ЛАБОРАТОРНАЯ РАБОТА №3

Шифрование гаммированием

Из всех схем шифрования простейшей и наиболее надежной является схема однократного использования (рис. 1). Формируется m- разрядная случайная двоичная последовательность – ключ шифра. Отправитель производит побитовое сложение по модулю два ($mod\ 2$) ключа

$$k = k_1 k_2 \dots k_i \dots k_m$$

и m- разрядной двоичной последовательности

$$p = p_1 p_2 \dots p_i \dots p_m,$$

соответствующей посылаемому сообщению:

$$c_i = p_i \oplus k_i, i = \overline{1, m},$$

где p_i – i-й бит исходного текста, k_i – i-й бит ключа, $\oplus$ – операция побитового сложения (XOR), c_i – i-й бит получившейся криптограммы

$$c = c_1 c_2 \dots c_i \dots c_m.$$

Операция побитного сложения является обратимой, т.е. $(x \oplus y) \oplus y = x$, поэтому дешифрование осуществляется повторным применением операции $\oplus$ к криптограмме:

$$p_i = c_i \oplus k_i, i = \overline{1, m}.$$

Рис. 1

Основным недостатком такой схемы является равенство объема ключевой информации и суммарного объема передаваемых сообщений. Данный недостаток можно убрать, использовав ключ в качестве «зародыша», порождающего

значительно более длинную ключевую последовательность. На рис. 2. представлена такая схема, которая и называется *гаммированием.*

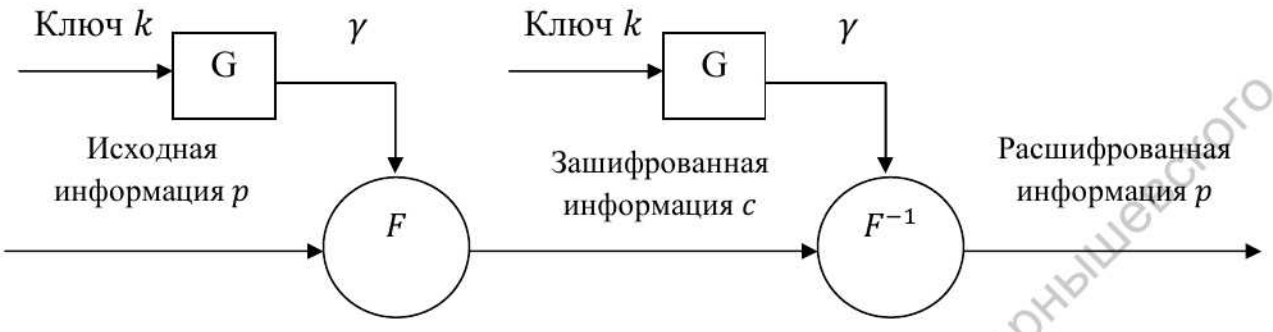

Рис. 2.

Гаммирование – процедура наложения при помощи некоторой функции F на исходный текст *гаммы* шифра, т.е. *псевдослучайной последовательности (ПСП)* с выходов генератора G. Псевдослучайная последовательность по своим статистическим свойствам неотличима от случайной последовательности, но является детерминированной, т.е. известен алгоритм ее формирования. Чаще Обычно в качестве функции F берется операция поразрядного сложения по модулю два или по модулю N (N – число букв алфавита открытого текста).

Простейший генератор псевдослучайной последовательности можно представить рекуррентным соотношением:

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

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: γ_{+1i}=γ_{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.

Стойкость шифров, основанных на процедуре гаммирования, зависит от характеристик гаммы – длины и равномерности распределения вероятностей появления знаков гаммы.

При использовании генератора ПСП получаем бесконечную гамму. Однако, возможен режим шифрования конечной гаммы. В роли конечной гаммы может выступать фраза. Как и ранее, используется алфавитный порядок букв, т.е. буква «а» имеет порядковый номер 1, «б» – 2 и т.д.

Например, зашифруем слово «ПРИКАЗ» («16 17 09 11 01 08») гаммой «ГАММА» («04 01 13 13 01»). Будем использовать операцию побитового сложения по модулю 33 ($mod\ 33$). Получаем:

$$c_1 = 16 + 4(mod\ 33) = 20 \qquad c_4 = 11 + 13(mod\ 33) = 24$$
$$c_2 = 17 + 1(mod\ 33) = 18 \qquad c_5 = 1 + 1(mod\ 33) = 2$$
$$c_3 = 9 + 13(mod\ 33) = 22 \qquad c_6 = 8 + 4(mod\ 33) = 12.$$

Криптограмма: «УСХЧБЛ» («20 18 22 24 02 12»).

Задания к лабораторной работе

Реализовать алгоритм шифрования гаммированием конечной гаммой.