Лабораторна робота №1

Тема: Шифр зсуву для латинського {\_, a,b,...,z} та українського {\_,а,б,в,г,ґ,..., я} алфавітів.

Мета: Розробити криптосистему на основі шифрів зсуву.

Хід виконання роботи

1. Розробіть інтерфейс криптографічної системи симетричного шифрування, передбачивши в ньому використання меню та/або панелі інструментів для виконання таких команд:

a. створення, відкривання, збереження, друкування файлів,

b. шифрування і розшифрування файлів українською та англійською мовами,

c. виведення відомостей про розробника та

d. виходу з системи.

2. Розробіть систему класів для реалізації симетричного шифрування, передбачивши в них методи валідації ключа, валідації, шифрування і розшифрування даних.

3. Виконайте тестування роботи системи.

4. Доповніть розроблену систему модулем для атаки на шифр методом «грубої сили» (перебору).

5. Розширте можливості системи, забезпечивши можливість шифрування даних в будь-якому форматі, а не тільки текстових.

Лабораторна робота №2

Тема: Шифр Тритеміуса

Мета: Розробити криптосистему на основі шифру Тритеміуса

Базові відомості

Шифр Тритеміуса - вдосконалений шифр Цезаря, в якому кожен символ повідомлення зміщується на символ, який відстає від даного на деякий крок. Але крок зміщення робиться змінним, тобто залежним від будь-яких додаткових чинників. Наприклад, можна задати закон зміщення у вигляді лінійної функції позиції літери, що шифрується, або за допомогою використання гасла – текстового рядка, який багаторазово записується під текстом повідомленням.

Таким чином, шифрування і розшифрування для шифру Тритеміуса можна виразити наступними рівняннями:

***y=(x+k) mod n x=(y+n−(k mod n)) mod n,***

де ***x*** - символ відкритого тексту, ***y*** - символ шифрованого тексту, n - потужність алфавіту.

Крок зміщення ***k*** розраховується:

* за лінійним рівнянням ***k*** ***=* A*p +* B**;
* за нелінійним рівнянням ***k =* A2 *+* B*p +* C** ;
* за гаслом.

Тут ***p*** - позиція букви в повідомленні. Ключем шифрування виступають відповідно коефіцієнти вказаних рівнянь та гасло.

Хід виконання роботи

1. Модифікуйте інтерфейс криптографічної системи симетричного шифрування з лабораторної роботи №1, забезпечивши можливість використання в якості ключа:

a. 2-вимірного вектору для зберігання коефіцієнтів лінійного рівняння шифрування,

3-вимірного вектору для зберігання коефіцієнтів лінійного рівняння шифрування, c. Текстового рядка (гасла).

2. Доповніть систему класів з лабораторної роботи №1 класами та методами, необхідними для реалізації симетричного шифрування методом Тритеміуса, передбачивши в них методи валідації ключа, валідації шифрування і розшифрування даних.

3. Виконайте тестування роботи системи.

4. Побудувати частотні таблиці для української та англійської мов.

5. Доповніть систему модулем активної атаки на шифр Тритеміуса, який би забезпечував знаходження ключа шифрування у випадку, коли зловмиснику вдалось отримати пару повідомлень «незашифроване –зашифроване».

Лабораторна робота №3

Тема: Шифр гамування

Мета: Розробити криптосистему на основі шифру гамування

Базові відомості

Метод полягає в тому, що символи тексту, який шифрується, послідовно складаються з символами деякої спеціальної послідовності, яка називається *гамою*. Іноді такий метод представляють як накладення гами на вхідний текст, тому він отримав назву «гамування». При цьому символи вихідного тексту і гамми замінюються цифровими еквівалентами, які потім складаються по модулю ***n***, де ***n*** - число символів в алфавіті, тобто шифрування і розшифрування для шифру гамування можна виразити наступними рівняннями:

***y=(x+g) mod n x=(y+n−(g mod n)) mod n,***

де ***x*** - символ відкритого тексту, ***y*** - символ шифрованого тексту, ***g*** – символ гами.

Найбільш часто на практиці зустрічається двійкове гамування. При цьому використовується двійковий алфавіт, а складання здійснюється за модулем два:

***z = x + g (mod 2) = x XOR g.***

Операція складання по модулю два в алгебрі логіки називається також "виключне АБО" або поанглійськи XOR. Операція XOR дуже швидко виконується на комп'ютері (на відміну від багатьох інших арифметичних операцій), тому накладення гами навіть на дуже великий відкритий текст виконується практично миттєво.

Цю ж саму операцію використовують і для розшифрування.

При використанні методу гамування ключем є послідовність, з якою проводиться складання - гамма. Якщо гамма коротше, ніж повідомлення, призначене для шифрування, гамма повторюється необхідну кількість разів. Чим довше ключ, тим надійніше шифрування методом гамування.

Розрізняють два різновиди гамування - з кінцевою і нескінченною гамами. При хороших статистичних властивостях гами якість шифрування визначається тільки довжиною періоду гами. При цьому, якщо довжина періоду гами перевищує довжину шифротексту, то такий шифр є абсолютно стійким, тобто його не можна розкрити за допомогою статистичної обробки зашифрованого тексту. При шифруванні за допомогою ЕОМ послідовність гами може формуватися за допомогою генератора псевдовипадкових чисел (ПВЧ).

Хід виконання роботи

1. Адаптуйте інтерфейс криптографічної системи симетричного шифрування з лабораторної роботи №1 або №2 для реалізації шифрування методом гамування.

2. Доповніть систему класів з попередніх лабораторних робіт класами та методами, необхідними для:

a. генерації гами, період якої перевищує довжину вхідного тексту;

b. реалізації симетричного шифрування методом гамування.

3. Виконайте тестування роботи системи.

4. Модифікуйте розроблену систему, забезпечивши можливість шифрування і розшифрування за допомогою шифроблокноту, як це передбачено в шифрі Вернама.

Лабораторна робота №4

Тема: шифр Віженера

Мета: Розробити криптосистему на основі шифру Віженера для латинського {\_, a,b,...,z} та українського {\_,а,б,в,г,ґ,..., я} алфавітів

Хід виконання роботи

1. Розробіть інтерфейс криптографічної системи для реалізації шифрування.

2. Доповніть систему класів з попередніх лабораторних робіт класами та методами, необхідними для шифрування і розшифрування шифром Віженера.

3. Виконайте тестування роботи системи.

Лабораторна робота №5

Тема: Шифрування з відкритим ключем.

Мета: Реалізувати криптосистему RSA з використанням бінарного алгоритму піднесення до степеня за модулем

Хід виконання роботи

1. Відшукайте в Інтернет-ресурсах чисельний приклад з використання бінарного алгоритму піднесення до степеня за модулем (наприклад, в Вікіпедії ) та опрацюйте його.

2. Розробіть інтерфейс криптографічної системи RSA для шифрування з використанням бінарного алгоритму піднесення до степеня за модулем, передбачивши окремий діалог для формування відкритого ключа.

3. Розробіть методи, які б забезпечували:

a. Генерацію пари «відкритий –закритий» ключі.

b. Шифрування з використанням відкритого ключа.

c. Розшифрування з використанням закритого ключа.

4. Перевірте правильність роботи системи на основі використання даних з чисельного прикладу.

Лабораторна робота №6

Реалізувати протокол обміну ключами Діффі-Гелмана