**Лабороторна работа №3**

**Тема:** Криптоалгоритм “Шифр Гамування”

**Мета:** Відпрацювання та закріплення теоретичних відомостей з криптоалгоритму “Гамування”

**Короткі відомості:**

Гаммірування - метод симетричного шифрування, полягає в «накладенні» послідовності, що складається з випадкових чисел, на відкритий текст.

Послідовність випадкових чисел називається гамма-послідовністю і використовується для шифрування і розшифровки даних.

Підсумовування, як правило, виконується в будь-якому кінцевому полі. Наприклад, в поле Галуа GF підсумовування набуває вигляду операції «виключне АБО (XOR)».

Довжиною періоду гамми називається мінімальна кількість символів після якого послідовність починає повторюватись, як тільки гамма починає використовуватись повторно шифр вже не буде являтись абсолютно стійким (математично).

Випадковість розподілу символів по періоду означає відсутність закономірностей між появою різних символів в межах періоду.

По довжині періоду розрізняються гами з кінцевим і нескінченним періодом. Якщо довжина періоду гамми перевершує довжину тексту, що шифрується, гамма є істинно випадковою і не використовується для шифрування вдруге повідомлень, то таке перетворення є абсолютно стійким (досконалий шифр).

Гаммірування частіше здійснюється:

- по модулю 2, якщо відкритий текст представляється у вигляді бінарної послідовності;

- по модулю 256, якщо відкритий текст представляється у вигляді послідовності байтів;

- по модулю 10, якщо відкритий текст послідовність цифр.

***Ci = (Pi + Ki) mod N,***

***Pi = (Ci + N - Ki) mod N,***

де ***Pi***, -перший символ відкритого повідомлення;

***Ci*** -перший символ шифрованного повідомлення;

***N*** – кількість символів в алфавіті;

***Кi*** – перший символ гамми (ключа) генерується за допомогою ГПВЧ(генератор псевдовипадкових чисел) кількість згенерованих чисел повинно відповідати кількості літер в повідомленні, яке буде шифруватись. Якщо довжина гамми менше, ніж довжина повідомлення, тоді вона використовується повторно.

Повинні бути пред'явлені, такі умови для забезпечити достатню якість шифру:

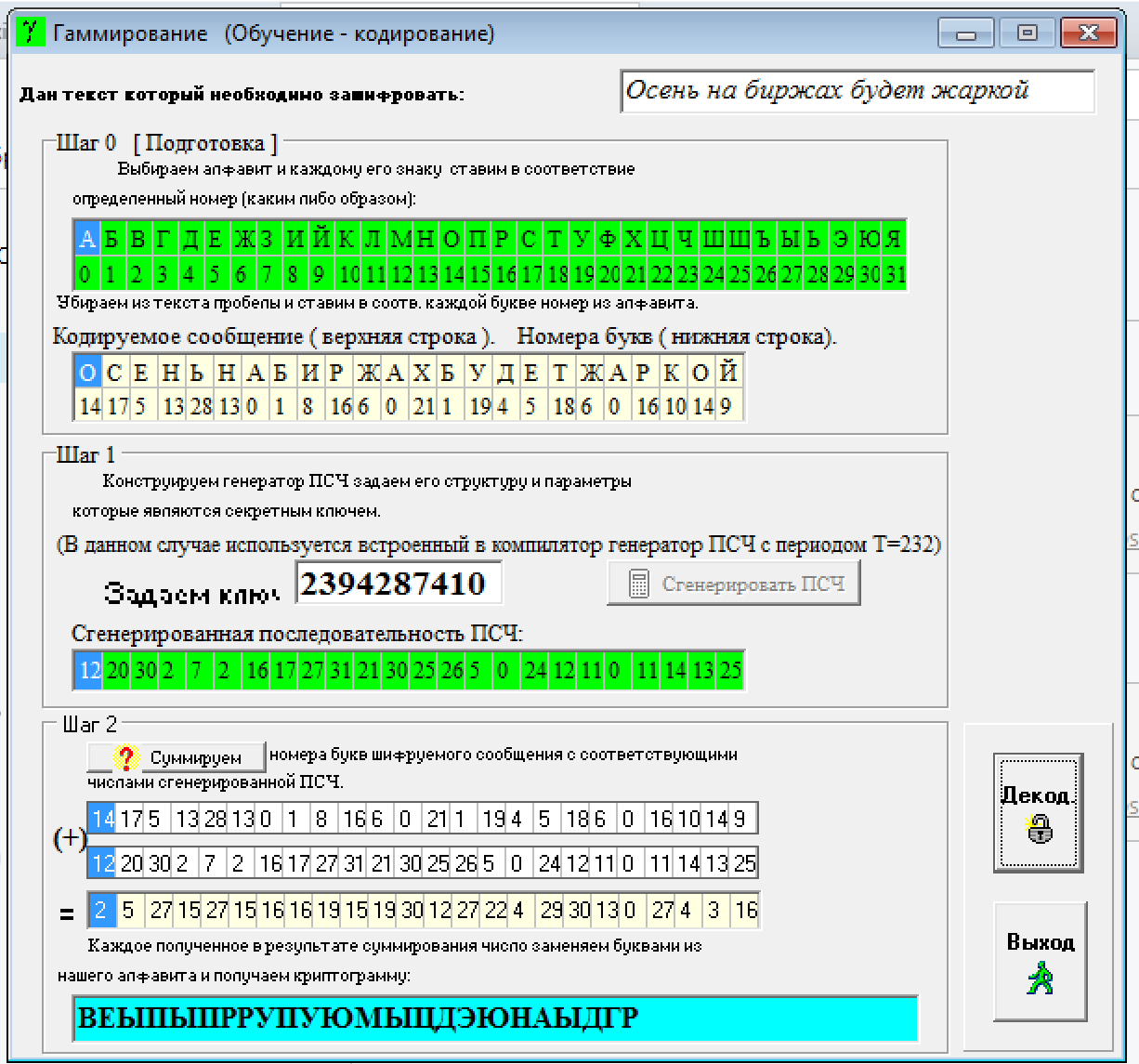
1. Необхідно, щоб період повторення генерування гами був досить великим, краще - максимально можливим. У всякому разі, він повинен перевершувати найбільшу можливу кількість символів в шифрованих повідомленні.

2. Необхідно, щоб сусідні або близькі по розташуванню елементи послідовності відрізнялися один від одного. Було б вкрай бажано, щоб відмінності між ними були в кожній позиції.

Сенс в тому, що метод гамування за своєю суттю вимагає одноразової гамми, інакше він легко розкривається по алгоритмічної лінії. Якщо ж період повторення вироблюваної гамми недостатньо великий, різні частини одного і того ж довгого повідомлення можуть виявитися зашифрованими за допомогою однакових ділянок гамми.

Друга вимога є менш очевидною, і має місце тільки для шифрів цілком певних архітектур, в яких крок шифрування є комбінацією декількох порівняно простих перетворень, в ході кожного з яких відмінності в шифрованих блоках даних збільшуються досить несуттєво.

Демонстрація роботи алгоритму:



**Висновок:** Перевагами метода гаммірування перед іншими методами являється висока криптостійкість при відносній простоті методу. Процедура кодування від процедури декодування нічим не відрізняється, процес сумування виконується через побітову операцію «виключення XOR». Використання поля Галуа дозволяє зроби процедуру кодування и декодування ідентичними.