Шифр гаммирования

Бакундукизе Эжид Принц НФИмд-01-21

21 сентября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма шифрования гаммированием

Выполнение лабораторной работы

Гаммирование

Гаммирование — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных

Схема шифрования гаммированием

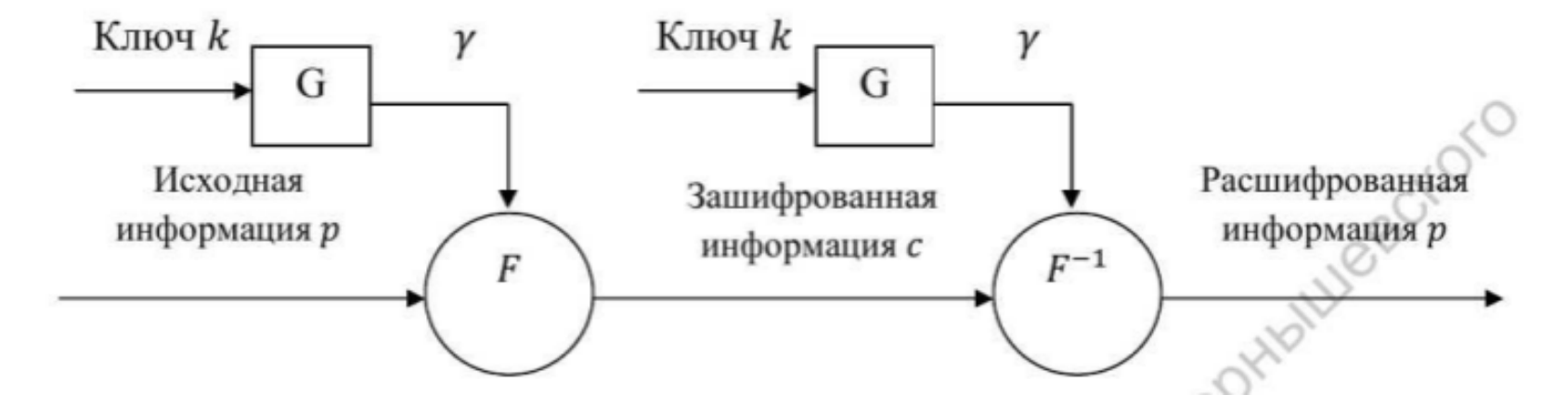

Figure 1: Схема шифрования гаммированием

Простейший генератор пседвослучайной последовательности

$$\gamma_i = a \cdot \gamma_{i-1} + b \; mod(m), i = \overline{1, m},$$

где γ_i – i-й член последовательности псевдослучайных чисел, a, γ_0, b – ключевые параметры. Такая последовательность состоит из целых чисел от 0 до $m - 1$. Если элементы γ_i и γ_j совпадут, то совпадут и последующие участки: $\gamma_{+1i} = \gamma_{j+1}$, $\gamma_{i+2} = \gamma_{j+2}$. Таким образом, ПСП является периодической. Знание периода гаммы существенно облегчает криптоанализ. Максимальная длина периода равна m. Для ее достижения необходимо удовлетворить следующим условиям:

1. b и m – взаимно простые числа;
2. $a - 1$ делится на любой простой делитель числа m;
3. $a - 1$ кратно 4, если m кратно 4.

Figure 2: Простейший генератор псевдослучайной последовательности

Стойкость алгоритма

Стойкость шифров зависит от характеристик гаммы - длины и равномерности распределения вероятностей появления знаков гаммы. При использовании генератора псевдослучайных последовательностей получаем бесконечную гамму.
Метод гаммирования становится бессильным, если известен фрагмент исходного текста и соответствующая ему шифрограмма. В этом случае простым вычитанием по модулю 2 получается отрезок псевдослучайной последовательности и по нему восстанавливается вся эта последовательность.

Пример работы алгоритма

```
In [24]: gamma()

Гамма: гамма
Текст для шифрования: приказ
Числа текста:  [16, 17, 9, 11, 1, 8]
числа гаммы:  [4, 1, 13, 13, 1]
Числа зашифрованного текста:  [20, 18, 22, 24, 2, 12]
Зашифрованный текст:  усхчбл
Дешифровка:  приказ
```

Figure 3: Работа алгоритма гаммирования

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритм шифрования с помощью гаммирования