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:

$$y=(x+g) \bmod n \qquad x=(y+n-(g \bmod n)) \bmod n,$$

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 англійською 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.