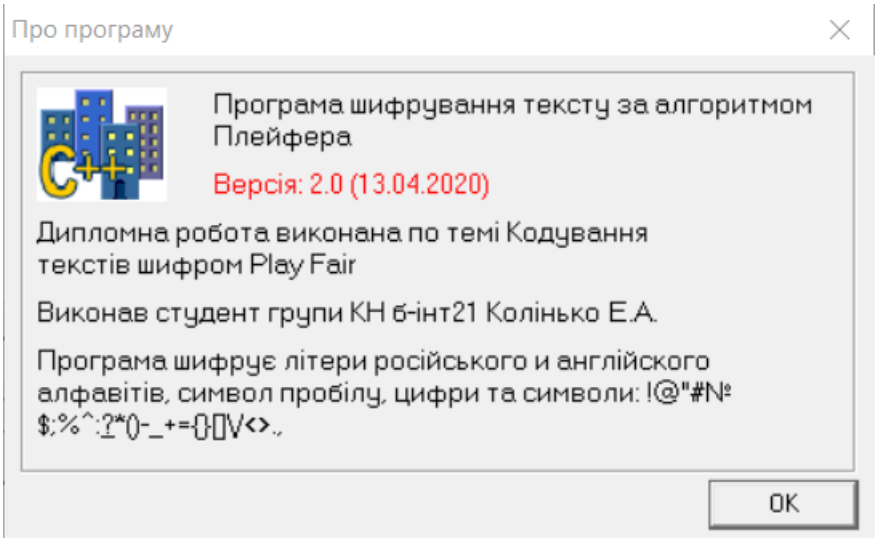

Рисунок 3.1.5 – Вікно з загальною інформацією про програмний продукт

До бакалаврської роботи додається диск з програмним продуктом та вихідним кодом. Також частини вихідного коду наведено в бакалаврській роботі (див. додаток А).

3.2 Приклад роботи програмного продукту

Програмний продукт розроблений в рамках бакалаврської роботи виконує функції шифрування та дешифрування вхідних повідомлень з допомогою певного ключа який задає користувач. Повідомлення для обробки можуть бути завантаженні з текстового файлу (див. рис. 3.2.1 – 3.2.2).

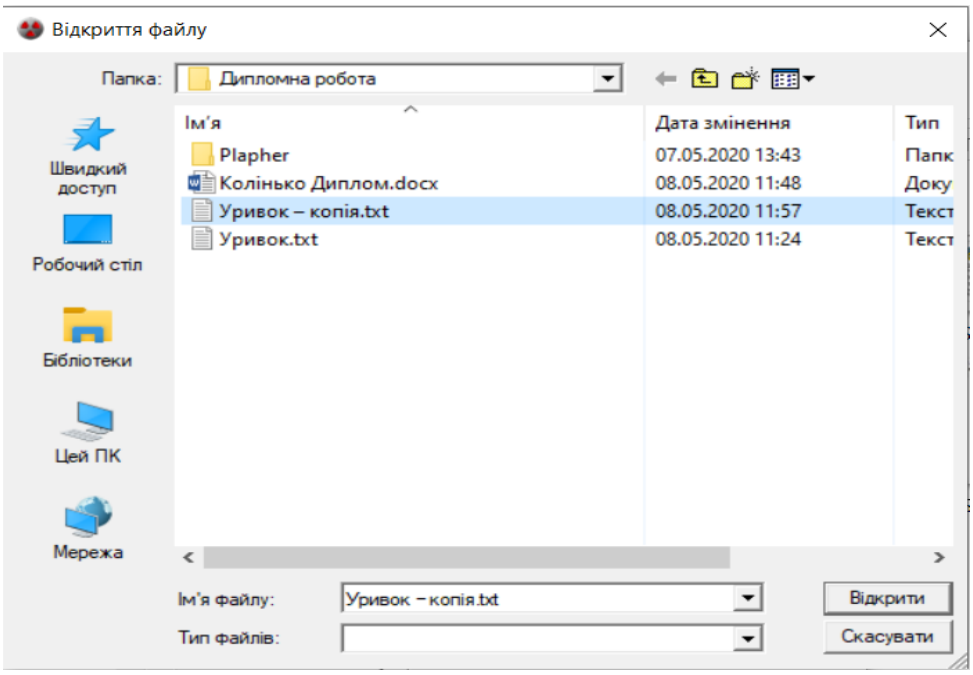

Рисунок 3.2.1 – Вибір текстового файлу з повідомленням

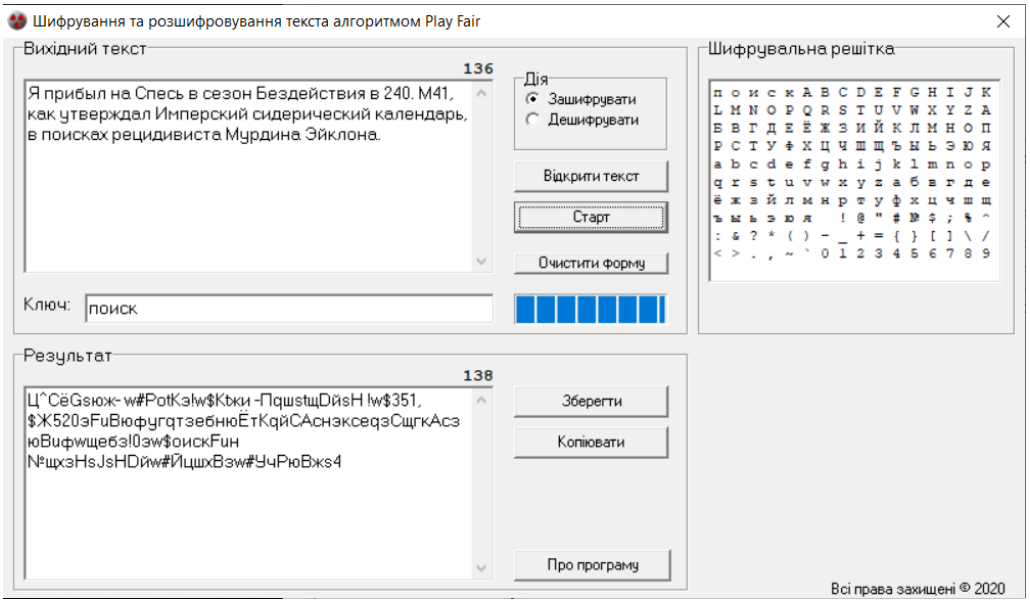

Рисунок 3.2.2 – Робота з повідомленням отриманим з текстового файлу

Також користувач має можливість ввести повідомлення власноруч у відповідне вікно. Така можливість показана на рисунку 3.2.3.

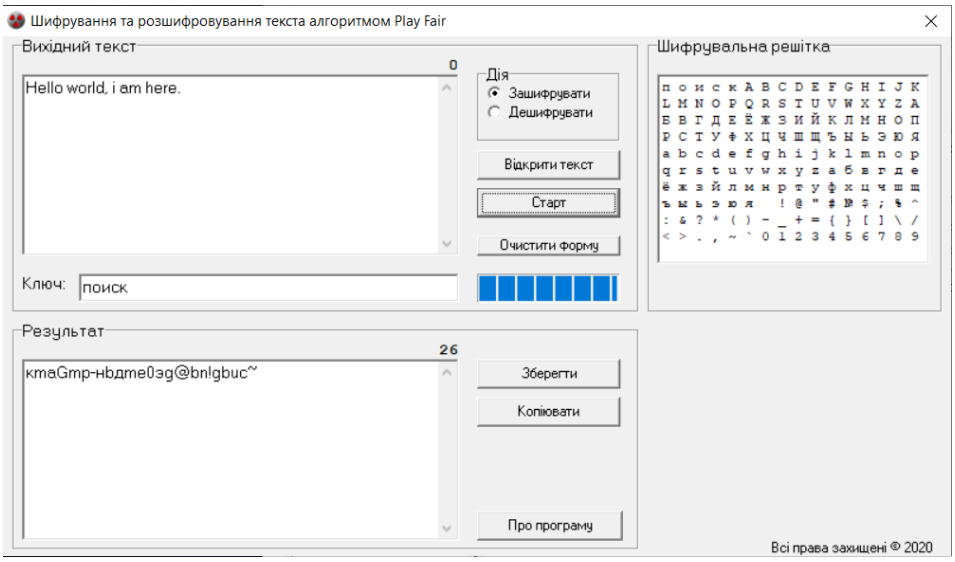

Рисунок 3.2.3 – Робота додатку з повідомленням, яке користувач вводив власноруч у відповідне поле

3.3 Інструкція користувача по роботі з програмою

Для початку роботи користувач повинен відкрити програму «Plefer.exe». після її відкриття на екрані з’явиться головне вікно додатку. (див. рис. 3.3.1).

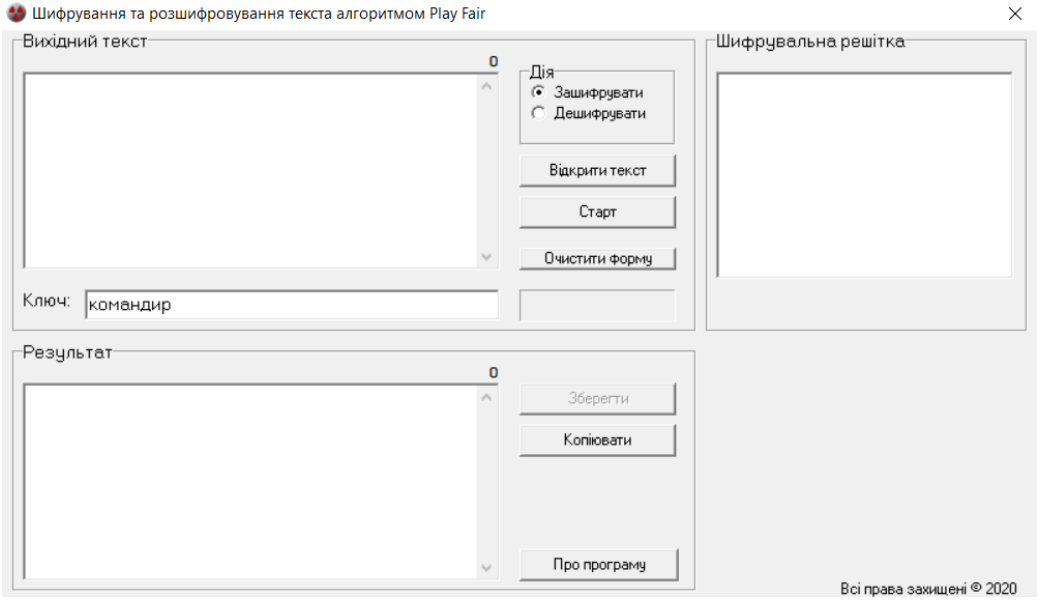

Рисунок 3.3.1 – Головне вікно програми

На головному вікні користувач може бачити 2 текстові поля які мають назву «Вихідний текст» куди користувач вводить текст який необхідно зашифрувати, та «Результат» де користувач може бачити перетворений текст (див. рис. 3.3.2 – 3.3.3). Також поле «Дія», де користувач обирає дію яку необхідно виконати програмі з текстом (див. рис. 3.3.4).

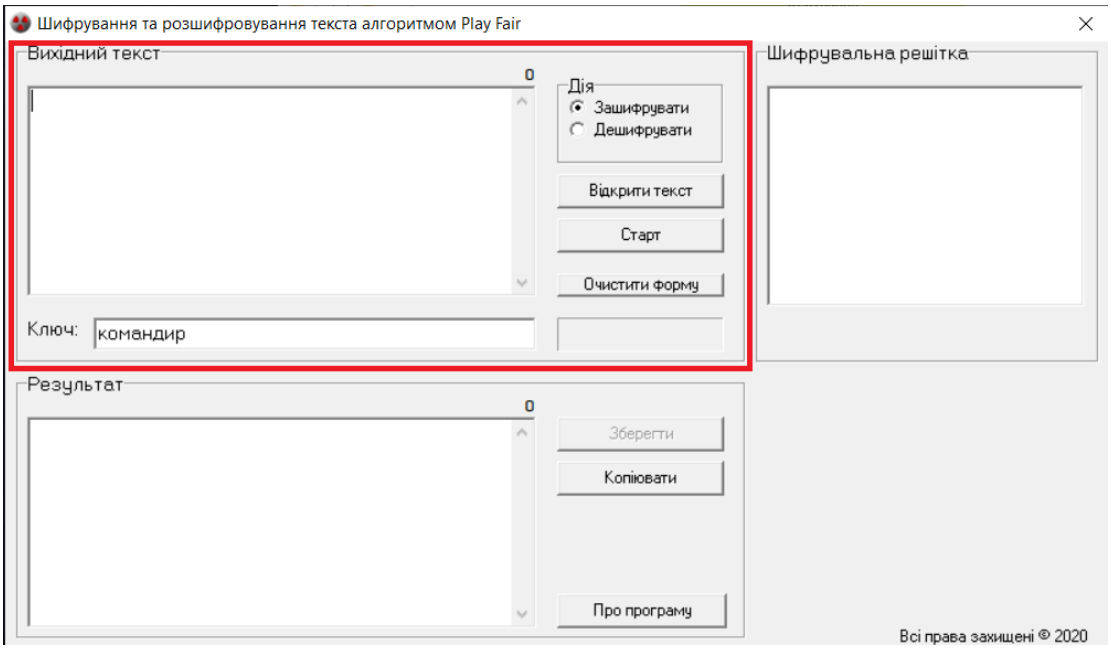

Рисунок 3.3.2 – Поле «Вихідний текст»

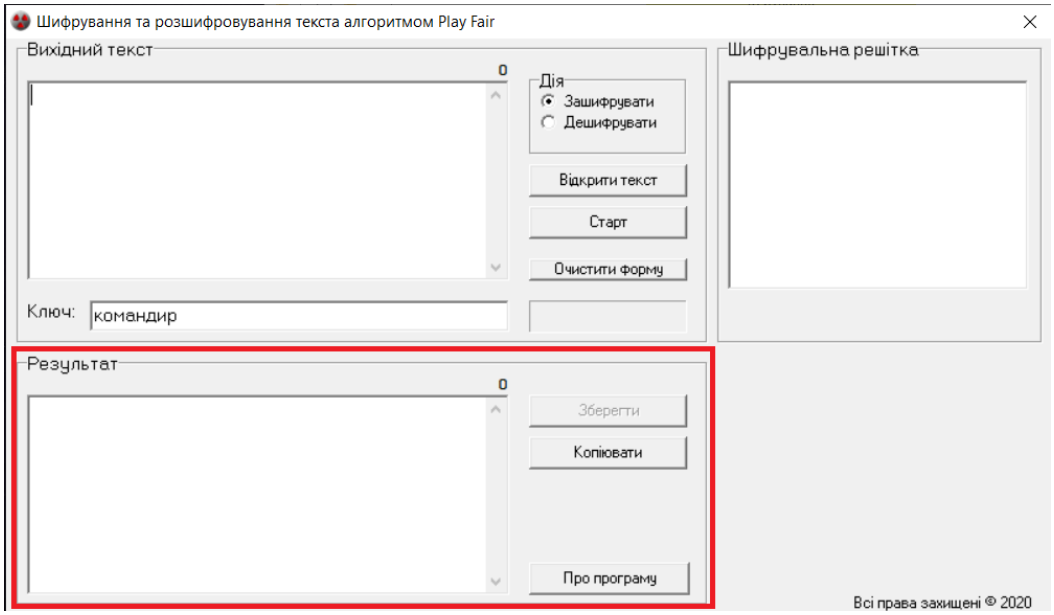

Рисунок 3.3.3 – Поле «Результат»

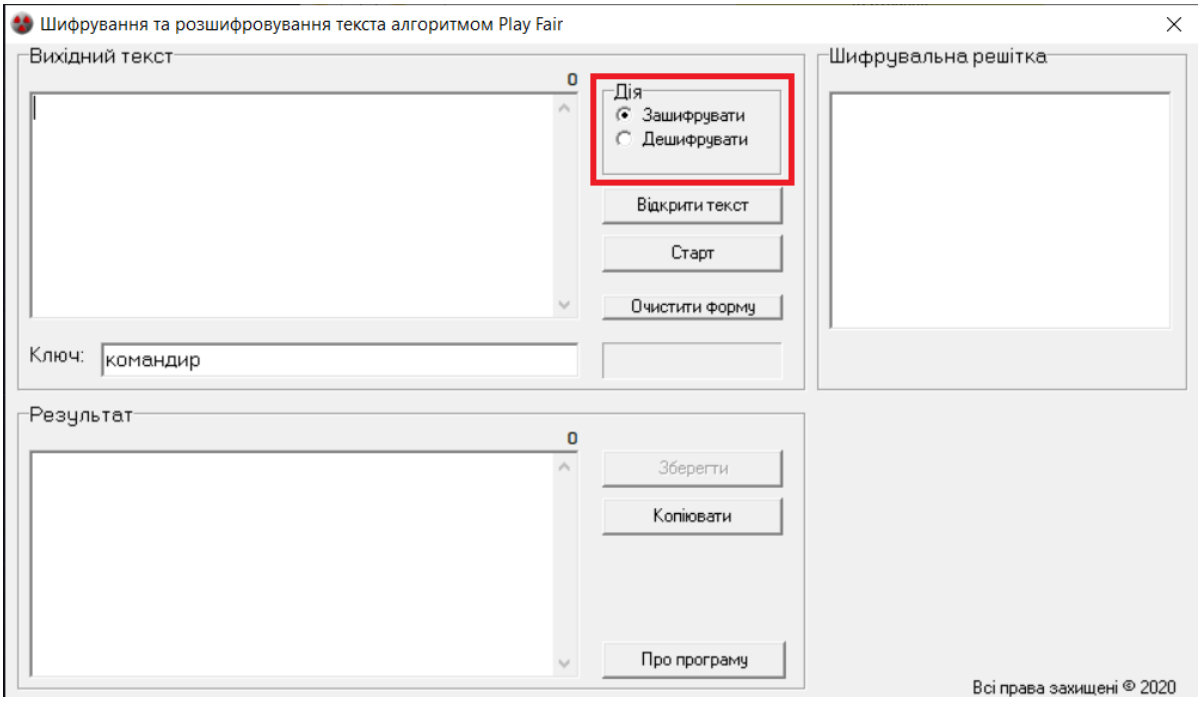

Рисунок 3.3.4 – Поле «Дія»

На рисунку 3.3.5 зображено кнопку «Відкрити текст» з допомогою якої користувач може обрати текстовий документ з повідомленням яке необхідно зашифрувати (рис. 3.3.5–3.3.6).

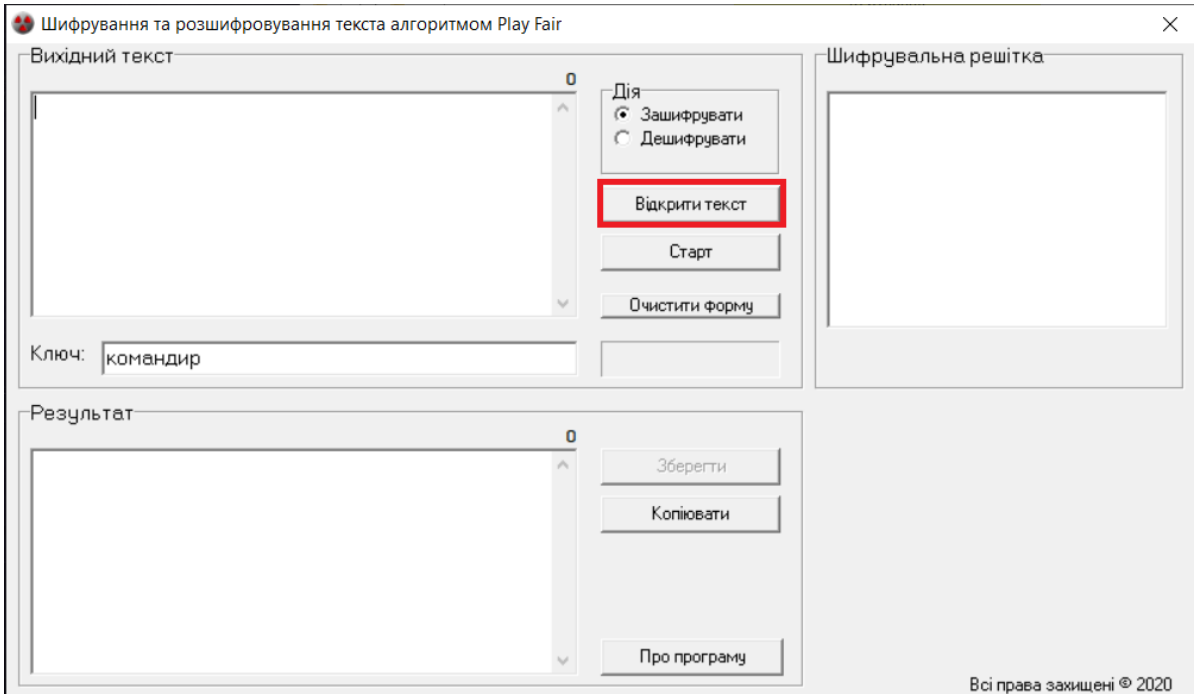

Рисунок 3.3.5 – Місцезнаходження кнопки «Відкрити текст»

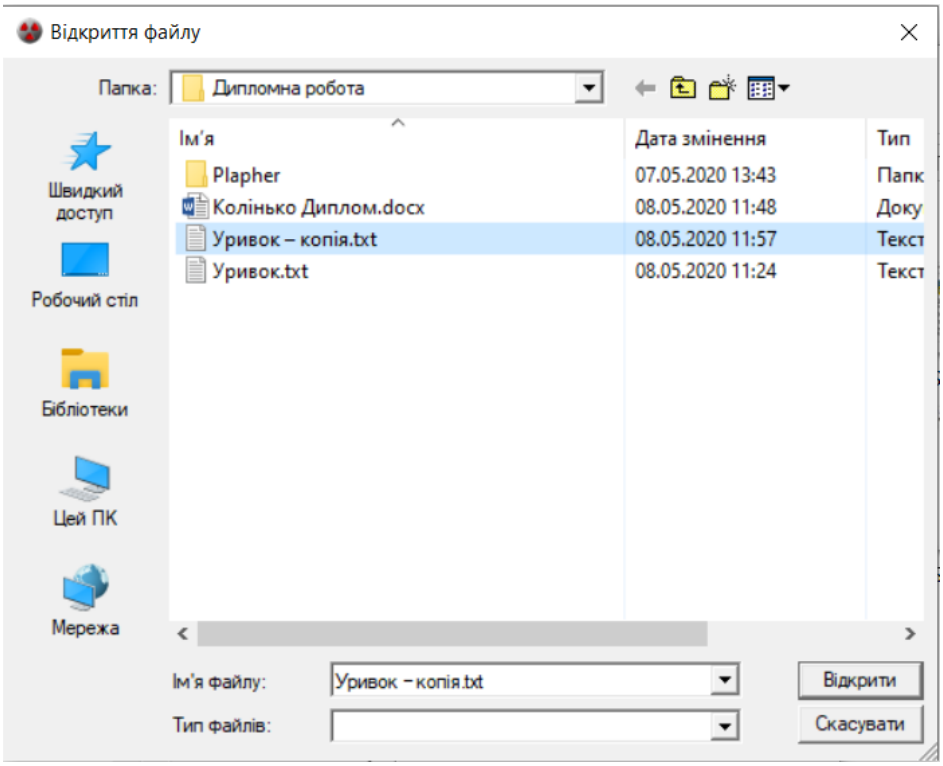

Рисунок 3.3.6 – Вікно вибору текстового файлу

На рисунку 3.3.7 зображено кнопку «Старт» котра запускає перетворення вхідного повідомлення. Одразу після цієї кнопки розташована інша «Очистити форму» (див. рис. 3.3.8).

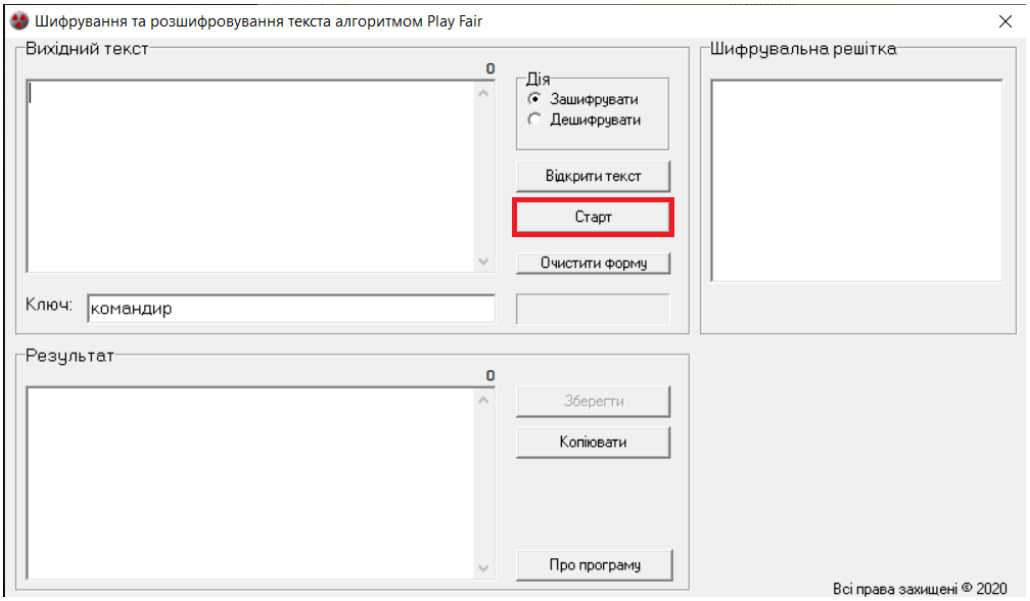

Рисунок 3.3.7 – Розташування кнопки «Старт»

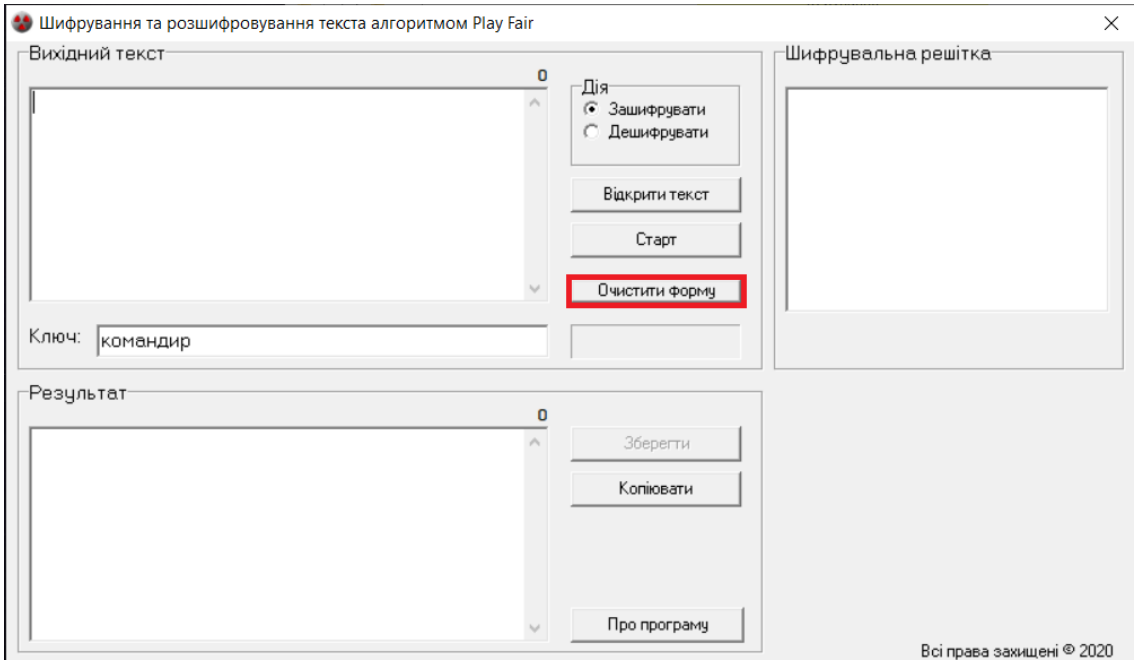

Рисунок 3.3.8 – Місцезнаходження кнопки «Очистити форму»

Напроти поля «Результат» розташовані кнопки «Зберегти», яка відповідає за збереження зашифрованого тексту в файл, та «Копіювати» яка копіює зашифрований текст в поле «Вихідний текст»(див рис. 3.3.9 – 3.3.10). На рисунку 3.3.11 розташована кнопка «Про програму» яка відкриває вікно що містить інформацію про програмний продукт.

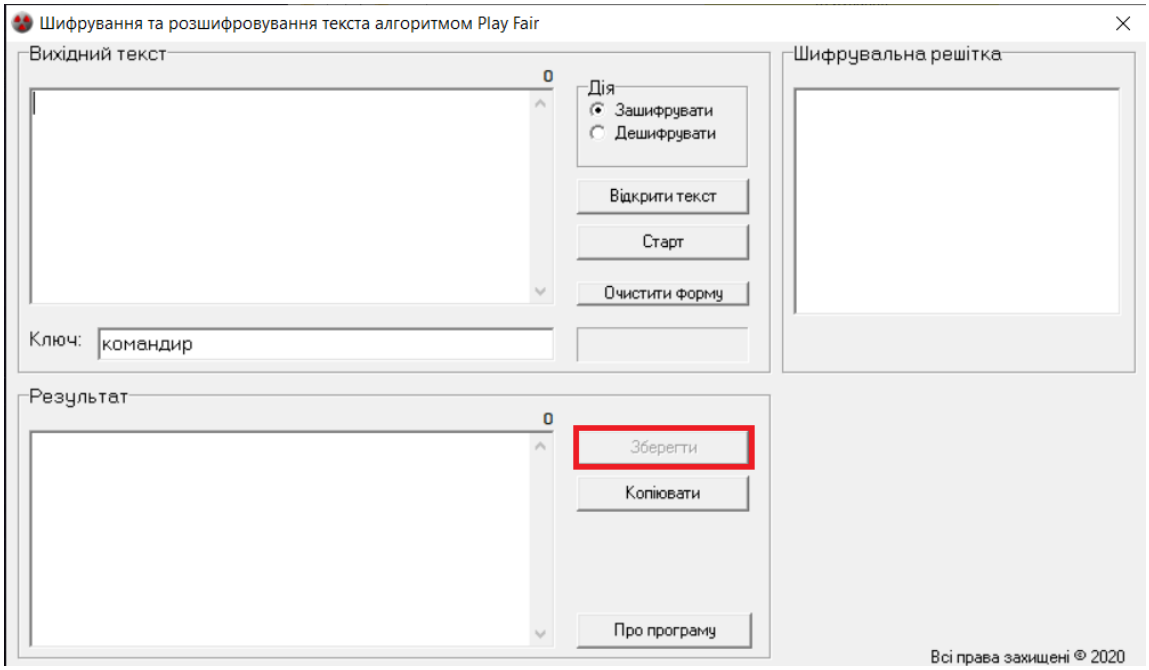

Рисунок 3.3.9 – Місцезнаходження кнопки «Зберегти»

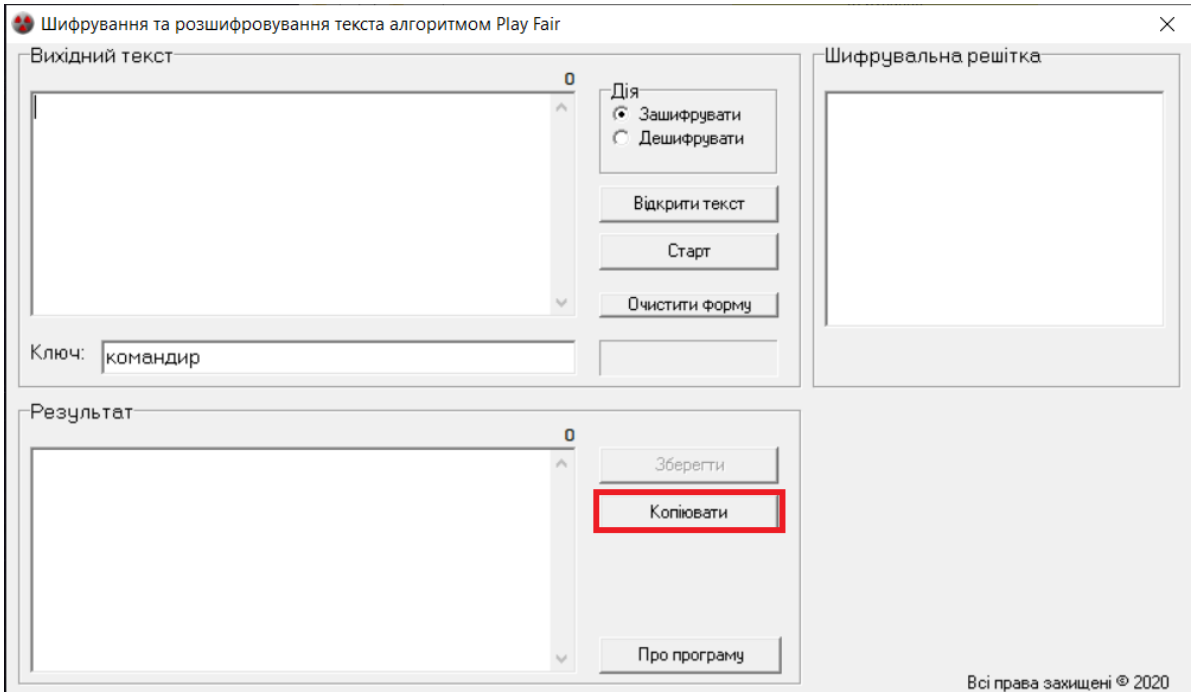

Рисунок 3.3.10 – Розташування кнопки «Копіювати»

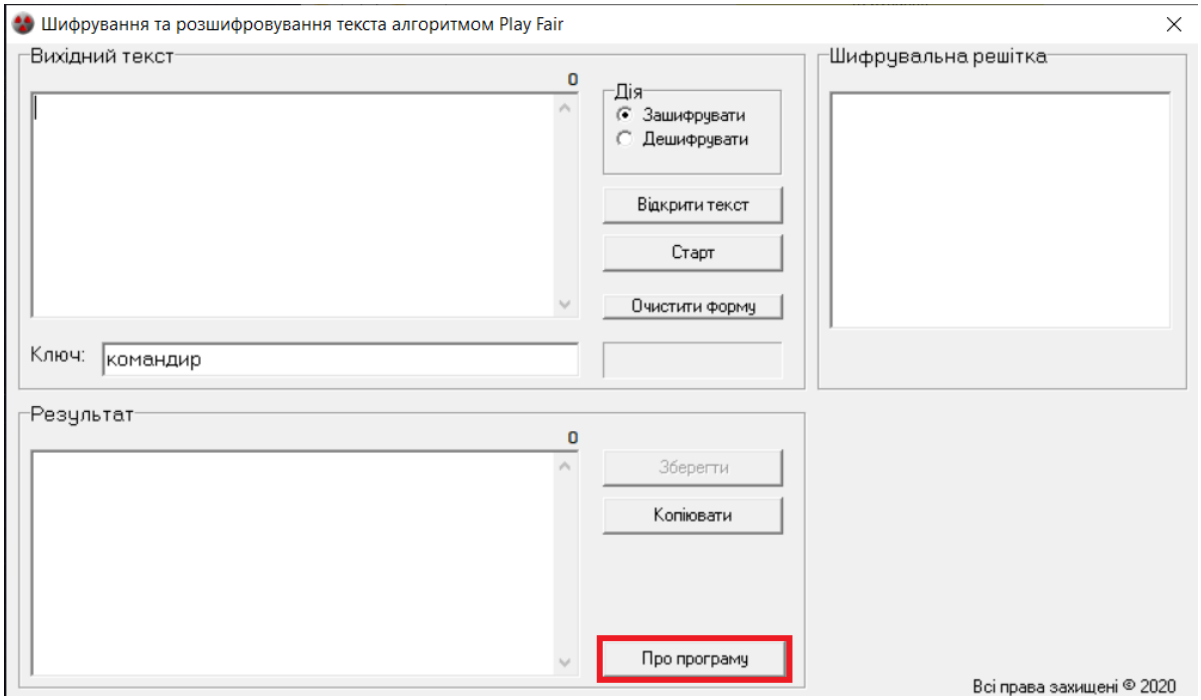

Рисунок 3.3.11 – Місцезнаходження кнопки «Про програму»

Також з лівого боку програми розташоване поле «Шифрувальна решітка» яка відображає матрицю за якою буде зашифрований текст (див. рис. 3.3.12).

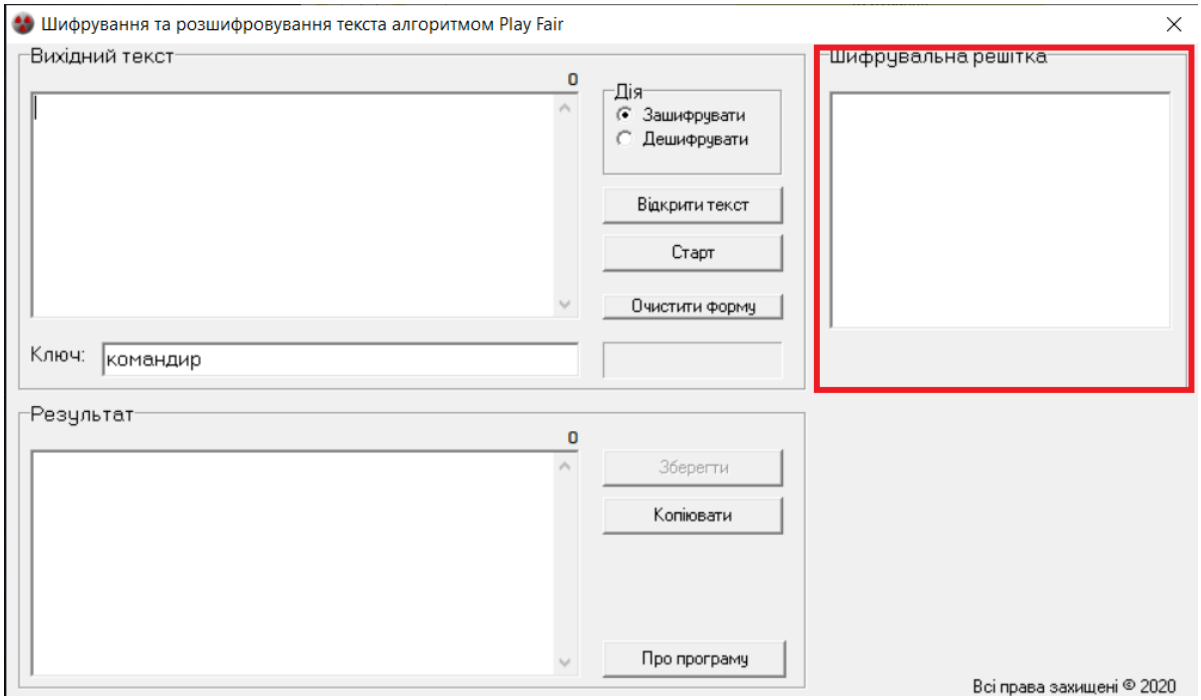

Рисунок 3.3.12 – Розташування поля «Шифрувальна решітка»

ВИСНОВКИ

На сьогоднішній день існує величезна кількість криптографічних алгоритмів, що відрізняються як своїми загальними характеристиками, так і принципами, на яких базується їх робота. Не всі вони є однаково надійними - серед них є навіть такі, що оформлені як стандарти та при цьому не забезпечують скільки-небудь реального захисту.

Створення надійного криптографічного алгоритму - дуже важка задача. Крім того, надійність є відносна річ - багато з раніше розроблених алгоритмів, які вважалися надійними, тепер або ненадійні, або ця надійність викликає великий сумнів. Тому при розробці криптографічного алгоритму необхідно враховувати тенденції розвитку комп'ютерної техніки а також інші фактори, що потенційно можуть знизити його стійкість в майбутньому [6, с. 138].

В процесі написання дипломної роботи було проведено аналіз різних методів шифрування тексту. За результатами проведено аналізу розроблено програмний продукт шифрування тексту методом Плейфера.

У ході виконання дипломної роботи виконано наступні задачі.

1. На основі порівняльного аналізу технологій програмування в різних мовах обрано C++ як найбільш оптимальну для вирішення поставленої задачі. Визначено пріоритетні цілі дипломної роботи та програмного продукту.

2. Визначено що для розробки подібних програмних продуктів часто використовуються С – подібні мови програмування, це зумовлено відносною легкість самого шифру та його невисокою вибагливістю. Як середовище програмування було обрано Borland C++, як засіб що надає досить широкий набір інструментів необхідних для написання програмного коду, низька витрата ресурсів необхідних для розгортання, та створення програмного продукту

Розроблено програмний продукт що реалізує шифрування тексту методом Плейфера.

Створений програмний продукт може слугувати як додатковий навчальний матеріал при вивчені дисциплін пов’язаних з захистом інформації, або як засіб

шифрування та розшифрування тексту методом Play Fair. Також даний програмний продукт можна використовувати як основу для більш розвинених криптографічних систем котрі зможуть шифрувати текст декількома методами або ж надавати інший додатковий функціонал.

Дана дипломна робота не охоплює всіх методів шифрування тексту оскільки в криптології їх значно більша кількість а засоби їх розробки мають досить широкий аспект вибору мов та середовищ програмування, деякі з яких дозволяють шифрувати повідомлення лише з допомогою підключення відповідних бібліотек.

СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов / М.В. Адаменко. – М.: ДМК Пресс, 2012. –. 243 с.
2. Бабаш А. В. Криптография / А. В. Бабаш. – М.: СОЛОН-Пресс, 2007. – 312 с.
3. Маховенко Е. Б. Теоретико-числовые методы в криптографии / Е. Б. Маховенко. – М.: Гелиос АРВ, 2006. – 254 с.
4. Мухачев В.А. Методы практической криптографии / В.А. Мухачев, В.А. Хорошко. – К.: ООО Полиграф-Консалдинг, 2014. – С. 138.
5. Розвинення криптології та її місце в сучасному суспільстві / М.В. Захарченко, Л.Г. Йона, Ю.В. Щербина, О.В. Онацький – Одеса: ОНАЗ ім. О.С. Попова, 2004. – 84 с
6. [Електронний ресурс]: Вікіпедія Шифр ADFGVX https://uk.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_ADFGVX
7. [Електронний ресурс] Основные понятия для начинающих Шифрованиеhttp://www.netcode.ru/cpp/?artID=4010courses/408/lecture/9355?page=4
8. [Електронний ресурс] Традиционные шифры с симметричным ключом https://www.intuit.ru/studies/courses/552/408/lecture/9355?page=4
9. [Електронний ресурс] Классический криптоанализ https://habr.com/ru/post/271257/
10. [Електронний ресурс] Основи інформаційної безпеки https://studfile.net/preview/6012701/page:1/
11. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навчальний посібник. – Вінниця ВНТУ, 2009 – 268 с.