Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Якушев Юрій Андрійович,
студент групи РЗ-181

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

Розробка алгоритму захисту особистих повідомлень в месенджерах

Спеціальність:
125 Кібербезпека

Спеціалізація, освітня програма:
Кібербезпека

Керівник:
Лебедєва Олена Юріївна
к.т.н., доцент

Одеса – 2022

Міністерство освіти і науки України
Національний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КБПЗ

_____
д.т.н.,проф. А.А.Кобозєва
____
_____202_р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Якушеву Юрію Андрійовичу

1.Тема роботи: *Розробка алгоритму захисту особистих повідомлень в месенджерах,*

керівник роботи *Лебедєва Олена Юріївна, к. ф.-м. н., доцент,*

затверджені наказом ректора від „17” 05. 2022 р. №168-в.

2. Зміст роботи: *огляд методів та засобів спілкування людей та захисту інформації в месенджерах, огляд методів шифрування даних, розробка та програмна реалізація алгоритму шифрування, який імітує роботу пристрою Базері.*

3. Перелік ілюстративного матеріалу: *циліндр Базері, робоче вікно програми, зашифроване повідомлення, варіанти розшифрованного повідомлення.*

4. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
Охорона праці	к.т.н, доцент Ярова І.А	Завдання видав	Завдання рийняв

5. Дата видачі завдання "_____"_____20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз джерел з теми випускної кваліфікаційної роботи*	*15.11.2021*	*виконано*
2	*Обґрунтування вибору рішення. Збір даних*	*15-12-2021*	*виконано*
3	*Аналіз методів та засобів спілкування людей та захисту інформації в месенджерах*	*11-01-2022*	*виконано*
4	*Аналіз методів шифрування даних*	*20-02-2022*	*виконано*
5	*Розробка та програмна реалізація алгоритму шифрування*	*30-03-2022*	*виконано*
6	*Підготовка тексту роботи*	*05-05-2022*	*виконано*
7	*Підготовка презентації та доповіді*	*31-05-2022*	*виконано*
8	*Попередній захист*	*02-06-2022*	*виконано*
9	*Нормоконтроль, рецензування*	*20-06-2022*	*виконано*

Здобувач вищої освіти _____ *Якушев Ю.А.*

Керівник роботи _____ *Лебедєва О.Ю.*

ЗАВДАННЯ

на розробку розділу «Охорона праці» у кваліфікаційній роботі бакалавра

студенту Якушеву Ю.А.

Інститут Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра Кафедра кібербезпеки та програмного забезпечення

Дата отримання завдання 09.06.2022
Консультації 09.06.2022
Дата закінчення розділу 14.05.2022

Тема роботи «Розробка алгоритму захисту особистих повідомлень в месенджерах»

Зміст розділу (перелік питань, які потрібно розробити)

1. Аналіз умов праці і вибір основних заходів виробничої безпеки.
2. Аналіз пожежної безпеки. Вибір заходів та засобів пожежної безпеки.

Керівник кваліфікаційної роботи

_____ Лебедєва О.Ю.
(підпис) (прізвище та ініціали)

« __ » _____2022 р.

Консультант з охорони праці

_____ Ярова І.А.
(підпис) (прізвище та ініціали)

« __ » _____ 2022 р.

АНОТАЦІЯ

Кваліфікаційна робота на тему «Розробка алгоритму захисту особистих повідомлень в месенджерах» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, спеціалізація Кібербезпека, освітня програма: Кібербезпекою, містить 6 рисунків, 1 таблицю, 1 додаток, 24 літературних джерела за переліком посилань. Робота виконана на 63 сторінках загального тексту і 47 сторінках основного тексту.

Метою даної роботи є захист інформації в месенджерах шляхом розробки алгоритму шифрування, який емулює дискові операції Базері.

У цій роботі розглядаються методи та засоби обміну інформацією та захисту інформації в месенджерах. Наведено основні поняття шифрування даних, класифікації шифрів та шифрувальних машин.

За результатами кваліфікаційної роботи розроблено та програмно реалізовано алгоритм шифрування, що імітує дискові операції Базері.

Результати даної роботи можуть бути використані будь-якою особою з метою захисту своїх повідомлень у месенджерах.

ШИФРУВАННЯ ДАНИХ, ДИСК БАЗЕРІ, ЗАХИСТ ІНФОРМАЦІЇ, PYTHON.

ANNOTATION

Qualification work on "Development of an algorithm for the protection of personal messages in messengers" for the first (bachelor's) level of higher education in 125 Cybersecurity, specialization Cybersecurity, educational program: Cybersecurity, contains 6 figures, 1 table, 1 appendix, 24 references. list of links. The work is performed on 63 pages of general text and 47 pages of main text.

The aim of this work is to protect the information in messengers by developing an encryption algorithm that emulates Baser disk operations.

This paper considers methods and means of information exchange and information protection in messengers. The basic concepts of data encryption, classification of ciphers and encryption machines are given.

Based on the results of the qualification work, an encryption algorithm that simulates Bazer disk operations was developed and implemented.

The results of this work can be used by anyone to protect their messages in messengers.

DATA ENCRYPTION, DISK BASERI, INFORMATION PROTECTION, PYTHON.

ЗМІСТ

ВСТУП

На сьогоднішній день технології стали основоположною сучасного світу, впевнено зайнявши всі людські сфери діяльності, сформував новий інформаційний простір.

Широкі та зростаючі можливості мобільних пристроїв, планшетів, персональних комп'ютерів, смартфонів, розвиток мобільних операційних систем та різноманітних послуг, які вони надають, а також засобів зв'язку в межах відносно обмежених апаратних ресурсів викликають занепокоєння щодо безпеки.

У контексті соціальної інформатизації захист персональної інформації привертає велику увагу. Сьогодні можливий доступ до інформації, що передається через мобільні мережі. Залишаються питання щодо можливості отримання даних від популярного месенджера, розробники якого оголосили суворі правила захисту особистої інформації.

Загальні занепокоєння щодо безпеки та посилення конкуренції серед месенджерів змусили розробників застосувати додаткові засоби захисту, такі як наскрізне шифрування даних, що передаються. Шифруються не тільки текстові повідомлення, а й аудіо та відео. Але повідомлення які ми безпосередньо бачимо у додатку доступні для читання любому, хто візьме наш пристрій.

На сьогоднішній день дуже важливо дати можливість користувачам месенджерів шифрувати свої повідомлення таким чином, як користувач вважатиме за потрібним. Тому тема роботи є актуальною.

Метою даної роботи є захист особистих повідомлень в месенджерах шляхом розробки алгоритму шифрування, який імітує роботу пристрою Базері.

Для досягнення мети в роботі поставлені такі задачі:

– огляд методів та засобів спілкування людей та захисту інформації в месенджерах;

– огляд методів шифрування даних та розробка алгоритму шифрування, який імітує роботу пристрою Базері;

– програмна реалізація розробленого алгоритму шифрування.

Під терміном месенджер будемо розуміти відношення до системи обміну повідомленнями в режимі реального часу через Інтернет і пов’язане програмне забезпечення.

Об’єктом дослідження є захист інформації в месенджері.

Предметом дослідження є методи шифрування повідомлень користувача в месенджері.

Джерелами інформації, що використовуються, є праці провідних вчених у галузі дослідження, нормативно-правові документи, навчально-методична література, журнали, Інтернет-джерела.

Для написання випускної кваліфікаційної роботи були задіяні такі програмні продукти, як бібліотека Tkinter для створення користувацького інтерфейсу, мова програмування Python для створення скриптів.

Практична цінність роботи полягає у розробці алгоритму шифрування, який імітує роботу шифру Базері, та його програмна реалізація, яка може бути використана з метою захисту повідомлень у месенджерах.

1 ОГЛЯД МЕТОДІВ ТА ЗАСОБІВ СПІЛКУВАННЯ ЛЮДЕЙ ТА ЗАХИСТУ ІНФОРМАЦІЇ В МЕСЕНДЖЕРАХ

1.1 Огляд сучасних способів спілкування людей

Спілкування – обмін інформацією за допомогою слів або жестів та інших засобів контакту. Спілкування – це комунікативна взаємодія між людьми або соціальними групами. У процесі спілкування між учасниками спілкування відбувається обмін різноманітною інформацією [1].

При спілкуванні через листи та телефони також відбувається взаємний обмін інформацією та емоціями між реальними людьми.

SMS – це послуга для надсилання текстових повідомлень довжиною до 160 символів з одного телефону на інший. Деякі моделі телефонів дозволяють вводити довший текст і автоматично розділяти його на кілька повідомлень. Ви можете не тільки надсилати SMS-повідомлення користувачам Інтернету з іншого телефону. Існує багато способів обміну інформацією між стільниковими терміналами та користувачами різних Інтернет-послуг. Спеціальні веб-сторінки, ймовірно, є одним із найпростіших способів надсилання коротких повідомлень. Вони містять поля для введення кодів мережі, ідентифікатора абонента, тексту повідомлення, лічильників символів та параметрів переадресації. Надсилання текстових повідомлень із таких сайтів зазвичай безкоштовне [2].

Взаємодія між WWW і SMS-сервісом не така проста. Здебільшого це стосується поштових та мобільних органайзерів. Основним недоліком є відсутність підтримки операторів, більшість сайтів працюють лише з одним або двома, а не з усіма існуючими операторами в Україні. Системні затримки повідомлень зазвичай виникають на поштовому шлюзі оператора. Несвоєчасне надходження SMS зробило його майже марним, а кількість інформації в пошті значно зменшилася. Оператори намагаються захистити своїх клієнтів від спаму, блокуючи деякі технології, які використовуються в комунікації [2].

Сьогодні методи електронного спілкування стають все більш поширеними. Характеризується відсутністю прямого фізичного контакту. Тому без візуальних зображень на електронних носіях значна частина інформації, яку повідомляють невербальні сигнали, втрачається. Крім того, в цьому спілкуванні є анонімність: спілкуючись з людьми через Інтернет, ви можете не знати справжнього імені, статі та віку, національності та віросповідання співрозмовника. Він ніби нічого не знає один про одного. Щоб спілкування було анонімним, його учасники використовують псевдоніми — так звані ніки. Основним способом спілкування був і залишається обмін текстовими повідомленнями. Оскільки емоції в звичайних текстах довго і важко передати, а такі тексти не завжди сприймаються однозначно, з часом з’являється маркер, що вказує на емоційне забарвлення тексту — смайлики.

Електронна пошта – ця форма обміну повідомленнями продемонструвала здатність спілкуватися через Інтернет і є найпоширенішим методом комп’ютерного спілкування. Електронна пошта дуже схожа на звичайну пошту, за винятком того, що лист доходить до одержувача майже відразу після його відправлення. Часто програми електронної пошти також підтримують такі функції, як списки розсилки. Якщо група людей зі спільними інтересами хотіла довго обговорювати тему, вони створювали список, давали йому назву, а потім усі повідомлення на це ім’я надсилалися всім учасникам групи.

Соціальна мережа (соцмережа) – онлайн-платформа, яку використовують для спілкування, створення соціальних відносин з іншими людьми, які мають схожі інтереси або офлайн-зв'язки.

Соціальні мережі використовуються рекламодавцями тому, що в системі є рекламні інструменти, за допомогою яких можна показувати рекламу найбільш релевантним для них людям, а також інструменти для просування особистих брендів; деякі соціальні мережі надають інструменти для створення майже повноцінних інтернет-магазинів. та формування

громадської думки Інструмент.

Інтерактивна бесіда (чат) – це відкрита дискусійна група в Інтернеті, де ви можете спілкуватися з іншими людьми в режимі реального часу, використовуючи псевдонім. Чатам і групам чату часто призначаються імена на основі тем або вікових груп. Багато користувачів можуть брати участь в обговореннях, але зазвичай між двома користувачами відбувається особисте спілкування.

Форум (web - forum) – це спеціальний сайт, або розділ на сайті чи порталі, для спілкування та обміну ідеями. Повідомлення користувачів на форумі згруповані за темами, як правило, першим повідомленням. Усі відвідувачі можуть побачити тему та опублікувати свої повідомлення у відповідь на написане. Як правило, теми поділяються на тематичні форуми, а системою керують адміністратори та модератори.

Блог – це інформаційний веб-сайт або онлайн-журнал, який відображає останні публікації у верхній частині сторінки. У цих сервісах кожен учасник має свій журнал, тобто залишає записи в хронологічному порядку. Записаним предметом може бути будь-який предмет. Найпоширеніший спосіб – використовувати блог як власний журнал. Інші відвідувачі можуть коментувати допис автора. При цьому користувач, крім ведення власного щоденника, має можливість організувати стрічку – список записів з журналу «друзі», регулювати доступ до записів, знаходити зацікавлених співрозмовників. На основі такої системи створювалися журнали, керовані колективом громад. Будь-який учасник такої спільноти може опублікувати повідомлення про напрямок спільноти.

Google Talk – це пакет програмного забезпечення для обміну миттєвими повідомленнями, розроблений компанією Google. Він складається з клієнта миттєвого обміну повідомленнями Google Talk та модулів голосового та відеочату. Google Talk дозволяє спілкуватися за допомогою голосового чату та текстових повідомлень. Він тісно інтегрований з Gmail.

Skype – це інструмент спілкування в реальному часі, розроблений

Skype Limited. Програма дозволяє спілкуватися особисто, обмінюватися повідомленнями з іншими користувачами (чат), передавати файли (Word, Excel, Power Point тощо), організовувати спілкування з групою користувачів.

1.2 Месенджери та їх призначення

Месенджер – це програма, мобільний додаток або веб-сервіс для обміну миттєвими повідомленнями. У більшості випадків під месенджером розуміють програму, в якій записують та читають повідомлення. За кожною такою програмою стоїть мережа передачі повідомлень, яка також є частиною концепції «месенджера». Це може бути мережа всередині компанії або глобальна мережа.

Коли повідомлення шифруються на телефоні, а розшифровуються на телефоні співрозмовника це називається end-to-end шифрування.

Символ – це будь-який символ, включаючи літери, цифри або розділові знаки. Текст – це впорядкований набір символів алфавіту. Алфавіт - обмежений набір символів, що використовуються для кодування інформації.

Месенджер замінив SMS-повідомлення як альтернативу голосовим дзвінкам, тому що тепер вам не потрібно поповнювати телефон – ви можете використовувати програму під час підключення до Wi-Fi, тобто вам не потрібен мобільний Інтернет на телефоні. У цьому випадку повідомлення та дзвінки будуть необмеженими та безкоштовними.

Facebook Messenger – програма для обміну миттєвими повідомленнями та відео, створена Facebook. Він інтегрується з системою обміну повідомленнями на головному сайті Facebook (Facebook Chat) і заснований на відкритому протоколі MQTT. У Facebook Messenger ви можете відкласти повідомлення. Іноді хочеться просто відпочити від прикрих новин, іноді це необхідно, щоб не відволікати від невідкладної роботи. У месенджері можна відключити всіх співрозмовників або деякі особливо дратівливі повідомлення.

Щоб зробити миттєві повідомлення приватними, ми рекомендуємо

вимкнути розділ попереднього перегляду повідомлення/повідомлення. За замовчуванням Messenger відображає текст повідомлень, отриманих користувачами, у рядку стану. Однак це не завжди зручно, якщо на дзвінок відповідає хтось іншийTelegram хороший як текстовий месенджер, на який цілком можна покладатися для оперативного зв'язку з групою друзів.

Telegram має простий, іноді примітивний і недружній для всіх інтерфейс, але за ним стоїть сила тематичних каналів і ботів, які приваблюють користувачів.

Крім особистих чатів, у Telegram також є групи для приватних розмов з друзями чи колегами. Супергрупи (до 5000 осіб) збирають повідомлення та інструменти модерації, необхідні в публічному чаті.

Telegram розробляє свій API для ботів, і їх стає все більше. Кожен бот також має ім’я користувача, щоб його можна було знайти в глобальному пошуку. Черевики діляться на дві категорії – звичайні та вбудовані. Вони безпосередньо взаємодіють із звичайними ботами, надсилаючи текст (наприклад, пошукові запити) звичайним ботам або команди, надані розробниками. Вбудовані боти можуть отримувати команди з інших чатів.

У Telegram є функція захисту чатів паролем. Ця функція дозволяє приховати листи від сторонніх очей. Це корисно, якщо ви випадково залишите свій смартфон розблокованим. Список чату неможливо відкрити навіть без коду підтвердження. Функція називається «Код пароля» і доступна в налаштуваннях конфіденційності та безпеки. Після створення чотиризначного пароля в списку чату вгорі потрібно натиснути значок замка. Потім можна згорнути програму або вимкнути екран смартфона. Цей пароль вам знову знадобиться, коли ви спробуєте відкрити Telegram.

1.3 Види атак, методи та засоби захисту інформації в месенджерах

Атака на інформаційну систему — це свідомий комплекс дій зловмисника, спрямованих на порушення однієї з трьох властивостей інформації — доступності, цілісності чи конфіденційності.

Існує багато видів хакерських атак, і вони доповнюються та вдосконалюються в міру розвитку технологій. Важливо визначити основні типи файлів cookie, які найчастіше використовуються [7].

Переповнення буфера є одним з найпоширеніших видів атак в Інтернеті. Принцип цієї атаки заснований на використанні програмних помилок, які дозволяють порушувати ліміти пам'яті та аварійно завершувати роботу програм або виконувати довільний двійковий код від імені користувача, який запускає вразливу програму. Якщо програма запускається під обліковим записом системного адміністратора, атака отримає повний контроль над комп’ютером жертви, тому рекомендується запускати під обліковим записом користувача з обмеженими системними привілеями та виконувати операції, які вимагають лише адміністративних прав під обліковим записом системного адміністратора.

Віруси є найпопулярнішим видом злому. Трояни, поштові хробаки, сніфери – кожен вірус може вразити комп’ютерну систему, а мета вірусу – передати таємну інформацію від гаджетів до хакерів.

DoS (відмова в обслуговуванні) - атака, призначена для того, щоб змусити сервер не відповідати на запити. Цей тип атаки не передбачає отримання певної конфіденційної інформації, але іноді корисно запустити інші атаки.

DDoS (Distributed Denial of Service) – має те ж призначення, що і DoS, але не з одного комп’ютера, а з кількох комп’ютерів у мережі. Ці типи атак використовують помилки, які призводять до збою послуг або запускають захист, який блокує послуги і, таким чином, забороняє обслуговування.Розглянемо атаковані месенджери, та типи цих атак.

Співробітники WhatsApp виявили вразливість у системі безпеки під час тестування Messenger у середині 2019 року [8]. Зловмисники використовують переповнення буфера повідомлень, щоб запровадити шкідливе програмне забезпечення в телефон або інший пристрій користувача, зробивши один голосовий виклик. Представник WhatsApp не уточнив, яке шкідливе

програмне забезпечення було встановлено через помилку месенджера, але зазначив, що це дозволило зловмиснику відстежувати переміщення користувача за допомогою камери та мікрофона його гаджета.

Зараз WhatsApp користується 1,5 мільярдами людей у всьому світі, і компанія поки не знає, скільки людей насправді постраждало від помилки Messenger. Однак у компанії виключили, що це явище може бути масштабним – швидше за все, цілеспрямованою атакою на конкретну групу людей.

У 2016 році іранським хакерам вдалося ідентифікувати номери телефонів близько 15 мільйонів людей у країні, які використовували Telegram Messenger. Крім того, хакерам вдалося отримати доступ до акаунтів десятків журналістів та активістів. Telegram відповів на інформацію про злом і повідомив, що хакери мали доступ лише до публічної інформації, але не до самих акаунтів. Розробники стверджують, що хакери лише перевіряли, чи зареєстровані в Telegram певні іранські номери. У результаті їм вдалося підтвердити існування акаунтів Telegram 15 мільйонів користувачів.

Також у 2019 році Telegram Messenger вийшов з ладу через злом серверів компанії [10]. Невідомі атакували сервери компанії, намагаючись їх перевантажити (DDoS-атака). У компанії заявили, що це не повинно призвести до витоку персональних даних користувачів.

Кожен зловмисник мріє отримати персональні дані громадян. При цьому часто використовуються соціальні мережі та месенджери, незалежно від того, яка інформація надається співрозмовнику і чи буде вона використана в особистих цілях третіх осіб. Щоб уникнути витоку інформації, слід використовувати наскрізне шифрування даних. Наприклад, Viber Messenger використовує такий тип захисту, тому ключ доступу зберігається виключно на пристрої співрозмовника. Це означає, що треті сторони не можуть отримати доступ до інформації без доступу до пристрою. Цей вид захисту дуже популярний серед компаній, оскільки вважається одним з найнадійніших у світі.

Основне завдання хакера – зламати систему та отримати інформацію. Наше головне завдання – не допустити цього. Є кілька важливих підказок [7, 11]:

- використовуйте захищену мережу, безпечні паролі, перевіряйте торгові сайти, ніколи не зберігайте дані картки в онлайн-рахунках, перевіряйте транзакції щотижня;
- використовуйте більш складний пароль. Якщо пароль 12345, то професійному хакеру зламати комп'ютер не складе труднощів. Слід використовувати більш складне шифрування, наприклад, великі та малі літери в словах, цифри та літери, довгі фрази паролів. Також пароль не варто розкривати нікому, навіть знайомим;
- ніколи не залишайте свій ноутбук або смартфон розблокованими на тривалий період часу. Навіть якщо ви залишитеся лише на кілька хвилин і залишите свій гаджет доступним, у професійних хакерів буде достатньо часу, щоб завантажити всю інформацію або пошкодити систему;
- не використовуйте повторювані паролі. Це означає використання пароля 12345 і пароля 54321 в іншій системі – поганий вибір;
- не підключайтеся до загальнодоступного Wi-Fi. Соціальні мережі не завжди захищені паролем і іноді вимагають реєстрації та входу. Але деякі мережі відкриті для всіх користувачів без додаткових дій. Хакери можуть створювати дублікати мереж з однаковою назвою і перехоплювати дані.

Огляд сучасних засобів зв'язку та методів захисту інформації виявив:

- останніми роками все більш поширеними стали методи спілкування електронними засобами (месенджером);
- найпопулярнішими засобами комунікації в Україні є Viber, Facebook Messenger, Telegram;
- приховати вміст спілкування в месенджері за допомогою таких

функцій, як прихований чат, перевірка контактів, захист паролем чату, наскрізне шифрування даних тощо;

- messenger не надає таких функцій, як створення зашифрованих повідомлень на випадок, якщо користувач не хоче, щоб ці повідомлення читали інші люди (навіть родичі чи члени сім'ї).

2 ШИФРУВАННЯ ДАНИХ В МЕССЕНДЖЕРАХ

2.1 Загальні поняття шифрування даних

Криптографія в перекладі з грецької означає «тайнопис». В даний час криптографія шукає і вивчає математичні методи перетворення інформації. Поряд з криптографією розвивається і вдосконалюється криптоаналіз – наука про подолання криптографічного захисту інформації. Криптоаналітики досліджують можливість розшифровки інформації, не знаючи ключа. Успішний криптоаналіз дозволяє отримати або ключ шифрування, або відкритий текст, або обидва. Криптографія і криптоаналіз часто об'єднуються в єдину науку - криптографію (kryptos - секрет, logo - наука), яка займається проблемою оборотного перетворення інформації для запобігання несанкціонованому доступу, оцінкою надійності криптографічних систем і аналізом міцності шифру.

Сьогодні криптографія швидко увійшла в наше життя. Розглянемо сферу застосування криптографії в сучасному інформаційному суспільстві [12]:

- шифрування даних, що передаються через відкриті канали зв'язку (наприклад, під час покупок в Інтернеті, інформації про транзакції, адреси, номери телефонів, номери кредитних карток, зазвичай зашифровані з метою безпеки);
- обслуговування банківських пластикових карток;
- зберігати та обробляти паролі користувачів у мережі;
- подавати бухгалтерську та іншу звітність через дистанційні канали зв’язку;
- надавати банківські послуги підприємствам через локальні або глобальні мережі;
- захищає сховище на жорсткому диску вашого комп’ютера від

несанкціонованого доступу (Windows навіть має спеціальний термін шифрована файлова система (EFS)).

Історія криптографії налічує близько чотирьох тисяч років. Основними критеріями криптографічної постановки можуть служити технічні характеристики використовуваних методів шифрування. За стадією розробки вона поділяється на три етапи розвитку [13]: перший етап – етап донаукової криптографії (до 1949 року); другий етап – етап наукової криптографії з використанням ключів (з 1949 по 70-ті роки); третій етап – етап наукової криптографії з використанням ЕОМ (з сімдесятих років до сьогодення).

Розглянемо основні поняття криптографії.

Шифрування – це процес шифрування набору відкритого тексту в набір закритого (зашифрованого) тексту. Дешифрування – це процес криптографічного перетворення закритого повідомлення у відкрите. Дешифрування – це процес пошуку відкритого повідомлення, що відповідає даному закритому повідомленню, за допомогою невідомого криптографічного перетворення.

Шифр – заздалегідь визначений набір методів для перетворення оригінального секретного повідомлення для його захисту. Вихідні повідомлення часто називають відкритим текстом. У зарубіжній літературі для відкритого тексту використовується термін відкритий текст.

Шифри, які використовуються на перших етапах розвитку криптографії, класифікуються так: шифри перестановки, заміни, гамування, шифрування аналітичним перетворенням.

Шифрування перестановки – це перегрупування символів відкритого тексту в блоці тексту за певними правилами. При достатній довжині блоків, в яких виконується перестановка, і складному унікальному порядку перестановки може бути досягнута криптографічна стабільність, прийнятна для простих практичних застосувань.

Шифрування гамування – це те, коли символи відкритого тексту складаються із символів деякої випадкової послідовності, яка називається

гамою шифру. Стабільність шифрування в основному залежить від довжини (періоду) неповторюваної частини гамми шифру.

Шифри підстановки виконують перетворення, у яких літери або інші сегменти відкритого тексту замінюються відповідними сегментами зашифрованого тексту.

При заміні символи відкритого тексту замінюються іншими символами. Система заміни заснована на ідеї алфавіту шифру – списку еквівалентів, які використовуються для перетворення відкритого тексту в шифрування. Іноді зашифрований текст включає кілька замін символів. Цей вибір називається гомофоном. Іноді зашифрований текст містить безглузді символи [14].

Якщо використовується лише один зашифрований текст, система заміни називається однобуквеною системою заміни. Але коли за певними правилами використовуються дві чи більше літер шифру, система заміни стає багатоалфавітною.

В якості алфавітів можна використовувати такі:

- алфавіт Z26 – 26 літер англійського алфавіту;
- алфавіт Z33 – 33 літери українського алфавіту;
- алфавіт Z256 – символи, що входять в стандартні коди ASCII та КОИ-8;
- бінарний алфавіт $Z2 = \{0,1\}$.
- алфавіт використаний в програмі Z40 – 26 літер англійського алфавіту,10 цифр та 4 знаки пунктуації.

У системі заміни слід розрізняти коди та паролі. Код складається з тисяч слів, фраз, букв і складів і відповідних їм кодових слів або кодових символів, які замінюють ці елементи відкритого тексту. По суті, код являє собою гігантський код заміни, де основними одиницями відкритого тексту є слова та фрази. У паролі основною одиницею є символ, а іноді і пара символів.

Шифрування аналітичним перетворенням полягає в тому, що відкритий текст перетворюється за певним аналітичним правилом, формулою.

Колекція, з якої вибираються ключі, називається простором ключів. Набір процесів шифрування, набір відкритих повідомлень, набір можливих закритих повідомлень і простір ключів називають алгоритмами шифрування. Сукупність процесів дешифрування, набір можливих закритих повідомлень, набір відкритих повідомлень і простір ключів називають алгоритмом дешифрування.

Величезний вплив на розвиток криптографії мають досягнення науково-технічного прогресу. Наприклад, у середині дев’ятнадцятого століття після винаходу телеграфу з’явилося кілька дипломатичних і комерційних шифрів, які зосереджені на використанні телеграфу. Збільшення швидкості передачі даних вимагає збільшення швидкості шифрування. Механічні кодери Т. Джефферсона і Ч. Вітстона з'явилися наприкінці XIX ст. З кінця XIX століття криптографія стала серйозною галуззю наукового знання і стала вивчатися як самостійна наука у військових академіях.

Існують різні підходи до класифікації шифрів:

- за методом шифрування – шифри заміни та шифри перестановки;
- за технологією шифрування – блокові шифри та потокові шифри;
- за особливостями ключів – симетричні шифри та асиметричні

У блоковому шифрі метод шифрування застосовується до блоку простого тексту з певним розміром (кількістю символів).

У потоковому шифрі метод шифрування застосовується до кожного символу відкритого тексту окремо.

Якщо для шифрування та дешифрування повідомлення використовується той самий алгоритм і той самий ключ, цей метод шифрування називається симетричним шифруванням. Цей єдиний ключ має бути секретним і відомим лише відправнику та одержувачу повідомлення. Тому ці методи ще називають шифрами з одним ключем або шифрами з секретним ключем. Симетричні шифри характеризуються нерозв'язною проблемою, а саме складністю передачі ключа користувачеві, і

неможливістю перевірити справжність отриманого користувачем ключа.

Якщо алгоритми шифрування і дешифрування різні, і якщо використовуються два ключі – один для шифрування, а інший для розшифровки повідомлення, то такий метод шифрування називається асиметричним шифруванням. Його характерна особливість – один із ключів секретний, а інший відкритий. Тому асиметричні методи шифрування називаються шифрами з подвійним ключем або шифрами з відкритим ключем.

Роботу системи засекреченого зв'язку можна описати таким чином:

- з ключового простору вибирається ключ шифрування K та відправляється по надійному каналу передачі;
- до відкритого повідомленням C, призначеному для передачі, застосовують конкретне перетворення Fk, яке визначається ключем K, для отримання зашифрованого повідомлення M: M = Fk(C);
- отримане зашифроване повідомлення M пересилають по каналу передачі даних;
- на приймаючій стороні до отриманого повідомленням M застосовують конкретне перетворення Dk, яке визначається з усіх можливих перетворень ключем K, для отримання відкритого повідомлення C: C = Dk(M).

Основною характеристикою шифру є те, що він зашифрований, що визначає його стійкість до криптоаналітичного розкриття. Зазвичай ця функція визначається інтервалом часу, необхідним для відкриття пароля.

Поліморфізм є відносно розвиненою практикою в криптографії, яка часто використовується в комп'ютерному шифруванні. Поліморфне перетворення – це техніка, яка незалежно модифікує криптографічний алгоритм після кожного виконання, так що після кожної ітерації отримують різні результати. Тобто, якщо вам потрібно двічі зашифрувати одну й ту саму інформацію, алгоритм видасть різні зашифровані тексти.

2.2 Шифрувальні машини

Людям завжди потрібно було таємно спілкуватися, тому шифрування не стоїть на місці. Оскільки деякі паролі розкриваються, інші є більш стабільними. Паперові паролі були замінені криптографічними машинами, які не мають собі рівних для людей. Навіть досвідчені математики не можуть зламати шифри, обчислені на обертових машинах.

Шифрувальні машини можна розділити на дві категорії: механічні; ротаційні.

Одним із ключових винаходів, що дозволили створити багато криптографічних машин, був винахід так званого ротора. Це електромеханічний компонент, що складається з корпусу з бакелітових або металевих дисків, всередині якого розміщені дроти, з'єднані попарно, не обов'язково в звичайному порядку, але бажано в якомусь таємному порядку, в роторі Сторони контактів. контактів відповідає кількості літер в алфавіті. Ротори можуть бути певною комбінацією всередині шифруючої машини і рухатися незалежно або незалежно один від одного.

Приблизно в той же час, у 1920-х роках, ротор був винайдений різними авторами в різних країнах, які використовували його у своїх шифрувальних машинах. До них належать Едвард Хеберн, автор машини Хеберна зі Сполучених Штатів, Артур Шербіус, ймовірно, автор найвідомішої шифруючої машини Німеччини «Енігма», і Арвід Дамм, автор шифрувальної машини Дамма, хоча і не обертається, але засновник знаменита шведська компанія Hagelin А разом виготовляє машини для шифрування. У Німеччині та інших країнах на основі роторів створено багато шифрувальних машин.

Ідея такої системи полягає в тому, що після шифрування кожного символу внутрішній стан машини змінюється, навіть той самий символ, знову виведений з клавіатури, і більшість цих машин шифруються абсолютно різними символами.

Електричний сигнал проходить через ротор і замикає електричне коло,

наприклад, до лампочки. Альтернативою цій системі є так звана система «штифт і виступ», яка використовується для механічних машин, які не потребують електроенергії.

Леон Баттіста Альберті, італійський вчений, який працює у Ватикані, написав книгу про шифри, в якій описав шифри заміни, використовуючи два концентричних кола: (зовнішній) відкритий текстовий алфавіт, інший (внутрішній) - алфавіт шифротексту. Його пристрій, два концентричних кола, був одним із перших механічних пристроїв шифрування, в якому використано метод заміни літер вихідного тексту. Ключем до цього шифру є порядок букв на диску та початкове положення внутрішнього диска відносно зовнішнього диска [15].

Цей метод забезпечує можливість з’являтися з однаковою частотою в зашифрованому тексті однієї літери. Автори прийняли таке рішення, виходячи з ймовірності ідентифікації вихідного повідомлення за нерівномірним виглядом окремих літер у словах природної мови, тим самим зменшуючи ймовірність несанкціонованої ідентифікації.

Колесо шифрування Bolton – цей пристрій заснований на зашифрованому диску Леона Баттісти Альберті. Пристрій, типовий для дизайну кінця 19 століття, міг просто замінювати одну букву на іншу.

Механізм М-94 використовувався в армії США з 1924 по 1943 рік. Його робота була заснована на принципі роботи шифруючого пристрою XVIII століття, винайденного Томасом Джефферсоном, що складається з кількох обертових дисків, на яких вигравірувано літери та цифри.

Подальшою модифікацією виробу М-94 стала шифрувальна машину М-209, яка була розроблена шведським криптографом Б.Хагеліном в 1934 році за завданням французьких спецслужб.

Циліндр Джефферсона був одним із перших сучасних шифрів, створених Томасом Джефферсоном між 1790 та 1800 роками. Томас Джефферсон називає свою систему шифрування «дисковими шифрами». Він сам не був упевнений у надійності свого винаходу, тому діяв обережно, не

використовуючи його як президент Сполучених Штатів, а продовжуючи використовувати традиційні шифри та шифри. Він підтримував зв'язок з математиком Р. Паттерсеном, щоб той міг проаналізувати винахід. Оскільки Джефферсон не нав'язував свій винахід для використання, він незабаром потрапив в архів. До двадцятого століття, коли його знову згадали, він був визнаний дуже стійким до криптоаналітичних пристроїв шифрування, а самого Джефферсона називали «батьком американського шифрування».

Циліндр Базери був створений на основі дуже простого принципу, 20 дисків із буквами, надрукованими у випадковому порядку, у певній послідовності ключів на одній осі, обертаються, доки перші 20 літер повідомлення не будуть введені в один рядок, потім зчитують шифрування з іншого рядка, також визначають ключ і повторюють . Майже всі шифрувальні машини до Другої світової війни були створені на основі цього принципу (рисунок 2.1).

Рисунок 2.1 – Циліндр Базері

2.3 Алгоритм шифрування, який імітує роботу пристрою Базері

Диск Базері – це фізичний пристрій. Для імітації його роботи у вигляді програми необхідно розробити алгоритми шифрування та дешифрування, які далі будуть реалізовані в програмному додатку.

Нехай маємо людей, які хочуть використовувати шифрування за допомогою диска Базері для обміну повідомленнями один одному в якомусь месенджері.

Маємо такі вхідні параметри, необхідні для роботи розробленого алгоритму шифрування:

– кількість дисків для шифрування m;
– кількість символів нанесених на диск n;
– використаний алфавіт A_n;
– випадкові послідовності, що складаються з символів обраного алфавіту, та їх кількість: $a_1, a_2, \dots, a_d$, де $a_i = \{a_i^1, a_i^2, \dots, a_i^n\}$ – символи i-ої послідовності.

Розглянемо основні етапи та кроки розробленого алгоритму.

Етап шифрування даних.

Крок 1. Створюємо порожню матрицю символів $S_{m \times n}$.

Крок 2. Обираємо секретний числовий ключ, який складається з двох чисел A і B де A $\in [1;\ d]$.

Крок 3. Заповнимо матрицю номерів дисків P наступним чином: $A * i + B\ mod(d)$. Маємо $P = \{p_1, p_2, \dots, p_m\}$, де $p_i \in [1;\ d]$.

Крок 4. Заповнимо матрицю символів $S_{m \times n}$ відповідними дисками згідно з обраних номерів з матриці дисків P.

Крок 5. Нехай маємо відкритий текст $X = \{x_1, x_2, \dots, x_m\}$, де x_i – i-ий символ відкритого тексту.

Крок 6. Для кожного символу відкритого тексту виконуємо наступну операцію: пошук x_i символу в i-му рядку матриці. Нехай для кожного символу відкритого тексту маємо індекс його знаходження у відповідному рядку: $\{j_1, j_2, \dots, j_n\}$, тобто символ x_1 знаходиться у першому рядку за індексом j_1, символ x_2 – за індексом j_2 у другому рядку тощо.

Крок 7. Зсуваємо елементи кожного рядка таким чином, щоб в першому стовпці з'явилися букви відкритого тексту:

$$\begin{bmatrix} s_{p_1}^{j_1} & s_{p_1}^{j_1+1} & \dots & s_{p_1}^{j_1-1} \\ s_{p_2}^{j_2} & s_{p_2}^{j_2+1} & \dots & s_{p_2}^{j_2-1} \\ \dots & \dots & \dots & \dots \\ s_{p_m}^{j_n} & s_{p_m}^{j_n+1} & \dots & s_{p_m}^{j_n-1} \end{bmatrix}$$

Крок 8. Генерується випадкове число $k \in [2;\ n]$.

Крок 9. Шифртекст є послідовність символів $\{a_{p_1}^k,\ a_{p_2}^k,\ \dots,\ a_{p_m}^k\}$.

Етап розшифрування даних.

Крок 1. Створюємо порожню матрицю символів $S_{m \times n}$.

Крок 2. Маємо секретний числовий ключ, який складається з двох чисел A і B. Заповнимо матрицю номерів дисків P наступним чином: $A * i + B\ mod(d)$. Маємо $P = \{p_1, p_2, \dots, p_m\}$, де $p_i \in [1;\ d]$.

Крок 3. Заповнимо матрицю символів $S_{m \times n}$ відповідними дисками згідно з обраних номерів з матриці дисків P.

Крок 4. Нехай маємо шифртекст $Y = \{y_1, y_2, \dots, y_m\}$, де y_i – i-ий символ шифртексту.

Крок 5. Для кожного символу шифртексту виконуємо наступну операцію: пошук y_i символу в i-му рядку матриці. Нехай для кожного символу шифртексту маємо індекс його знаходження у відповідному рядку: $\{t_1, t_2, \dots, t_n\}$, тобто символ y_1 знаходиться у першому рядку за індексом t_1, символ y_2 – за індексом t_2 у другому рядку тощо.

Крок 6. Зсуваємо елементи кожного рядка таким чином, щоб в першому стовпці з'явилися букви шифртексту:

$$\begin{bmatrix} s_{p_1}^{t_1} & s_{p_1}^{t_1+1} & \dots & s_{p_1}^{t_1-1} \\ s_{p_2}^{t_2} & s_{p_2}^{t_2+1} & \dots & s_{p_2}^{t_2-1} \\ \dots & \dots & \dots & \dots \\ s_{p_m}^{t_n} & s_{p_m}^{t_n+1} & \dots & s_{p_m}^{t_n-1} \end{bmatrix}$$

Крок 7. Відкритим текстом буде осмислена послідовність символів, яка обирається серед наступних:

$\{s_{p_1}^{t_1},\ s_{p_2}^{t_2},\ \dots,\ s_{p_m}^{t_n}\},\ \{s_{p_1}^{t_1+1},\ s_{p_2}^{t_2+1},\ \dots,\ s_{p_m}^{t_n+1}\},\ \dots,\{s_{p_1}^{t_1-1},\ s_{p_2}^{t_2-1},\ \dots,\ s_{p_m}^{t_n-1}\}.$

Отже, у другому розділу наведено основні теоретичні поняття про шифрування даних. Наведено розроблений алгоритм шифрування даних, який імітує роботу диску Базері.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОГО АЛГОРИТМУ

3.1 Обґрунтування вибору програмного засобу Python

Python — це інтерпретована високорівнева об’єктно-орієнтована мова програмування зі суворою динамічною типізацією. Розроблено Гвідо ван Россумом у 1990 році. Високорівневі структури даних разом з динамічною семантикою та динамічним зв’язуванням роблять його привабливим для швидкої розробки програмного забезпечення, а також способом об’єднання наявних компонентів. Python підтримує модулі та пакети модулів, які сприяють модульності та повторному використанню коду. Інтерпретатор і стандартна бібліотека Python доступні у зібраному та вихідному вигляді на всіх основних платформах. Мова програмування Python підтримує декілька парадигм програмування, включаючи об’єктно-орієнтовану, процедурну, функціональну та аспектно-орієнтовану.

Python має ефективні високорівневі структури даних і простий, але ефективний підхід до об’єктно-орієнтованого програмування. Вільний синтаксис Python, динамічна обробка типів і інтерпретована мова роблять його ідеальним для написання сценаріїв і швидкої розробки додатків у багатьох галузях на більшості платформ.

Інтерпретатор мови Python і багата стандартна бібліотека (вихідні та двійкові дистрибутиви для всіх основних операційних систем) доступні на веб-сайті Python www.python.org і розповсюджуються безкоштовно. Той самий сайт має дистрибутиви та посилання на багато модулів, програм, утиліт та іншу документацію.

Інтерпретатор Python може бути розширений функціями та типами даних, розробленими на C або C++ (або інших мовах, які можна викликати з C). Python також можна використовувати як мову розширення для програм, які потребують подальшого налагодження.

Програмне забезпечення (додатки або бібліотеки) в Python розроблено як модулі, які, у свою чергу, можуть бути зібрані в пакети. Модулі можуть

бути розташовані в каталогах і ZIP-архівах. Модулі можуть бути двох типів: модулі, написані на «чистому» Python, і модулі розширення, написані іншими мовами програмування. Наприклад, стандартна бібліотека має «чистий» модуль pickle та його аналог C: cPickle. Модуль оформлений як окремий файл, а пакет - як окремий каталог. Модулі пов’язуються з програмами через оператор імпорту. Після імпорту модуль представлений окремим об’єктом, який надає доступ до простору імен модуля. Під час виконання програми модуль можна перезапустити за допомогою функції reload().

Python підтримує повну інтроспекцію під час виконання. Це означає, що для будь-якого об’єкта можна отримати всю інформацію про його внутрішню структуру.

Використання інтроспекції (метапрограмування) є важливою частиною так званого «пітонічного стилю» і широко використовується в бібліотеках і фреймворках Python, таких як PyRO, Pyro, PLY, CherryPy, Django тощо, що економить час програмістів на їх використання.

3.2 Опис розробленого додатку

Скрипти потрібні для того, щоб програми виконували певні дії. Скрипти - це логічна команда, яка повідомляє об'єкту, як поводитися в певній ситуації. У більшості випадків в Python всі скрипти можна розділити на три частини. Перша частина полягає в підключенні різних бібліотек, які будуть використовуватися в цьому скрипті. Спочатку цей розділ пов’язує базові бібліотеки, необхідні для керування об’єктами. Друга частина — це підклас сценарію та до якого сценарію він належить. Остання частина — це логіка, задана користувачем.

У програмному коді операції необхідно виконувати над об’єктами різних класів. Описи класів містяться в спеціальних бібліотеках. Бібліотека tkinter містить описи всіх стандартних об’єктів у Python. У бібліотеці є випадкові функції для генерації випадкових чисел, букв, випадкового відбору

мікроелементів.

Для запуску програми запускаємо файл «BAZERI_GUI.py». З’являється вікно з якого починається робота програми (рисунок 3.1).

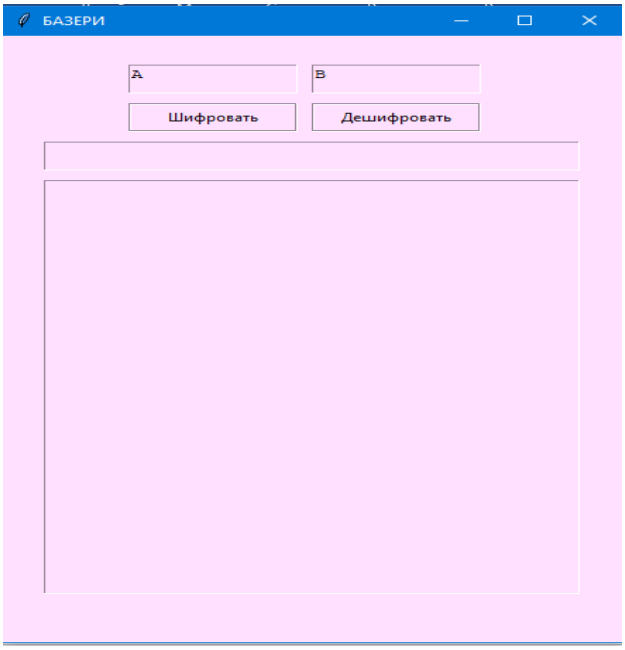

Рисунок 3.1 – Робоче вікно програми

У поле A і B необхідно ввести або скопіювати ключі, які використовуються для випадкового вибору дисків. Поля A та B повинні бути числами, де A повинно бути взаємно простим з числом 100. При вводі ключа який не взаємно простий з A на екрані з’явиться помилка яка сигналізує про некоректно введенні данні (рисунок 3.2).

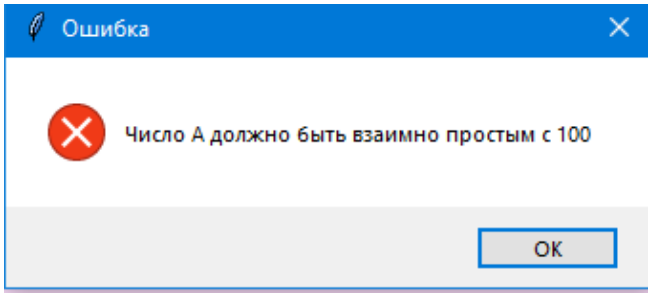

Рисунок 3.2 – Вікно помилки

Диски шифрування вже зашиті в програмі і для правильного вибору дисків для шифрування та дешифрування необхідно знати ключі A та B.

Після того як ключі введені, вводимо данні в поле нижче. Символи які

можна використовувати для шифрування наступні: «'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', ',', '.', ':', '1', '2', '3', '4', '5', '6', '7', '8', '9', '0', ' '». Натисніть кнопку «Шифрувати», і алгоритм шифрування почне працювати.

Результатом шифрування є будь-який інший рядок, утворений диском. Програма генерує випадкове число для використання в якості номера рядка. Рядок є результатом шифрування. У програмі, яка маскує кількість використаних дисків із рядка результату, беремо перші N символів, де N – кількість символів у вхідному повідомленні. Отриманий рядок записується в останнє поле. Цей рядок можна відправити співрозмовнику в месенджері (рисунок 3.3).

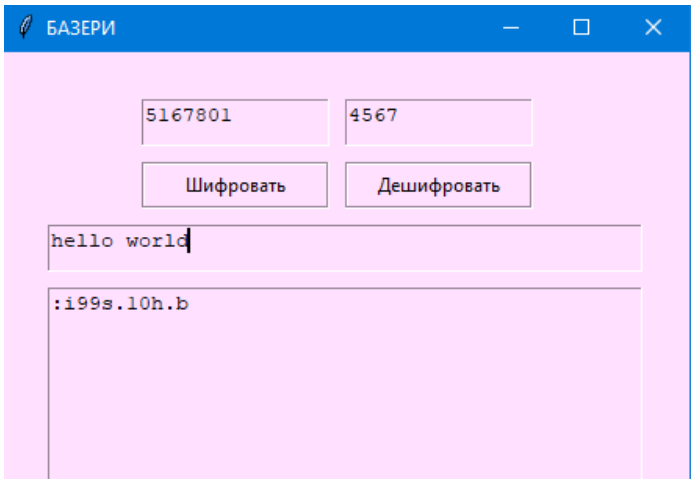

Рисунок 3.3 – Зашифроване повідомлення

При повторному запуску шифрування ми отримуємо інший результат, це пов’язано з тим що при шифруванні вибирається випадковий рядок з усього алфавіту (рисунок 3.4)

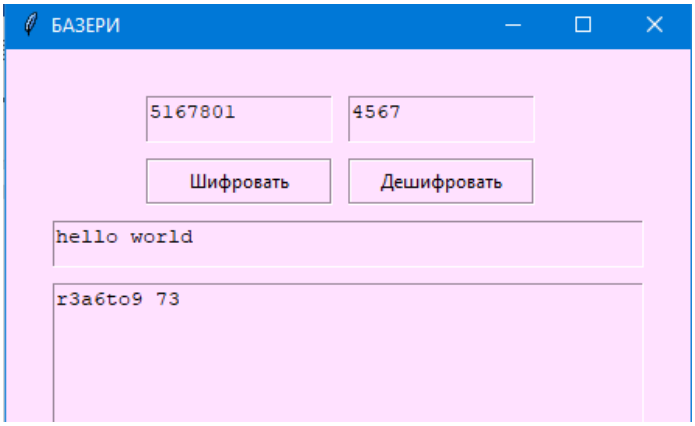

Рисунок 3.4 Повторне шифрування повідомлення

Абонент копіює повідомлення, надіслане тій самій програмі на своєму комп’ютері, у першому полі. Щоб розшифрувати його, потрібно натиснути кнопку «Розшифрувати» та ввести той самий ключ, який використовувався для шифрування. Результатом розшифрування є будь-яка смуга, яка утворює диск (рисунок 3.5).

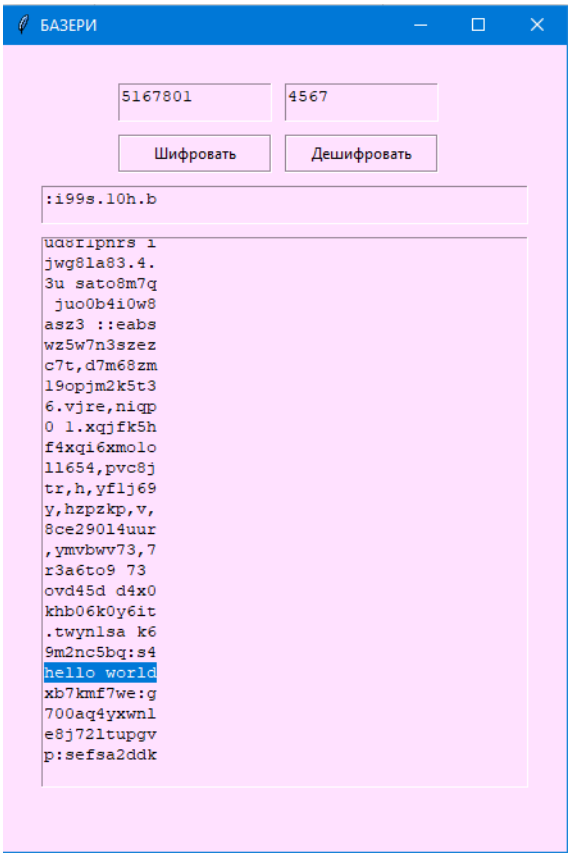

Рисунок 3.5 – Варіанти розшифрованного повідомлення

Тому програма захищає інформацію від заміни автором повідомлення. Тобто кожен раз, коли вона шифрує і розшифровує, програма запитує пароль.

Якщо користувач хоче вийти з комп’ютера, він повинен закрити програму. Якщо незнайомець має доступ до комп’ютера користувача, він не зможе читати зашифровані повідомлення, не знаючи пароля.

Якщо ви не використовуєте шифрування для всіх повідомлень, а лише для більш приватних, ці зашифровані повідомлення будуть виглядати як текст, введений у неправильній розкладці клавіатури ззовні.

4 ОХОРОНА ПРАЦІ

Кваліфікаційна робота присвячена розробці алгоритмів захисту інформації в месенджері. Захист інформації здійснюється за допомогою персонального комп'ютера. Тому предметом дослідження є сучасне робоче місце з персональним комп’ютером (ПК).

Необхідно визначити та проаналізувати набір небезпек гігієнічних технологій та шкідливих виробничих факторів, які впливають на здоров’я користувачів ПК на робочому місці. Аналіз полягає у виявленні факторів ризику та несприятливих наслідків та порівнянні їх фактичних значень з максимально допустимими значеннями, визначеними нормативно-правовими актами: національними стандартами, будівельними нормами, гігієнічними нормами.

На користувачів ПК під час роботи впливають такі небезпечні та шкідливі фактори виробництва:

- знижена чи підвищена температура повітря робочої зони;
- знижена чи підвищена вологість повітря робочої зони;
- знижена чи підвищена рухомість повітря робочої зони;
- підвищений рівень шуму;
- підвищений рівень електромагнітного випромінювання;
- знижений рівень освітленості на робочому місці;
- напруга зору;
- напруга уваги;
- тривалі статичні навантаження;
- великий обсяг інформації, оброблюваної в одиницю часу;
- підвищене значення напруги в електричному ланцюзі, замикання якої може відбутися через тіло людини;
- підвищений рівень пожежної небезпеки.

Показники в комплексі, що характеризують повітря (температура,

вологість, рухливість) робочої зони, називають параметрами мікроклімату. Відомо, що параметри мікроклімату впливають на здоров'я та працездатність людини. Для створення оптимальних умов праці по відношенню до мікроклімату необхідно керуватися певними вимогами. Значення параметрів мікроклімату, які необхідно дотримуватися, встановлені ДСН 3.3.6-042-99.

Санітарні норми поширюються на мікрокліматичні умови в межах робочих зон виробничих приміщень підприємств, установ, установ незалежно від їх форми власності та належності. Цей нормативний закон визначає оптимальні та допустимі нормативні значення для показників мікроклімату та встановлює вимоги до вимірювання параметрів мікроклімату та методи їх оцінки. Робота інженера-програміста як користувача ПК відносять до робота середньої ваги, оскільки вимагає великого розумового навантаження. Специфікаційні значення параметрів мікроклімату для цього виду робіт наведені в таблиці 4.1.

Таблиця 4.1 – Нормування параметрів мікроклімату на робочому місці

Найменування параметра мікроклімату	Період року			
	Холодний		Теплий	
	Оптимальні	Припустимі	Оптимальні	Припустимі
Температура, °С	19 – 21	17 – 24	21 – 23	18 – 27
Відносна вологість, %	40 – 60	75	40 – 60	65 при 26 °С
Швидкість руху повітря, м/с	0,2	0,3	0,3	0,4 – 0,2

У приміщеннях з робочими місцями для користувачів ПК необхідно підтримувати оптимальні параметри мікроклімату за допомогою систем загальнообмінної припливно-витяжної вентиляції, а також систем зимового опалення. Температура повітря в холодний і теплий період протягом усього року повинна бути від +20 - 25 °С, відносна вологість - 60-40%, швидкість вітру - не більше 0,2 м/с, подача зовнішнього повітря повинна бути забезпечена. 20 м3 на людину і не повинна бути нижче 30 м3/год.

Повітря в приміщенні має бути очищено від шкідливих речовин, пилу та мікроорганізмів. Повітря в робочій зоні має відповідати встановленим

вимогам для приміщень, що злегка перегріті від відеотерміналів та обладнання для відображення інформації.

Наступним фактором є вплив шуму на організм людини. Навіть тихий шум, який присутній протягом робочого дня, може негативно вплинути на організм людини. Гучність офісного шуму може досягати 55-60 децибел, а вуличного шуму – 80-90 децибел. При цьому майже завжди чути роботи з сильним перевантаженням. Нормування шуму виконано згідно з LTO 3.3.6.037-99. Вибір методу нормування залежить від тимчасових характеристик шуму. Рекомендований рівень шуму для робочих місць користувачів ПК не повинен перевищувати 50 дБА. Стандартизований рівень шуму забезпечується за рахунок використання малошумного обладнання, облицювання звукопоглинаючими матеріалами.

Під час роботи з комп'ютером навантаження на органи зору збільшується, тому важливим заходом гігієни праці є створення оптимального освітлення, тобто організація комфортного та гігієнічного природного та штучного освітлення робочих місць, де використовуються комп'ютери та місць з Дослідження показали, що якщо освітленість робочого місця збільшити зі 100 лк до 500 лк, то продуктивність праці з помірною інтенсивністю збільшується на 5-6%, а для важких робіт – на 15%. Спектральний склад випромінювання штучного джерела світла має значний вплив на психологічний стан користувачів ПК. Є тепле і холодне світло і тіні. Вважається, що холодні тони створюють веселий і працьовитий настрій, а теплі кольори, навпаки, розслаблюють.

Аналіз нормативних вимог до освітлення робочих місць за допомогою ПК показує, що рівень горизонтального освітлення повинен бути не менше 400 люкс, а коефіцієнт пульсації освітлення при штучному освітленні не повинен перевищувати 5%.

Для освітлення робочого місця за допомогою ПК необхідно використовувати поєднання освітлення – природного та штучного. В якості системи штучного освітлення виберіть комбіноване освітлення (загальне та

місцеве). Загальне освітлення створює однакові умови освітлення без великої різниці в яскравості між робочим місцем і в приміщенні, а точкове освітлення створює додатковий світловий потік на робочому місці.

Для загального освітлення рекомендуються переважно стельові або вбудовані світильники з люмінесцентними лампами. Використовуйте джерело нейтрального білого світла з індексом передачі кольору не менше 70. Допустимий рівень дискомфорту для освітлювальних приладів у цих місцях становить 40.

Основні причини уражень електричним струмом користувачів ПК:

- випадкове доторкання до струмоведучих частин електрообладнання (ПК та периферійних пристроїв) внаслідок помилкових дій або несправності захисних засобів;
- поява напруги на неструмоведучих конструктивних частинах ПК та периферійних пристроїв внаслідок пошкодження ізоляції струмоведучих частин або замикання фази електромережі на землю;
- поява напруги на відімкнених струмоведучих частинах ПК та периферійних пристроїв внаслідок замикання між струмоведучими частинами, що включені або знаходяться під напругою, після розряду блискавки в електроустановку тощо.

Робоче місце користувачів комп’ютерів для забезпечення електробезпеки обладнання та захисту самих користувачів ПК від ураження електричним струмом повинно мати технічні засоби захисту згідно з НПАОП 40.1-1.21-98.

Місце, де розташоване робоче місце ПК, повинно бути обладнане захисним заземленням або зануленням відповідно до експлуатаційних умов. Металевий корпус електрообладнання повинен бути заземлений. Категорично забороняється використовувати в якості контурів заземлення такі труби радіатора, як пара, вода, газ, опалення. Залежно від потужності, що передається, силові кабелі повинні мати повну ізоляцію і перетин.

Персональні комп’ютери та їх периферійні пристрої та обладнання для обслуговування, ремонту та регулювання, інше обладнання (контрольні, лампи тощо), проводи та кабелі повинні бути розраховані на працездатність та захист зони ПУЕ, із пристроями захисту від короткого замикання та іншими аварійними режимами.

У приміщенні, де одночасно експлуатується або обслуговується більше п’яти комп’ютерів, на видному і легкодоступному місці має бути встановлений аварійний резервний вимикач, щоб повністю вимкнути живлення приміщення, за винятком аварійного освітлення.

Розетки для живлення ПК та периферійних пристроїв повинні бути прокладені вздовж стіни на підлозі впритул до стіни, як правило, в металевих трубах і гнучких металевих шлангах з кранами відповідно до затвердженого компонування обладнання та технічних характеристик. Якщо до 5 комп’ютерів розташовані по периметру приміщення та використовують трипровідні екрановані дроти або кабелі в корпусах з негорючого або негорючого матеріалу, їм дозволяється працювати без металевого трубопроводу та гнучкого металевого кабелепроводу.

Переносне електрообладнання необхідно підключати надійним ізольованим гнучким шнуром.

Використання комп’ютера вимагає тривалого сидіння, що може призвести до різних форм опорно-рухового апарату. Використання комп’ютера характеризується недостатньою фізичною активністю та монотонністю. Монотонна робота знижує професійний інтерес, негативно впливає на продуктивність праці, сприяє розвитку неврозів, які можуть призвести до професійних захворювань. Ергономічна проблема полягає в бездіяльності користувача ПК. Робота користувачів ПК характеризується зниженою часткою фізичної праці, підвищеним розумовим навантаженням і, в деяких випадках, віддаленістю конкретних результатів роботи. Особливістю роботи у сфері інформаційної безпеки є підвищене зорове напруження, пов’язане зі сприйняттям зображень на екрані, диференціацією

тексту в друкованих матеріалах, тобто виконанням роботи, що негативно впливає на зір.

Зона робочого місця користувача ПК повинна відповідати ергономічним вимогам. Відповідно до гігієнічних вимог робочого місця користувача, з метою забезпечення безпечних умов праці ПК встановлюється на робочому місці: об'ємом не менше 24 м3 і площею не менше 6 м2. Ширина проходів між окремими робочими місцями повинна бути не менше 1,2 м.

При організації робочого місця враховуються антропометричні дані працівників і розміщення елементів обладнання за характером і послідовністю виконуваної роботи. Це дозволяє співробітникам вибрати оптимальну висоту і положення нахилу для всіх компонентів обладнання робочого місця. Робочий стіл повинен мати стійку конструкцію. Мінімальний розмір стільниці 160 х 90 см. Висоту сидіння оператора та стільниці слід відрегулювати на 42-55 см і 65-85 см відповідно. Тип робочого стільця залежить від тривалості роботи: довге - величезне крісло, коротке - крісло легкої конструкції, яке можна вільно втягувати.

Клавіатура ПК повинна бути відокремлена від екрану і вільно рухатися. При використанні роботизованої «мишки» кожен раз, коли рука піднімається і багаторазово тримається над предметом, передпліччя значно навантажується. Тому користувачам ПК з маніпуляторами з клавіатурою та «мишкою» найкраще використовувати кисті, які підтримують повторювані рухи. Ці кронштейни необхідно розташувати так, щоб щітки могли вільно звисати. Підніжка стільця повинна мати п'ять опор, щоб уникнути перекидання.

Під час роботи екран ПК слід тримати на відстані витягнутої руки від обличчя користувача. Неприпустимо, щоб працівники мали візуальний контакт з іншими моніторами або екранами телевізора як джерелом надмірних відблисків.

Для попередження психічного напруження використовується

раціоналізація режимів праці та відпочинку. Це досягається зменшенням додаткових перерв, створенням умов для ефективної розваги в приміщенні за звичайних погодних умов, змінами характеру виконуваної роботи, наприклад створення документації, написання алгоритмів на папері, написання та налагодження програм. Емоційному перевантаженню найкраще запобігти тренуваннями в команді, робочими сесіями на місці та проходженням курсів підвищення кваліфікації.

Пожежна безпека на робочих місцях користувачів ПК має забезпечуватися організаційними заходами та технічними засобами для запобігання пожежам, забезпечення особистої безпеки, зменшення можливого майнового збитку та зменшення негативних екологічних наслідків при їх виникненні, створення умов для успішного гасіння пожежі. Правила пожежної безпеки України.

Основні причини виникнення пожеж у приміщеннях користувачів ПК:

- використання несправної або незаземленої апаратури;
- використання електронагрівальних приладів;
- експлуатація апаратури з пошкодженою ізоляцією проводів;
- користування пошкодженими розетками, рубильниками, іншим електрообладнанням;
- включення в мережеві фільтри, блоки безперебійного живлення та спеціалізовані розетки, розташовані в коробах, побутової техніки та іншого
- обладнання, що не пов’язане із ПК;
- залишення без нагляду включеної до мережі апаратури, ПК, оргтехніки;
- обгортання (накривання) світильників папером, тканиною та іншими горючими матеріалами;
- нагромадження паперових документів і зайвих предметів на електрообладнання;

– куріння в приміщенні.

ПК, обладнання, обладнання, проводи та кабелі повинні відповідати вимогам PUE, а також обладнання проти струму короткого замикання та інших аварійних режимів.

Об'єкти для постійного або тимчасового проживання 100 і більше осіб або об'єкти з хоча б однією одномісною кімнатою для одночасного проживання 50 і більше осіб, у разі одночасного проживання, в будинках і будинках (крім квартир) на два поверхи і більше Для поверхів понад 25 осіб і понад 50 осіб слід скласти план (план) евакуації та вивішувати його на видному місці на випадок пожежі.

План евакуації повинен містити як графічні, так і текстові компоненти. Графічний розділ – це план поверху кожного поверху. На плані показані суцільні шляхи евакуації суцільними зеленими стрілками та альтернативні шляхи евакуації пунктирними стрілками. Місця розташування вогнегасників, гідрантів і телефонів позначаються символами на плані поверху. Текстова частина плану евакуації у вигляді таблиці. Він містить інструкції щодо дій у разі пожежі, доповнені знаками безпеки та символами для наочності. Розмір плану евакуації становить не менше 600 х 400 мм для поверхового та часткового плану евакуації та 400 х 300 мм для плану часткової евакуації.

На видному місці біля телефону має бути вивішена табличка з номером для виклику пожежно-рятувальних служб.

На території об'єкта, а також на будинках, будівлях і місцях повинні бути встановлені відповідні охоронні знаки. Двері на шляхах евакуації повинні відкриватися в бік виходу з будівлі (приміщення). Якщо в кімнаті хтось знаходиться, то двері до евакуаційного виходу можна закрити лише на внутрішній замок, який можна відкрити зсередини без ключа.

Сходи і майданчики повинні мати доступні перила з поручнями і не повинні зменшувати ширину сходів і майданчиків. Сходові клітки, внутрішні відкриті та зовнішні сходи, коридори, проходи та інші шляхи евакуації повинні бути обладнані аварійним освітленням.

Більшість вуглекислотних вогнегасників встановлюють у приміщеннях, де працюють користувачі ПК. Вогнегасний засіб цього вогнегасника не проводить електрику. Випарений вуглекислий газ не залишає слідів і не пошкоджує офісну техніку та інші електроприлади.

Вогнегасники повинні бути розміщені на місці, щоб захистити їх від прямих сонячних променів, механічної дії та інших несприятливих факторів, таких як вібрація та висока вологість. Вогнегасники слід розміщувати в легкодоступних і помітних місцях. Не зберігайте та не експлуатуйте вогнегасники там, де температура може перевищувати 500°C та під прямими сонячними променями. При гасінні електроустановок під напругою не дозволяється розміщувати розетку на відстані менше 1 м від електроустановки та полум’я. Після використання вогнегасника в приміщенні необхідно провітрити приміщення. Кожен працівник повинен бути ознайомлений з правилами експлуатації вогнегасників.

Під час прийняття на роботу всі працівники повинні проходити інструктаж з пожежної безпеки. Підготовка та перевірка знань з питань пожежної безпеки офіцерів та службовців проводиться в порядку, визначеному постановою Кабінету Міністрів України від 26.06.2013 р. № 444 «Про затвердження Порядку навчання населення діям у надзвичайних ситуаціях».

ВИСНОВКИ

В роботі проведено огляд сучасних способів спілкування людей. Розглядаються методи та засоби обміну інформацією та захисту інформації в месенджерах. Згідно з опитуванням, останніми роками спілкування через електронні засоби месенджери стає все більш поширеним. Найпопулярнішими месенджерами в Україні є Viber, Facebook Messenger, Telegram. Месенджер надають можливості спілкування в прихованих месенджерах, із прихованими чатами, контактами Аутентифікація, захист паролем у чаті, наскрізне шифрування даних тощо. Однак месенджери не пропонують такої функції для створення зашифрованих повідомлень, що актуально у випадках, коли користувачі не хочуть, щоб ці повідомлення читали інші (навіть близькі чи рідні).

Розглянуто загальні поняття шифрування даних, класифікація історичних шифрів та шифрувальних машин. Розроблено алгоритм шифрування, який імітує роботу пристрою Базері. В роботі наведено основні кроки, що складають етапи шифрування та дешифрування інформації.

Був програмно реалізований розроблений алгоритм шифрування, який імітує роботу пристрою Базері. Програмний додаток реалізовано за допомогою мови програмування Python.

ПЕРЕЛІК ПОСИЛАНЬ

1. Общение. URL: http://ru.wikipedia.org/wiki/Общение

2. Энциклопедия SMS. URL: https://itc.ua/articles/jenciklopediya_sms_8075/

3. Обзор средств общения в сети интернет. URL: http://wiki.tgl.net.ru/index.php/Обзор_средств_общения_в_сети_интернет

4. Top 15 Most Popular Social Networking Sites and Apps [2020]. URL: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/

5. Веремеева Т. Мессенджеры в Украине: основные игроки, проблемы и перспективы. URL: https://comments.ua/article/it/technology/641679-messendzhery-v-ukraine-osnovnye-igroki-problemy-i-perspektivy.html

6. Что такое Viber, как им пользоваться? URL: https://uznayvse.ru/voprosyi/chto-takoe-viber-kak-im-polzovatsja.html

7. Як захистити систему від хакерських атак. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-kak-zashhitit-sistemu-ot-xakerskix-atak

8. Хакерська атака на WhatsApp: У чому суть проблеми та як захистити свій телефон від встановлення шпигунських програм. URL: https://ua.112.ua/golovni-novyni/khakerska-ataka-na-whatsapp-u-chomu-sut-problemy-ta-iak-zakhystyty-svii-telefon-vid-vstanovlennia-shpyhunskykh-prohram-491676.html

9. Масштабна хакерська атака на месенджер Telegram: у компанії дали роз'яснення. URL: https://www.5.ua/svit/masshtabna-khakerska-ataka-telegram-u-kompanii-prokomentuvaly-napad-121848.html

10. Хакерська атака: стала відома причина збою у роботі Telegram. URL: https://prm.ua/hakerska-ataka-stalo-vidoma-prichina-zboyu-u-roboti-telegram/

11. 5 шляхів захисту особистих даних в інтернеті. URL: https://beetroot.academy/uk/blog/5-shlyahiv-zahistu-osobistih-danih-v-interneti/

12. Основные понятия криптографии. URL: https://www.intuit.ru/studies/courses/691/547/lecture/12371

13. Дегтярьов А.К. Методи сучасної криптографії. URL: https://dehtyarov09.wordpress.com/2014/03/16/криптографія-загальні-визначення-кл-2/

14. Кан Д. Взломщики кодов. М.: Центрполиграф, 2000.

15. Информационная безопасность и защита информации: учебное пособие. URL: http://window.edu.ru/catalog/pdf2txt/482/57482/27741?p_page=6

16. Jefferson disk. URL: https://www.cryptomuseum.com/crypto/usa/jefferson/ index.htm

17. Сильные стороны и преимущества Unity. URL: http://develop-unity3d.blogspot.com/2016/01/Silnie-storoni-Unity.html

18. Язык программирования C#: история, специфика, место на рынке. URL: https://geekbrains.ru/posts/yazyk-programmirovaniya-c-sharp-istoriya-specifika-mesto-na-rynke

19. Игровой движок Unity 3D. Курс обучения. 2. Интерфейс программы. URL: https://gamesisart.ru/game_dev_unity_2.html

20. ГОСТ 12.0.003-74 Небезпечні і шкідливі виробничі фактори. Класифікація.

21. ДСН 3.3.6-042-99. Державні санітарні норми мікроклімату виробничих приміщень.

22. ДСН 3.3.6.037-99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

23. НПАОП 40.1-1.21-98. Правила безпечної експлуатації електроустановок споживачів.

24. Правила пожежної безпеки України. Затв. Наказом Міністерства внутрішніх справ України 30 грудня 2014 року № 1417.

Додаток А. Лістинг програмного коду

Файл BAZERI_GUI.py

```
from tkinter import *
from tkinter import filedialog
from tkinter import messagebox
import random

def SHIFT(lst, steps):
 if steps < 0:
      for i in range(steps):
           lst.append(lst.pop(0))
 else:
      for i in range(steps):
           lst.insert(0, lst.pop())

def GCD(a, b):
    while b != 0:
        a, b = b, a % b
        #print(a,b)
    return a

def COMPIRE(a, b):
    return GCD(a, b) == 1

def CHECK_KEY(KEYS_A,KEYS_B):
 if (KEYS_A.isnumeric() & KEYS_B.isnumeric()) == True:
      if COMPIRE(int(KEYS_A),100) == True:
           return True
      else:
           messagebox.showerror(title="Ошибка",
message="Число A должно быть взаимно простым с 100")
           return False
 else:
```

```
          messagebox.showerror(title="Ошибка", message="Введите в
поля A,B числа")
          return False

    def ENCRYPT_TEXT():
     #try:
          OUTPUT_TEXT.delete(1.0,END)
          PLAIN_TEXT                                              =
ENTER_TEXT.get(1.0,END).rstrip('\n').lower()
          CASE_A                                                  =
KEY_A.get(1.0,END).rstrip('\n').lower().replace(" ","")
          CASE_B                                                  =
KEY_B.get(1.0,END).rstrip('\n').lower().replace(" ","")
          N = ''
          AFFINA = []
          FULL_SWAPED_ALF = []
          if CHECK_KEY(CASE_A,CASE_B) == True:
               for i in range(len(PLAIN_TEXT)):
                    AFFINA.append((int(CASE_A)     *     i     +
int(CASE_B))%100)
                    print(AFFINA)
               for i in range(len(PLAIN_TEXT)):
                    FULL_SWAPED_ALF.append(DIALS[AFFINA[i]])
                    ind             =             40            -
FULL_SWAPED_ALF[i].index(PLAIN_TEXT[i])
                    SHIFT(FULL_SWAPED_ALF[i],ind)
               print(FULL_SWAPED_ALF)
               rand_part = random.randint(0,40)
               print(rand_part)
               for i in range(len(PLAIN_TEXT)):
                         N += (FULL_SWAPED_ALF[i][rand_part])
               print(N)
               OUTPUT_TEXT.insert('end',u"" + N)
     #except:
```

```
     #    messagebox.showerror(title="Ошибка",  message="Создайте
или откройте ключ-файл")

    def DECRYPT_TEXT():
     #try:
          OUTPUT_TEXT.delete(1.0,END)
          PLAIN_TEXT                                          =
ENTER_TEXT.get(1.0,END).rstrip('\n').lower()
          CASE_A                                              =
KEY_A.get(1.0,END).rstrip('\n').lower().replace(" ","")
          CASE_B                                              =
KEY_B.get(1.0,END).rstrip('\n').lower().replace(" ","")
          N = ''
          AFFINA = []
          FULL_SWAPED_ALF = []
          if CHECK_KEY(CASE_A,CASE_B) == True:
               for i in range(len(PLAIN_TEXT)):
                    AFFINA.append((int(CASE_A)     *     i     +
int(CASE_B))%100)
                    print(AFFINA)
               for i in range(len(PLAIN_TEXT)):
                    FULL_SWAPED_ALF.append(DIALS[AFFINA[i]])
                    ind             =             40            -
FULL_SWAPED_ALF[i].index(PLAIN_TEXT[i])
                    SHIFT(FULL_SWAPED_ALF[i],ind)
               print(FULL_SWAPED_ALF)

          for i in range(40):
               for j in range(len(PLAIN_TEXT)):
                    N += (FULL_SWAPED_ALF[j][i])
               N += "\n"
          print(N)
          OUTPUT_TEXT.insert('end',u"" + N)
     #except:
```

```
    #           messagebox.showerror(title="Ошибка",
message="Создайте или откройте ключ-файл")

    MainFrame = Tk()
    MainFrame.title("БАЗЕРИ")
    MainFrame.geometry("440x630")
    MainFrame.config(bg="thistle1")

    KEY_A = Text(MainFrame,bg = "thistle1",fg = "black",relief =
"groove")
    KEY_A.place(x = 90,y = 30,height = 30,width = 120)
    KEY_A.insert(END,"A")
    KEY_B = Text(MainFrame,bg = "thistle1",fg = "black",relief =
"groove")
    KEY_B.place(x = 220,y = 30,height = 30,width = 120)
    KEY_B.insert(END,"B")
    Button(bg = "thistle1",fg = "black",relief = "groove",text =
"Шифровать",command=ENCRYPT_TEXT).place(x = 90,y = 70,height =
30,width = 120)
    Button(bg = "thistle1",fg = "black",relief = "groove",text =
"Дешифровать",command=DECRYPT_TEXT).place(x = 220,y = 70,height
= 30,width = 120)
    ENTER_TEXT    =    Text(MainFrame,bg    =    "thistle1",fg    =
"black",relief = "groove")
    ENTER_TEXT.place(x = 30,y = 110,height = 30,width = 380)
    OUTPUT_TEXT    =    Text(MainFrame,bg    =    "thistle1",fg    =
"black",relief = "groove")
    OUTPUT_TEXT.place(x = 30,y = 150,height = 430,width = 380)

    DIALS = [
    ['5', 'q', 'j', '6', '7', 'e', '4', 't', 'p', '0', 'y', 'z',
'2', 'v', 'x', 'a', 'n', 'l', '1', 'h', '3', ' ', 'u', 's', 'm',
'o', '8', 'i', 'r', 'c', '9', '.', 'b', 'g', 'w', 'k', 'd', ',',
':', 'f'],
```

```
    ['2', '7', '.', 'n', '9', '1', '4', 'b', 'x', '3', '8', '6',
',', 'a', 'y', 'j', 'z', 'w', 'u', 'o', 't', 'l', 'h', 'd', 'e',
'm', 'c', 'p', 'i', 's', 'g', 'q', 'f', '0', 'k', ' ', 'r', 'v',
':', '5'],
    ['0', 'w', '6', 'g', 'p', '9', 'x', 'e', 'c', 'y', 't', ':',
'7', '5', ' ', 'r', 'd', 'v', 'q', 'j', '.', '8', '1', 'm', '4',
'o', 'u', 'f', 'n', 'k', 's', ',', 'z', 'a', 'b', '3', 'h', 'l',
'i', '2'],
    ['o', 'u', ',', '3', 'e', '8', 'a', '5', 'm', 'c', 'n', 'h',
'i', '7', 'w', 'z', '1', 'k', ' ', 'j', 'f', 'p', '.', 'y', 'r',
'4', 'd', ':', 'l', '9', 'v', 'q', 'b', '6', 'g', 't', 'x', 's',
'2', '0'],
    ['c', ',', '5', 'w', '6', 'x', 'q', 'b', 'z', 'n', 'h', 'u',
'l', 'v', 't', 'p', '1', '9', '0', 'm', 'i', ':', 'd', 's', '7',
'y', 'o', '4', '8', '.', 'r', 'e', 'j', 'k', ' ', '3', '2', 'g',
'f', 'a'],
    ['k', '8', '2', 'd', 'a', 'i', '.', 'v', 'f', 'e', 'o', 'h',
' ', 'r', 'n', '9', '6', ':', 'b', 'c', 'z', 'm', 'l', 'j', '4',
't', '3', 's', '7', '1', 'q', 'g', '0', 'p', 'w', 'y', 'u', 'x',
',', '5'],
    ['d', 'b', '5', '0', 'k', 'q', '3', 'o', ':', 'z', 'n', '9',
' ', '2', 's', 'h', '8', 'f', 'i', '.', 't', ',', 'g', 'u', 'a',
'1', 'p', 'w', 'x', 'm', 'c', 'l', 'v', '4', '6', 'j', 'r', 'y',
'e', '7'],
    ['e', 'g', 'u', 'p', 's', 'h', '2', '.', 'l', '3', '4', 'f',
'm', '0', 'y', 'z', ',', 'r', 'b', 'n', 'x', '7', 't', 'w', 'q',
'c', '1', 'a', '9', '6', 'd', 'i', 'o', 'k', 'v', 'j', '5', ' ',
':', '8'],
    ['f', 'b', '1', '2', 'a', 'h', '8', '5', ':', '7', '9', 's',
'6', '3', 'e', 't', '0', 'w', 'o', 'y', 'q', 'z', 'r', 'm', 'd',
'u', '.', ' ', 'j', 'c', 'x', 'n', 'v', 'p', 'k', ',', 'i', 'g',
'l', '4'],
    ['g', 'j', '3', '8', '9', 'z', ',', '7', '5', '1', 'b', 'q',
':', 'k', '.', 's', 'd', 'p', 'y', 'x', 'v', 'm', 'e', 'r', 'u',
```

```
'o', ' ', 't', 'f', 'l', 'h', 'a', 'i', '6', '0', '2', '4', 'w',
'c', 'n'],
   ['p', '8', 'q', 'a', 'c', 'r', 'e', 'o', 'b', 'f', '3', 'i',
'k', '4', '5', 'w', '9', 'l', ':', 'x', 'z', 'n', 'h', 'y', '.',
'0', 'u', 'd', '7', ' ', ',', 'j', 't', '1', 's', 'm', 'v', '6',
'2', 'g'],
   ['p', 'i', 'j', 'h', '1', 'b', 'n', 'c', 'x', '4', '3', ' ',
'r', 'l', ',', 'u', 'y', 'o', 'z', 'w', '6', ':', '2', '0', 'f',
'e', 'd', 'q', 'k', '5', 'a', 't', 'v', '7', 'g', 'm', 's', '.',
'8', '9'],
   ['s', 'm', 'c', 'a', 'j', '6', '.', 'k', '4', 'd', ',', 'w',
'z', '3', '7', ':', 'r', 'o', 'g', '5', '0', 'p', '9', 'f', 'q',
'8', 't', 'h', 'e', ' ', 'v', '1', 'n', 'u', 'i', 'b', 'x', 'y',
'l', '2'],
   ['c', 'r', 'z', 'a', 'e', '3', '0', 'x', 'p', ',', '.', 'i',
'b', 'w', 'h', '1', 'j', '8', 'v', 'k', ':', '9', 'q', 'l', 'u',
'n', 'o', '2', 'f', '4', '7', 'y', 'g', 's', 'm', '5', '6', 't',
'd', ' '],
   ['k', 'c', '5', 'p', 'j', 'f', '6', 'y', 'q', 'g', 'n', 'r',
'w', 'h', 's', 'i', '8', '1', '9', '.', 'o', '2', 't', ',', ':',
' ', '3', '7', 'b', '4', 'd', 'u', 'v', '0', 'm', 'x', 'z', 'l',
'a', 'e'],
   ['z', 't', '3', 'p', 'q', '5', 'a', 'n', 'e', 'k', 'o', '4',
' ', 'v', '8', '0', '6', 'w', 'm', ',', 'l', '.', 'j', 'r', 'b',
'7', '2', 'x', 'g', 'f', ':', 'h', 'y', 'u', '9', '1', 'd', 'i',
'c', 's'],
   [' ', 'p', '1', '5', '0', 'q', 's', 'u', 'j', 'y', 'z', 'w',
':', 'h', 't', 'f', 'e', 'n', 'k', 'd', 'b', 'm', '6', 'x', '7',
'l', '4', '2', 'o', 'g', 'r', '.', 'v', ',', 'i', '8', '3', 'c',
'a', '9'],
   ['x', 'c', '.', '6', 'l', 'u', 's', 'd', 'k', 'v', '1', 'e',
'4', 'z', 'm', 'w', 'a', ' ', '3', 'j', 'n', ',', 'r', '5', 'h',
'8', 'p', 't', 'f', '9', 'y', '7', 'o', 'b', '2', ':', 'i', '0',
'q', 'g'],
```

```
    ['c', 'e', '4', 'o', 'g', 'k', '0', 'p', 'n', 'm', '1', 'f',
':', '7', 'd', '2', 'q', 'z', '5', 'w', 'v', 'u', 'i', 's', 'l',
',', 'j', 'x', '6', 'b', ' ', 'a', '9', 'r', '3', 'h', 't', '8',
'.', 'y'],
    ['v', '4', 'o', '9', 'b', 'j', 'y', 'x', 'r', 'd', '7', 'a',
't', '3', ':', 'w', '1', 'u', 'q', 's', '2', 'i', 'e', 'c', '8',
' ', 'h', ',', '6', 'k', '.', 'p', 'n', '0', 'm', 'f', '5', 'g',
'z', 'l'],
    ['1', '0', '3', 'l', '4', 'e', ' ', 'z', 'c', 'v', 'o', '2',
'j', '9', 'k', '.', 'h', 'y', 'w', 'g', 'f', 'x', 's', '8', '6',
':', '5', 't', 'i', 'p', 'q', 'a', ',', '7', 'b', 'd', 'r', 'm',
'n', 'u'],
    ['1', 'o', '8', ',', 'q', 'c', 'f', 'e', 'n', 'x', 'i', 'l',
'w', 'a', 'p', 'h', 't', 'v', 'k', ':', 'r', '5', 'u', '6', '0',
'd', 'y', 'z', '7', '4', 'b', 'm', '3', ' ', 'g', '2', 'j', '9',
's', '.'],
    ['i', 'o', 'w', 'j', '4', 'm', '0', '5', '7', 'c', 'l', 'z',
'2', 'y', 'h', 'k', 't', '8', 'f', ' ', 'a', '3', 'g', 'x', 'q',
'.', 'r', 'b', 'u', 's', '9', ':', 'n', '1', ',', 'v', 'd', 'p',
'6', 'e'],
    ['i', 'q', 'j', 'd', 'n', '2', 's', 'r', 'y', 'u', 'z', '6',
',', ':', 'a', '7', '0', 'o', 'm', 'e', 'h', 'l', '1', 'p', ' ',
't', 'c', 'f', '.', 'x', 'k', '8', '3', 'v', 'g', '5', 'w', 'b',
'9', '4'],
    ['g', 'm', 'p', '7', '.', 'k', '8', 'f', ':', 'v', ' ', '3',
'd', '0', ',', 'q', '1', 's', 'z', 'i', '2', '4', 'x', '6', 'j',
'l', 'c', 'a', 'n', 'h', 't', 'y', 'o', 'w', 'u', '5', 'b', 'r',
'9', 'e'],
    ['c', '5', 'y', '8', 'j', 's', 'v', ':', '9', 'k', 'o', 'a',
'x', '6', 'b', 'n', '2', 'h', 'p', '0', '7', 'w', '3', 'z', 'i',
'.', 'u', 'l', ' ', 't', ',', 'e', 'g', 'r', 'q', 'f', '4', 'd',
'm', '1'],
    ['x', '3', 'z', 'l', 'e', 'm', 'g', 'w', '6', 'd', 'h', '0',
's', '.', '9', 'n', 'y', ' ', 'r', 'b', '4', 'a', '8', 't', '7',
```

```
'1', 'p', 'u', 'f', 'k', 'o', ':', 'i', '5', 'c', '2', 'v', 'j',
',', 'q'],
   ['5', 'w', 'u', '1', '7', 'm', 'f', 'c', '2', 'd', 'n', 't',
'g', ':', 'k', ',', 'h', 'r', '0', ' ', 'j', 's', 'i', 'v', '9',
'a', '8', '6', 'x', 'p', '4', 'y', '.', 'o', 'q', 'l', 'z', '3',
'e', 'b'],
   ['c', ',', 'o', 'd', 'b', '4', '8', 'l', 'e', 'u', 'm', 'j',
'a', 'i', '3', '2', '0', 'r', '7', '6', 'q', '5', 'z', 'x', 'f',
'.', 't', 'p', 'w', ':', 'h', 'g', '1', 'v', 'y', 'k', ' ', 's',
'n', '9'],
   ['g', 'j', 't', 'l', '5', 'y', 'f', '6', '1', 'm', ' ', 'w',
'3', 'p', 'n', '2', 's', ',', 'r', 'u', '7', '.', 'x', '0', '8',
'v', '9', 'k', 'o', 'b', 'd', ':', 'e', 'q', '4', 'c', 'i', 'z',
'a', 'h'],
   ['h', '3', ',', 'z', '7', 'i', '0', ' ', '8', '5', 'm', 'k',
'n', ':', 'q', '.', 'e', '1', 'r', 's', 't', 'x', 'c', 'j', 'l',
'9', 'd', 'f', 'b', '2', 'o', 'p', '4', '6', 'w', 'v', 'a', 'u',
'g', 'y'],
   ['r', '2', ':', 'm', 'j', '7', 'o', '4', 'i', '5', 'u', ' ',
'c', 'g', 'l', 't', 'w', ',', 'q', '9', 'n', '.', 'e', 'k', 'v',
'h', 'b', '6', 'y', '0', '3', 's', '8', 'z', 'f', 'a', 'p', 'd',
'1', 'x'],
   ['j', '.', 's', ' ', 'e', 'w', '1', 'f', '5', 'b', 'c', 'p',
'l', 'v', 'y', '0', 'n', ':', '6', 'g', ',', 'r', '2', 'q', '4',
'7', 'd', 'z', '3', 'a', 'k', 'o', 'x', 't', 'u', '8', 'i', 'm',
'h', '9'],
   ['t', '2', '4', 'm', ':', ' ', 'f', '0', '1', 'h', '9', ',',
'i', '3', 'w', 'v', 'g', 'd', 'b', 'k', '8', 'n', 'a', 'y', 'x',
'j', 'l', 'q', '6', 'r', 'p', '7', '.', 'e', 'c', 'z', 's', 'o',
'5', 'u'],
   ['b', ':', 'k', 'd', 'p', 'e', 's', 'r', ' ', 'h', 'v', 'c',
'8', 'n', '2', '9', 't', 'g', 'i', '3', 'o', '6', 'q', '1', 'u',
'y', 'z', '.', '7', 'w', 'l', ',', '4', '5', 'f', 'a', 'x', '0',
'm', 'j'],
```

```
    ['v', 'a', '7', 'k', 's', 'f', ',', ' ', 'l', 'm', 'd', 'o',
'w', '2', '8', 'y', 'n', 'b', '.', 'e', 'q', 'h', '3', 'u', '1',
'z', 'c', '9', 'g', 't', 'i', '4', '6', 'r', '5', 'p', ':', 'j',
'0', 'x'],
    ['n', 'j', 'f', '3', '5', 'u', 'k', '7', '4', 'x', 'z', '2',
'y', 'v', '1', ',', 'g', 's', 'i', ':', 'l', 'd', '0', 'c', '9',
'6', 'r', '8', 'w', 'e', 'p', 'h', 'o', 't', '.', 'q', 'b', 'a',
'm', ' '],
    ['5', 'x', 'v', 'h', 'd', '.', 'n', 'p', '0', 'y', '4', 'z',
'a', 'l', 't', 'q', '3', 'e', 'u', '8', ' ', 'j', 'o', '2', ':',
'k', '6', 'f', '7', '9', 'm', 'g', 'r', 'b', 'c', '1', 'i', ',',
's', 'w'],
    ['z', 'c', 'x', 'i', 'b', ',', 'd', '1', '6', '5', '9', 'h',
'm', 'q', 'a', 'n', '7', 'g', ':', 'e', 'j', 'y', 'l', 'r', '0',
's', '.', 'p', ' ', 'f', 'w', 'o', 'k', '4', '3', 'v', 'u', '8',
'2', 't'],
    ['y', '5', 't', 'b', 'a', '0', 'n', '4', '7', 'h', '2', 'o',
's', ',', 'r', 'k', 'q', 'g', '8', 'c', 'e', 'z', 'p', 'v', '1',
'l', ':', '3', '6', 'i', 'f', 'm', 'j', '.', ' ', 'u', 'd', 'w',
'x', '9'],
    ['8', 'p', '9', 'y', 'f', 'e', 'a', ',', '5', 'x', '3', 'c',
'b', 'w', 'd', 'h', 's', 'z', 'g', ':', 'k', '.', 'r', '1', ' ',
't', 'i', 'n', '4', '0', '2', 'm', 'u', 'v', 'q', '6', 'o', 'l',
'7', 'j'],
    [':', '7', '6', ' ', 'j', 'r', '0', '.', 'v', 'b', '2', ',',
'k', 'h', '3', 'e', 'n', 'g', '9', '5', 'o', 'l', 'd', 'q', '8',
't', 'a', '4', 's', 'x', 'i', 'c', 'p', 'f', 'w', '1', 'z', 'y',
'u', 'm'],
    ['8', 'b', '2', 'd', ',', 'v', 'l', '1', 'm', 'x', 's', 'h',
'7', 't', '9', 'e', 'p', '0', 'c', 'r', '5', 'k', 'f', 'i', 'q',
'.', 'y', 'z', 'w', 'g', 'j', 'a', ':', ' ', '4', 'u', 'o', '3',
'n', '6'],
    ['l', '0', '7', 'x', '.', 'g', 'b', 'i', 'e', '5', 'y', 'r',
'w', 'k', '2', 'o', '6', 'u', 'p', 'c', '9', 'd', 'h', 's', '4',
```

```
':', 'm', 'j', ',', 'v', 'z', '1', 'a', ' ', 'f', 't', '8', 'n',
'3', 'q'],
    ['l', 'z', 'p', '8', 'j', 'c', '7', '6', '2', '9', 'y', 'a',
's', 'n', 'v', 't', '1', ' ', ':', 'e', 'r', '3', '5', ',', '4',
'w', 'b', '.', 'q', 'd', 'm', 'h', 'i', 'k', 'x', 'f', 'g', '0',
'o', 'u'],
    ['j', 'k', 't', ':', '2', 'm', 'a', 'c', 'u', 'i', 'w', 'z',
'7', 'o', 'l', '9', 'r', 'n', '6', 'p', '1', 'g', 'v', '4', 'y',
'3', ' ', '5', 's', ',', 'f', 'q', 'b', 'e', 'x', 'd', 'h', '0',
'8', '.'],
    ['.', '5', '1', ',', 'v', 'f', 'h', '2', 'r', 'k', '8', 'j',
'6', 'u', 'n', 'm', 'z', 'l', 'e', 'b', 't', 'd', 'o', 's', '3',
'x', 'q', 'p', ' ', 'w', '4', 'g', 'a', 'i', '0', '7', ':', 'c',
'9', 'y'],
    ['g', 'f', 'v', 'k', 'b', '2', '5', 'l', 'm', 'w', 's', '8',
'y', '3', 'q', '1', 'i', 'j', ':', '9', 'n', 'u', '0', 'p', '7',
'c', 'r', 'e', 't', 'a', 'x', 'o', 'h', ' ', 'd', '6', '4', '.',
'z', ','],
    ['8', 'y', 'p', '2', 'z', '9', 'r', 'l', 'w', 'o', '.', 'v',
'g', 'h', '0', ',', 'k', 's', 'c', '4', 'b', 'i', '3', '5', '7',
'u', 'm', ':', '1', 'j', 'e', 'f', '6', 'd', 'n', 't', 'x', 'a',
'q', ' '],
    ['5', 'f', 'e', '2', 'z', '0', 'l', 's', 'u', 'o', '6', 'v',
'4', 'i', 't', 'd', '3', 'p', 'c', ':', 'n', 'h', '8', ' ', 'b',
'1', 'm', '7', '.', 'a', 'q', 'y', '9', 'g', 'j', 'x', 'r', ',',
'w', 'k'],
    ['v', 'o', '.', 'u', '5', 'j', '2', 'z', 'f', 'c', 'p', 'x',
'e', ',', 'm', '7', 'd', '8', 'l', '1', 'y', 'q', '9', 'r', '4',
'n', 'b', '6', ' ', 's', 'i', 'a', 'k', '3', 't', 'h', '0', 'g',
'w', ':'],
    ['r', 'o', ':', '1', 's', ' ', 'h', 'e', '3', 'j', '7', '9',
'x', 'v', '5', 'z', 'm', '2', 'f', 'b', 'n', '6', 'u', '8', 'k',
'4', 'i', 'a', 'c', ',', 'l', '.', 'd', 'w', 'q', 'y', 'g', 'p',
'0', 't'],
```

```
    ['x', 'm', 'n', ',', 'a', 'l', 'p', ' ', '4', 'k', '.', '7',
'q', 'd', '1', '8', 'g', '2', 'f', '0', ':', 't', 'r', 'w', 's',
'j', '3', '9', 'z', 'o', '6', 'b', 'v', 'i', 'u', 'c', 'h', 'y',
'e', '5'],
    ['3', '5', 'p', 'l', ' ', 't', 'h', 'k', '7', 'm', '0', 'g',
'z', 'e', 'u', 'a', '9', 'j', ',', 'r', 'b', ':', '.', 'v', 'x',
'o', '6', '1', 'f', '4', 'w', 'd', 'q', '2', 's', 'y', 'n', 'c',
'8', 'i'],
    ['d', 'n', 'g', 'b', 'e', '9', 'u', '7', 'v', '4', 'a', '3',
'.', '8', '6', 'q', '5', 'w', 'o', 'f', 's', 'z', '0', 'i', 'j',
':', ' ', 'k', 'm', 'p', '1', '2', 'l', 'y', 'x', 'c', 'h', 't',
',', 'r'],
    ['1', 'q', 'z', 'r', 'i', 'j', 'y', 'f', ':', 'e', ' ', '.',
'h', 'o', 'a', '4', 'w', '0', 'm', 'v', 'n', 'g', ',', 'p', 'c',
'9', 'd', '8', 'b', 'l', '3', 'u', 't', '2', '6', 'x', '7', '5',
's', 'k'],
    ['v', '6', 't', '2', 'w', 'l', '0', 'o', 'n', 'r', 'b', '8',
'u', 'd', 'j', 's', ',', 'm', '7', 'y', 'e', 'p', 'c', 'q', '.',
'3', '5', 'g', '9', 'f', 'k', ':', '4', ' ', 'x', '1', 'z', 'i',
'h', 'a'],
    ['f', '.', 'y', 'r', 'b', 'c', 'm', 't', 'd', '2', 'o', 'a',
'q', '1', ':', '3', 'j', 'i', 'p', 'x', '5', '4', 'z', '7', 'w',
's', '0', 'h', 'n', 'k', 'l', '8', 'v', ' ', 'g', ',', '9', 'u',
'e', '6'],
    ['r', 'j', 'n', 'c', 'a', 't', 'h', 'y', '0', 'o', '3', 'm',
'4', '7', ':', 's', ' ', '6', 'e', 'f', '8', 'k', 'i', 'l', 'x',
'1', 'b', '5', ',', 'u', '9', 'q', 'v', 'w', 'p', 'z', '.', '2',
'g', 'd'],
    ['p', 'e', 't', '2', 'i', 'z', '9', 'b', 'f', 'u', '.', '0',
'd', 'q', ',', 'l', '8', '1', 'r', 'c', 'w', '5', 'v', 'o', 'n',
'x', ':', 'h', '3', '7', 's', 'm', '4', 'k', 'a', 'j', '6', 'y',
' ', 'g'],
    ['d', ':', 'm', '.', '0', '8', 'r', 'j', '9', 'n', '2', 'l',
'a', '1', 'x', '5', 'f', 'v', 'i', 'q', ',', 'c', 'k', 'h', '3',
```

```
' ', 'y', 'e', 'g', '7', 'p', 'u', '4', '6', 'o', 's', 't', 'b',
'w', 'z'],
    ['.', 'k', 'a', 'b', '6', '7', 'e', 'w', 'm', 'p', 'y', 'd',
'z', '2', ':', '8', 'r', 'i', '9', 'j', '1', 'n', 's', 'q', '4',
'o', ',', ' ', 'c', 'v', '5', 't', 'g', 'u', 'x', '0', 'f', '3',
'l', 'h'],
    ['x', 'r', 'w', 'l', '1', 'o', 'j', 'u', '6', 'y', 'i', 'k',
'a', '9', 'g', 'm', 'p', 'd', 'z', ' ', 'e', '.', 't', 'b', 'n',
'c', ':', '7', 'q', 's', 'h', '4', '3', '8', '5', 'v', ',', '0',
'2', 'f'],
    ['e', 'v', '.', 'd', 'g', 'n', 'c', '2', '5', ':', 'h', '9',
'0', '4', 'm', 'a', 'l', 'p', '8', '3', ' ', 'k', 'q', 'i', 'b',
't', 's', 'z', ',', '1', '7', '6', 'x', 'u', 'o', 'w', 'y', 'f',
'j', 'r'],
    ['4', 'g', '3', 'k', '.', '0', 'v', 'b', 'a', 'l', 'o', 'm',
'd', 'j', 'n', 'w', '2', 'u', ',', '1', 'q', 't', 'z', 'i', 'p',
'h', ' ', '7', 's', 'x', 'c', '8', '5', '9', 'y', '6', 'e', 'r',
'f', ':'],
    ['2', 'x', 'b', ',', 'v', 'q', '9', 'c', 'm', ':', '6', 't',
'n', 'w', 'e', '.', ' ', '7', 'h', '8', '5', 'l', 's', 'i', 'a',
'r', '3', '4', 'j', 'k', '1', 'u', 'd', 'z', 'p', 'y', 'o', '0',
'f', 'g'],
    ['i', 'x', '0', ':', 'e', 's', 't', 'h', 'z', 'j', 'n', 'a',
'd', 'o', '7', '4', '6', '8', 'r', 'b', '1', 'l', 'g', 'f', 'q',
'.', '2', 'c', '3', '9', 'm', ' ', 'w', ',', 'k', 'y', 'p', 'u',
'5', 'v'],
    ['1', '6', '0', 'f', 'l', 't', 'y', '8', ',', 'r', 'o', 'k',
'.', '9', 'h', 'x', '7', 'e', 'p', ':', 'b', '5', 'v', 'i', 'z',
'd', 'g', 'm', 'q', '2', 's', 'n', '4', 'u', 'j', '3', ' ', 'a',
'w', 'c'],
    ['k', 'q', 'd', 'w', 'u', 'j', 's', 'z', '7', '9', '.', ' ',
'4', 'l', 'r', ',', 'c', 'y', '3', 'v', 'h', 't', 'm', 'e', 'b',
'0', '8', ':', 'i', '1', 'f', '5', 'a', 'n', 'x', '2', 'g', 'o',
'6', 'p'],
```

```
    ['x', '6', ',', 'h', 'e', 'm', 'a', 'd', 'b', 'w', '2', 'l',
'7', '0', 'j', 's', '9', 'p', '4', '.', 'r', 'q', 'i', '3', 'k',
'f', 'c', 'n', ':', 'y', '8', 'g', ' ', 'u', 'z', '5', 't', 'o',
'v', '1'],
    ['s', 'o', '3', 'w', ',', 'p', 'j', '.', 'q', '5', 'h', 'z',
'2', 'v', '6', '4', '0', 'y', 'n', 'l', 'k', 'a', '7', 'e', '9',
':', '1', 'b', 'x', 'u', 'g', 't', ' ', 'r', 'm', 'c', 'd', 'i',
'f', '8'],
    ['7', 'd', 'j', 'r', 'x', 'i', '4', ',', 'p', '9', 'b', 't',
'5', '6', 'n', 'c', 'o', 'm', 'q', '2', 'f', 's', 'w', 'k', 'u',
'h', 'e', 'y', ':', '.', '8', 'v', 'z', 'g', '3', '1', 'l', 'a',
'0', ' '],
    ['9', 'h', 'j', 'x', 'g', 'u', 'c', '2', 'p', 'a', 't', 'b',
':', 'n', '7', 'm', 'e', 'q', '6', ',', 'y', 'z', '0', 'w', 'o',
'd', 'k', '1', '5', ' ', 'f', '4', 'l', 's', '.', 'i', '3', 'v',
'r', '8'],
    ['0', 's', 'b', 'w', '7', 'y', 't', 'a', '1', 'h', '.', '5',
'u', '6', 'q', 'i', 'g', 'z', 'e', 'r', 'd', 'c', 'n', '8', 'o',
'4', ':', '3', 'm', '2', ',', 'j', 'x', 'p', 'f', 'k', 'l', 'v',
'9', ' '],
    ['r', '3', '8', 'i', 'e', 's', '6', 'k', 'n', 'f', 'm', 'v',
'1', 'p', '4', '7', ' ', 'd', 'y', 'a', 'q', 'o', 'w', 'x', 'u',
'2', '0', 'b', '9', ',', 'g', 'j', '.', '5', 't', 'z', 'h', 'c',
':', 'l'],
    ['t', '9', 'g', 'n', 'f', '1', 'v', 'q', 'y', 'l', 'x', 'b',
's', '.', 'm', '0', 'a', 'z', '8', '5', 'i', 'k', 'o', 'c', 'j',
',', 'u', '3', '7', '4', '6', ' ', ':', 'r', 'e', 'w', 'p', 'd',
'h', '2'],
    ['b', 'e', 'z', 't', 'q', '5', '1', '8', '6', 'v', 'u', ',',
'3', 'x', 'i', 'k', 's', 'l', ':', 'n', 'g', 'd', '.', 'j', '9',
'0', 'm', 'o', 'p', 'h', 'r', 'a', 'c', 'y', 'f', '2', ' ', '4',
'7', 'w'],
    ['h', 'o', 'j', '9', ',', 'r', '7', ' ', '0', 't', '6', '4',
'd', 'g', 'l', 'v', 'k', 'b', 'x', ':', 'w', 'c', '1', 'u', '2',
```

```
'n', 'f', 'a', '5', 'y', 'e', 'i', '.', 'q', '8', 's', 'z', 'm',
'3', 'p'],
    ['a', '0', 'x', 'h', 'y', 'd', 'q', 'c', 'n', 'i', ' ', 'f',
'w', 'b', 'e', 'l', 's', 'g', '9', 'o', 'm', 'v', '8', ':', '.',
'j', '1', '5', '3', 'z', 'k', '6', ',', 'p', 'u', 't', '4', '2',
'r', '7'],
    ['9', 'g', 'a', '8', ',', '1', 'r', 'z', 'o', 'e', 'u', '7',
'd', 'p', 'n', '0', 'c', 'v', 'y', 'k', 'm', '3', 'f', '6', '2',
'5', 'l', 'b', 'i', 'h', ':', '4', 'q', 's', 'x', 'j', '.', 'w',
't', ' '],
    ['f', '4', 'n', 'a', ' ', 's', 'x', 't', 'b', '9', 'e', '5',
'm', '7', 'y', 'i', 'u', '.', 'l', 'd', ',', 'p', '1', '6', 'r',
':', 'g', 'k', 'c', '2', '0', '3', '8', 'w', 'o', 'q', 'v', 'j',
'z', 'h'],
    ['o', ':', 'g', 's', ',', '1', 'd', 'q', 't', 'n', 'l', ' ',
'.', 'k', 'v', 'f', '4', '7', 'h', 'e', '6', '0', '9', 'b', '8',
'i', 'j', '2', 'x', 'a', 'y', '5', 'p', '3', 'z', 'u', 'r', 'c',
'm', 'w'],
    ['x', '3', '0', 'y', 'f', 'm', '5', '.', 'p', 'd', '2', 't',
'w', 'o', 'b', 'q', 'v', 'j', '9', 'h', 'e', '6', ',', 's', ':',
'i', 'a', 'l', 'r', 'z', '7', 'k', 'c', 'u', '1', 'n', '8', 'g',
' ', '4'],
    ['9', 'z', 'm', '1', '4', 'b', 'd', '7', 'k', 'i', 'j', 'q',
'8', '5', '.', '2', 's', ' ', ',', 'c', 'v', 'o', 'f', 'h', ':',
'p', 'n', '0', 'a', 'u', 'w', '3', 't', 'g', 'l', 'y', 'x', '6',
'e', 'r'],
    ['g', 't', 'i', 'm', '7', '8', 'h', 'x', 'c', 'y', '9', '3',
'e', 'u', 'j', ' ', '0', ',', 'a', 'f', '6', '1', 'v', 'p', 'o',
'2', 'w', 'q', 'z', 'b', '5', 'd', ':', 'l', 's', 'k', '4', 'n',
'.', 'r'],
    ['e', 'b', 'm', 'j', '6', 'r', 'q', '1', '4', ':', '7', 'k',
'f', 'w', '5', 'c', 'n', ',', 'z', 'u', '0', '8', 'y', 's', 'x',
'v', '3', 'a', 'i', 'p', 't', 'g', ' ', '9', '2', 'l', 'o', 'h',
'd', '.'],
```

```
    ['i', '5', 'f', ',', '0', 'g', 'y', 'a', '2', 'n', 't', 'c',
'b', 'r', '8', 'p', 'x', 'o', 'm', '7', 'j', '.', 'e', 'l', '1',
'd', '9', 'u', 'k', ' ', 's', 'h', '4', 'v', 'w', ':', '6', '3',
'q', 'z'],
    ['9', 'f', 'g', 'b', 'x', 'q', ' ', 'i', 'y', 't', '8', 's',
'1', 'e', ',', 'u', 'c', 'l', 'm', ':', '2', 'v', 'z', 'r', '0',
'h', '5', 'p', 'w', 'j', '4', '3', 'd', 'k', '7', '.', 'a', '6',
'o', 'n'],
    ['z', 'q', '8', 'x', 'b', 'j', 'l', 'y', 'g', 'i', '1', 's',
'h', ':', 'm', 'c', '6', 'u', '2', 'r', 'k', '0', 'o', 'a', 'e',
'3', 'w', 't', 'd', 'n', 'f', '.', '5', '9', ' ', 'p', 'v', ',',
'7', '4'],
    ['a', '8', '2', 'f', 's', '9', '3', 'b', 'c', '1', 'u', 'w',
'h', '6', '0', '.', '7', 'l', '5', 'j', 'r', 'i', 'z', ':', '4',
' ', 'd', 'e', 'p', 'y', 'n', 'k', ',', 'o', 'm', 'g', 'v', 'q',
't', 'x'],
    ['4', 't', '5', '1', 'e', '.', 'u', 'n', 'a', 'j', 'k', 'h',
'9', 'f', '0', '7', 'z', 'y', 'p', ',', 'b', '2', '8', 'l', '6',
'3', 's', 'm', 'o', 'i', 'v', 'w', ':', 'c', ' ', 'x', 'd', 'r',
'q', 'g'],
    ['o', 'l', '6', '2', '1', ':', 'n', 'b', 'p', 'z', 'h', 'j',
'y', 'm', 'a', 'c', 'r', '.', '4', ',', 'u', 'd', '8', 's', '0',
'x', '7', '9', '5', 'q', 'v', '3', 'i', 'g', 'e', ' ', 'k', 'f',
'w', 't'],
    ['i', '0', 'g', 'l', 's', 'q', 'o', 'w', ',', '.', '7', '8',
'p', 'k', 'a', ' ', 'e', '2', 'y', 'b', '9', 'v', 'r', '3', '6',
'n', '5', 't', 'f', 'z', 'h', ':', 'u', '4', 'm', 'c', 'd', 'x',
'j', '1'],
    ['t', ',', '6', '7', '5', '.', 'e', 'c', ':', '1', '8', '4',
'm', 'u', 'p', '3', 'g', 'o', 'l', 'n', 'y', 'q', '0', 'x', 'r',
'j', 's', '9', 'a', '2', 'i', 'b', ' ', 'z', 'd', 'v', 'h', 'w',
'f', 'k'],
    ['u', 'm', '4', 'r', 'l', '9', 'o', ' ', 'b', 'n', '1', 't',
's', 'k', ':', '0', '3', ',', 'j', 'e', 'h', 'c', '.', 'y', 'x',
```

```
'p', 'd', '8', 'v', 'i', 'w', 'z', 'q', 'g', 'f', '6', '2', '7',
'a', '5'],
    ['v', 'q', 'j', 'g', 'x', '3', 'b', 'u', '4', '7', 'l', 't',
'p', 'c', 'm', 'f', 'n', 'r', '0', '9', ':', ',', 'y', '5', '2',
'i', 'a', 'd', 'e', 'h', 'w', '8', 'k', '6', 'o', ' ', 's', '.',
'1', 'z'],
    ['.', 'i', 'e', 'm', 'z', '8', '4', 'o', ':', '9', 'a', 'y',
't', 'b', 'f', 'k', '0', '6', 'x', 'q', '5', 'p', 's', '2', 'w',
'v', '7', 'c', 'j', ',', '3', 'n', 'g', ' ', 'l', 'd', 'h', 'r',
'u', '1'],
    ['b', 'w', 'l', 'i', 'p', '1', '0', 'h', ':', '5', ',', 'o',
'd', 'f', 'v', 'u', 'j', 'n', 's', 'y', 'e', ' ', 'm', 'c', 'z',
'3', '.', '2', '7', 'k', 'q', 't', 'x', '8', '6', 'a', '4', '9',
'g', 'r'],
    ['7', 'p', '9', 'c', 'd', 'a', 'z', 'y', 'j', 'i', 's', 'u',
'3', 'e', '0', '2', 'r', '.', '4', 'n', ':', ' ', 'm', '1', 'g',
'w', 'q', 'o', '6', 'b', 't', 'h', 'x', '5', 'k', 'l', ',', 'f',
'8', 'v'],
    ['7', '4', '.', 'z', ' ', 'j', 'd', '5', 'v', '3', '0', 'e',
'x', 's', '8', 'r', '9', 'l', 'i', 'h', 't', 'm', 'o', 'p', 'c',
'f', 'q', 'u', '6', '1', ',', ':', '2', 'w', 'n', 'y', 'b', 'g',
'k', 'a']
    ]

    MainFrame.mainloop()
```