ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 5
2012

А. В. Бабаш, **И. А. Никитина**, **К. А. Занина** (Москва, МЭСИ)**. Определение периода гаммы в шифре гаммирования по известному шифртексту.**

В историческом плане основными инструментами решения задачи, сформулированной в заглавии, выступали метод Фридмана, основанный на введенном им понятии «индекса совпадения» [1], и метод Фридриха Казиского, представленный в 1863 году [2]. Этот же метод независимо от Казиского был разработан советским криптографом Соколовым. Итак, уравнение шифрования имеет вид $b_j = a_j + \gamma_j \bmod 26$, $j \in \{1, 2, \ldots, N\}$, где $a_1 a_2 \ldots a_N$ — открытый текст, представленный номерами букв, $\gamma_1 \gamma_2 \ldots \gamma_N$ — гамма наложения, $b_1 b_2 \ldots b_N$ — шифрованный текст. Будем считать, что гамма наложения является локально периодической, т. е существует натуральное число d, $2d \leqslant N$, при котором для любого j, в случае $j + d \leqslant N$, выполняется равенство $\gamma_j = \gamma_{j+d}$. Период d такой последовательности определен неоднозначно. Предлагаемый метод состоит в следующем. Выписываются все пары номеров (j, j'), для которых $b_j = b_{j'}$. Пусть $\Pi(B, =)$ — множество таких пар. Очевидно, $|\Pi(B, =)| = \sum_{i \in I} F_i(F_i - 1)$, где F_i – частота встречаемости буквы i в шифртексте. Каждой паре (j, j') из $\Pi(B, =)$ ставится в соответствие расстояние $\rho(j, j')$, равное абсолютной величине разности между j и j'. Ищется такое максимальное по мощности подмножество $\Pi(B, d, =)$ пар в $\Pi(B, =)$, что их расстояния $\rho(j, j')$ имеют некоторый общий наибольший делитель d, отличный от 1. Подсчитывается величина ИБШ $(B, d) = |\Pi(B, d, =)|/(N(N-1))$ и сравнивается с величиной $\mathbf{E}_U(\text{ИБШ}(B, d)) = [(k+1)kr + k(k-1)(d-r)][N(N-1)]^{-1} \sum_i P_i^2$, где k, r определены равенством $N = kd + r$. Если эти величины близки, то принимается гипотеза о том, что шифрование проводилось гаммой периода d. В противном случае эта гипотеза отвергается.

Обоснование метода БШ. Для шифрованного текста $B = b_1 b_2 \ldots b_N$ величина ИБШ (B, d) равна вероятности $\mathbf{P}_B\{b_j = b'_j, d\}$ того, что при случайном и равновероятном выборе различных позиций j и j' с расстоянием, кратным d, элементы b_j и b'_j совпадут. Обозначим I_d^N множество всех локально-периодических последовательностей периода d.

Теорема. *Пусть шифртекст $B = B(N) = b_1 b_2 \ldots b_N$ получается шифрованием случайного текста $A(N)$ (выборки из распределения P_o) при помощи равновероятного выбора ключа $G(N)$ из I_d^N. Тогда вероятность $\mathbf{P}_Y\{b_j = b_{j'}, d)$ того, что при случайном и равновероятном выборе различных позиций j и j' с расстоянием, кратным d, элементы b_j и $b_{j'}$ случайного шифртекста B совпадут (имеется в виду вероятность совместного события: равенство букв на местах j, j' и кратность расстояния между ними величине d), равна величине $\mathbf{E}_U(\text{ИБШ}(B, d))$.*

При указанной вероятностной модели получения шифртекста данная вероятность совпадает с математическим ожиданием $\mathbf{E}$ (ИБШ (B, d)) случайной величины ИБШ (B, d).

СПИСОК ЛИТЕРАТУРЫ

1. *Бабаш А. В.* Криптографические и теоретико-автоматные аспекты современной защиты информации. М.: МЭСИ, 2009.
2. *King J. C.* An algorithm for the complete automated criptanalysis of periodic polyalphabetic substitution ciphers. — Cryptologia, 1994, v. 18, № 4, p. 332-355.