УДК 681.322

Некоторые особенности модулярных шифров

Несенчук А.А.
Белорусский национальный технический университет

Определим алфавит A: $A=\{a_i\}$, i=1, 2, …, m; $I=\{i\}$; $i_p \in I$, $i_c \in I$, где m – объем алфавита (например, m=26), i – порядковый номер символа в алфавите, a_i – некоторый символ алфавита, i_p, i_c – порядковые номера символов исходного текста и шифротекста в алфавите соответственно.

Формула шифрования для модулярного шифра [1] имеет вид

$$E_k(a_i)= i_p * k (\mathrm{mod}\ m)= i_c, \qquad (1)$$

где k – ключ шифрования (натуральное число). Тогда

$$1 \le i_p \le m \rightarrow k \le i_p \mathrm{k} \le mk. \qquad (2)$$

Для обеспечения взаимно-однозначного соответствия символов исходного и шифрованного текстов, т.е. обратимости шифра, ставится следующее условие [1]:

$$\mathrm{НОД}(k,m) = 1. \qquad (3)$$

Рассмотрим более детально влияние условия (3) на корректность шифрования/дешифрования информации с использованием шифра (1).

Утверждение 1. Для обеспечения обратимости шифра в пределах (2) при шифровании по алгоритму (1) требуется, чтобы значения i_c пробегали полную систему классов вычетов по модулю m: $\overline{1}, \overline{2}, \ldots, \overline{m}$ и не было бы ни одной пары значений, принадлежащих к одному классу, т.е. среди значений i_c не должно быть более одного нулевого вычета, i_c=0.

На этом основании сформулируем следующее утверждение.

Утверждение 2. Если для шифра по алгоритму (1) справедливо соотношение

$$\mathrm{НОК}[k,m] \ge km, \qquad (4)$$

то условие обратимости шифра выполняется.

НОК$[k,m]=j_d^{\,k}\, m$ или НОК$[k,m]=j_d^{\,m}\, k$, где $j_d^{\,k}$ – число делителей НОД(k,m) в значении k, $j_d^{\,m}$ – число НОД(k,m) в значении m. Следовательно, при выполнении условия (3) НОК$[k,m]$ = km, и шифр является обратимым.

Рис. 1 иллюстрирует справедливость приведенных выше утверждений.

i_p	вычет i_c	i_p	вычет i_c	i_p	вычет i_c
1 → 3	—	4 → 2	—	7 → 1	—
2 → 6	—	5 → 5	—	8 → 4	—
3 → 9	—	6 → 8	—	9	7

а)

i_p	вычет i_c	i_p	вычет i_c	i_p	вычет i_c
1 → 2	—	4 → 8	—	7 → 4	—
2 → 4	—	5 → 0	—	8 → 6	—
3 → 6	—	6 → 2	—	9 → 8	—

б)

Рис. 1. Значения i_p и i_c при шифровании по формуле (1): а) m=10, k=3; б) m=10, k=2

1. Романец, Ю.В., Тимофеев, П.А., Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001.