ЗВІТ ПО ЛАБОРАТОРНІЙ РОБОТІ НОМЕР 4

ПРЕДМЕТУ КРИПТОГРАФІЯ

СТУДЕНТ: ПАНТЕЛЕЙЧУК ІЛЛЯ МИХАЙЛОВИЧ

**Короткі відомості про шифр**

Гамовий шифр - це метод шифрування, який використовує випадковий ключ під назвою «гама» для шифрування повідомлень. Шифри діапазону також відомі як потокові шифри та працюють шляхом поєднання символів відкритого тексту з відповідними символами діапазону за допомогою операції XOR.

**Вибраний ключ**

Я обрав таку послідовність символів в якості гами:

" WXYZABCDEFGHIJKLMNOPQRSTUV "

**Відкрите повідомлення**

Як відкрите повідомлення, я обрав речення “I am in love with a fairytale”.

Згідно з завданням потрібно замінити всі пропуски на BLN, тому наше вихідне повідомлення буде

“IBLNamBLNinBLNloveBLNwithBLNaBLNfairytale”

**Зашифроване повідомлення**

Ми будемо вираховувати кожний символ таким чином – брати символ з Вихідного повідомлення та віднімати його від символа з Гамми. Наприклад:

I -> 8, B -> 1, Г -> W -> 22 S = 22 - 8 = 14 (E)

B -> 1, L -> 11, О -> B -> 1 S = 1 - 11 = 16 (G)

N -> 13, a -> 0, О -> B -> 1 S = 13 - 0 = 13 (N)

И так далі...

Тому зашифроване повідомлення має вигляд як – “ EGNqdmEGQlnEGQsxEGQvrEGQoEGQwskbev ”

**Порядок зашифрування і розшифрування**

1. Створення гами: Ми вибрали послідовність гами в алфавіті.
2. Створення відкритого повідомлення: Відкрите повідомлення було створено з використанням латинських букв. Такой ми замінили всі пропуски на “BLN”
3. Зашифрування гамуванням: Для кожної букви відкритого повідомлення ми використовували формулу S = (Г - О) mod 26, де S - зашифрована буква, Г - буква з гами, О - буква з відкритого повідомлення (з урахуванням пропусків, ком та крапок).
4. Розшифрування зашифрованого повідомлення: Для розшифрування ми використовували формулу S = (О + Г) mod 26, використовуючи ту саму гаму, що і при шифруванні. Отримуємо вихідне повідомлення “IBLNamBLNinBLNloveBLNwithBLNaBLNfairytale”

**Висновки**

Гамовий шифр - це ефективний метод шифрування, який забезпечує високий рівень криптографічної безпеки, особливо при використанні одноразового ключа. Використовуючи правильний ключ та операцію XOR, ми змогли зашифрувати та розшифрувати відкрите повідомлення. Гамовий шифр важливий для багатьох систем зв'язку та інтернет-протоколів, де конфіденційність даних грає важливу роль.

ВІДПОВІДІ НА КОТРОЛЬНІ ЗАПИТАННЯ

1. **Основна суть шифрування гамуванням:**

У шифруванні гамуванням використовується гама (псевдовипадкова або повністю випадкова послідовність бітів), яка комбінується з відкритим текстом за допомогою побітової операції (зазвичай XOR). Суть полягає у тому, що кожен символ відкритого тексту (або біт) комбінується з відповідним символом гами, що призводить до шифрованого тексту.

1. **Класифікація гамувальних послідовностей та їхні розбіжності:**

* **За способом генерації:**
  + **Псевдовипадкові гама**: генеруються алгоритмами, що мають вигляд випадкової послідовності, але насправді є детермінованими.
  + **Повністю випадкові гама**: генеруються засобами випадкових подій у фізичних процесах (наприклад, випадковий шум в електроніці).
* **За періодичністю:**
  + **Періодичні гама**: мають період, після якого послідовність повторюється.
  + **Неперіодичні гама**: не мають повторюючихся візерунків у своїй послідовності. Розбіжності полягають у випадковості генерації і можливості передбачення наступних значень у псевдовипадкових гама, а також у способах застосування їх у криптографії.

1. **Відмітні риси шифрування гамуванням в порівнянні з іншими методами:**

* **Шифри заміни:** Замінюють символи відкритого тексту на інші символи згідно з ключем.
* **Коди:** Відображають символи відкритого тексту у числові або бітові послідовності.
* **Шифри перестановки:** Змінюють порядок символів відкритого тексту за допомогою ключа.

Відмітні риси гамування включають в себе велику стійкість до криптоаналізу, можливість безперервного потокового шифрування та здатність до ефективної реалізації на апаратному рівні.

1. **Криптографічна стійкість шифрування гамуванням:**

Криптографічна стійкість гамування залежить від якості гами та відповідного ключа. Повністю випадкові гама забезпечують найвищий рівень стійкості. Стійкість гамування забезпечується також відсутністю кореляцій між гамою та відкритим текстом.

1. **Спрощення побудови гамувальних послідовностей та їх вплив на стійкість:**
   1. **Лінійні зсувні реєстри (LFSR):** Дозволяють швидку генерацію гама, але можуть мати обмежену стійкість, особливо якщо короткий ключ.
   2. **Каскадні структури:** Комбінують декілька простих генераторів, що може підвищити стійкість, але збільшує складність реалізації та може збільшити вразливості. Спрощені методи можуть знизити загальну стійкість, особливо якщо ключі або генератори не вибрані з достатньою увагою до криптографічних аспектів.

Початок форми