

Для вычисления хеш-образа будем использовать упрощенную хеш-функцию квадратичной свертки:

$$h_i = (h_{i-1} + M_i)^2 \bmod p, \quad (16)$$

где $h_0 = 0$, p – модуль алгоритма, M_i – коды символов сообщения. После обработки последнего символа текста получаем хеш-образ h всего сообщения.

Таблица 1

Алфавит «Русские буквы» (без символов Ё и Ы)

| | | | | | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| А | Б | В | Г | Д | Е | Ж | З | И | К | Л | М | Н | О | П | Р | С | Т | У | Ф |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | | | | | | | | | |
| Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | | | | | | | | | |

Пример 7. Вычислим хэш-функцию в виде квадратичной функции свертки (16) сообщения «МАША». Коды символов соответствуют номеру буквы в алфавите (табл. 1), p – модуль эллиптической кривой (1) из примера 6. Результаты промежуточных вычислений сведем в таблицу.

| i | Символы исходного сообщения M_i | Коды символов M_i | Вычисление хеш-образа h |
|-----|--|---------------------------|---|
| | | | $h_0 = 0$ |
| 1 | М | 14 | $h_1 = h_0 + M_1^2 \bmod p = 0 + 14^2 \bmod 11 = 9$ |
| 2 | А | 1 | $h_2 = h_1 + M_2^2 \bmod p = 9 + 1^2 \bmod 11 = 1$ |
| 3 | Ш | 26 | $h_3 = h_2 + M_3^2 \bmod p = 1 + 26^2 \bmod 11 = 3$ |
| 4 | А | 1 | $h_4 = h_3 + M_4^2 \bmod p = 3 + 1^2 \bmod 11 = 5$ |

Результатом является хэш-образ сообщения $h = 5$.