ОБОЗРЕНИЕ ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ МАТЕМАТИКИ

Том 20 **Выпуск 3**

2013

А. В. Бабаш, И. А. Никитина, К. А. Занина (Москва, МЭСИ). **Модернизированный метод Симпсона дешифрования шифра последовательной замены.**

Предполагается, что читатель знаком с методом Симпсона дешифрования шифра последовательной замены при известном периоде ключевой последовательности [1, 2].

Введем обозначения и напомним основные положения: K — некоторое множество подстановок на алфавите I; множество U ключей шифра — множество всех начальных слов длины N периодических последовательностей элементов из I периода d; $b_j = \sigma_j(a_j)$, $j \in \{1, 2, \ldots, N\}$ — уравнение шифрования, где $a_1, a_2, \ldots, a_N$ — открытый текст, $\sigma_1, \sigma_2, \ldots, \sigma_N \in U$; вводится взаимный индекс совпадения — $MI_C(J, J') = N^{-2} \sum_{i\in I} F_i F'_i$, где F_i (F'_i) — частота встречаемости буквы i в последовательности J (J') длины N; $MI_c(P, P') = \sum_{i\in I} P_i P'_i$ для двух вероятностных распределений $P = (P_i)_{i\in I}$ и $P' = (P'_i)_{i\in I}$ на I; для реализаций выборок J, J' одинаковой длины N из распределений P, P' пользуются с некоторой надежностью приближением $MI_C(J, J') \approx MI_c(P, P')$; $Po = (P1, P2, \ldots, P|I|)$ — вероятностное распределение букв содержательных открытых текстов; для σ из K вводится вероятностное распределение $P(\sigma^{-1}) = (P\sigma^{-1}(1), P\sigma^{-1}(2), \ldots, P\sigma^{-1}(|I|))$ на I, $P\sigma^{-1}(j)$ — вероятность j-й буквы (для ее расчета, исходя из набора $Po = (P1, P2, \ldots, P|I|)$, необходимо найти $\sigma^{-1}(j)$ — образ буквы j при подстановке σ^{-1}).

В методе Симпсона для дешифрования шифртекста $b_1, b_2, \ldots, b_N$ выполняются следующие операции: подсчитывается значение $MI_c(P(\sigma^{-1}), P(\sigma'^{-1}))$ для $(\sigma, \sigma') \in K \times K$; на основе этих значений проводится разбиение множества K на классы $k \subset K$ эквивалентности; подсчитываются значения взаимных индексов совпадения $MI_C(J(1), J(j))$, $j \in \{1, 2, \ldots, d\}$ $(J(j) = b_j, b_{j+d}, b_{j+2d}, \ldots)$; сравниваются значения $MI_C(J(1), J(j))$ с $MI_c(P(\sigma^{-1}), P(\sigma'^{-1}))$, $\sigma' \in K$; для каждого $j \in \{1, 2, \ldots, d\}$ находят наиболее близкое значение $MI_c(P(\sigma^{-1}), P(\sigma'^{-1}))$; этому значению соответствует некоторый класс эквивалентности $k(j)$. Для нахождения σ_1 его опробуемому варианту σ ставят в соответствие множество $\{\sigma, k(2), \ldots, k(d)\}$ значений вариантов отрезка $\sigma_1, \sigma_2, \ldots, \sigma_d$ ключевой последовательности. Первый элемент любого такого варианта есть σ, второй — произвольный элемент из класса $k(2)$, и т. д. Получают объединение множеств вариантов $\{\sigma, k(2), \ldots, k(d)\}$ по всем $\sigma \in K$. Задача решается опробованием вариантов этого множества.

Предлагаемая модернизация метода Симпсона состоит в использовании вместо взаимного индекса совпадения следующего модернизированного взаимного индекса совпадения ВЗ $(Po, J(j)) = \sum_{i\in I} P_i F_i^j / N_j$, где N_j — длина последовательности $J(j)$, F_i^j — частота буквы i в $J(j)$. В качестве искомой подстановки σ_j предлагается брать подстановки σ, для которых ВЗ $(Po, J(j)) \approx MI_c(Po, P(\sigma^{-1})) = \sum_{i\in I} P_i P_{\sigma^{-1}(i)}$. Трудоемкость решения задачи в этом случае будет такой же, как и в методе Симпсона при условии, что первая подстановка σ_1 известна.

СПИСОК ЛИТЕРАТУРЫ

1. *Бабаш А. В.*, *Шанкин Г. П.* Криптография. М.: СОЛОН-Р, 2002.
2. *Бабаш А. В.* Криптографические и теоретико-автоматные аспекты современной защиты информации. Т. 1. М.: МЭСИ, Евразийский открытый ин-т, 2010.