Лабораторная работа №4
Вариант 13

Куприева С И
872302

$p = 7, \quad q = 29$

① Найти хеш-образ своей фамилии, используя хеш-функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, где $n = p \cdot q$

$M = \{13, 22, 18, 19, 7, 7, 4, 2\}$

К	У	П	Р	Е	Е	В	А
13	22	18	19	7	7	4	2

'А' = 2
'Б' = 3
'В' = 4
...
'Я' = 34

Пусть $H_0 = 200$.

$H_1 = (200 + 13)^2 \bmod 203 = 100$
$H_2 = (100 + 22)^2 \bmod 203 = 65$
$H_3 = (65 + 18)^2 \bmod 203 = 190$
$H_4 = (190 + 19)^2 \bmod 203 = 36$
$H_5 = (36 + 7)^2 \bmod 203 = 22$
$H_6 = (22 + 7)^2 \bmod 203 = 29$
$H_7 = (29 + 4)^2 \bmod 203 = 174$
$H_8 = (174 + 2)^2 \bmod 203 = 92$

→ $h(M) = H_8 = 92$

② Показать как изменится хеш-образ при изменении 1 из букв фамилии

$M = \{13, 22, 18, 19, 11, 7, 4, 2\}$

К	У	П	Р	И	Е	В	А
13	22	18	19	11	7	4	2

$H_0 = 200$
$H_1 = (200 + 13)^2 \bmod 203 = 100$
$H_2 = (100 + 22)^2 \bmod 203 = 65$
$H_3 = (65 + 18)^2 \bmod 203 = 190$
$H_4 = (190 + 19)^2 \bmod 203 = 36$
$H_5 = (36 + 11)^2 \bmod 203 = 179$
$H_6 = (179 + 7)^2 \bmod 203 = 86$
$H_7 = (86 + 4)^2 \bmod 203 = 183$
$H_8 = (183 + 2)^2 \bmod 203 = 121$

→ $h(M') = H_8 = 121$ (+29)

③ Показать как изменится хеш-образ при перестановке 2 любых букв в фамилии

$M = \{13, 22, 18, 7, 19, 7, 4, 2\}$

К	У	П	Е	Р	Е	В	А
13	22	18	7	19	7	4	2

$H_0 = 200$
$H_1 = (200 + 13)^2 \bmod 203 = 100$
$H_2 = (100 + 22)^2 \bmod 203 = 65$
$H_3 = (65 + 18)^2 \bmod 203 = 190$
$H_4 = (190 + 7)^2 \bmod 203 = 36$
$H_5 = (36 + 8)^2 \bmod 203 = 183$
$H_6 = (183 + 7)^2 \bmod 203 = 169$
$H_7 = (169 + 4)^2 \bmod 203 = 88$
$H_8 = (88 + 2)^2 \bmod 203 = 183$

→ $h(M'') = H_8 = 183$ (+91)

④ Вычислить электронную цифровую подпись своей фамилии по схеме RSA.

$r = p \cdot q = 203$

$\varphi(r) = (p-1)\cdot(q-1) = 6 \cdot 28 = 168$

$$\begin{cases} НОД(K_o, \varphi(r)) = 1 \\ K_o < \varphi(r) \end{cases}, \quad \begin{cases} K_o \cdot K_c = 1 \bmod \varphi(r) \\ K_c < \varphi(r) \end{cases}$$

$НОД(5, 168) = НОД(168, 5)$

$168 = 5 \cdot 33 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1 \Rightarrow K_o = 5$

$2 = 1 \cdot 2 + 0$

$5K_c = 1 \bmod 203$

$K_c = 5^{\varphi(203)-1} \bmod 203 = 5^{167} \bmod 203 = \left((5^4)^{41} \cdot 5^3\right) \bmod 203 = \left(16^{41} \cdot 125\right) \bmod 203 =$

$= \left((16^2)^{20} \cdot 16 \cdot 125\right) \bmod 203 = \left(53^{20} \cdot 173\right) \bmod 203 = \left(170^{10} \cdot 173\right) \bmod 203 =$

$= \left(74^5 \cdot 173\right) \bmod 203 = \left(74^4 \cdot 173 \cdot 74\right) \bmod 203 = \left(198^2 \cdot 13\right) \bmod 203 =$

$= (25 \cdot 13) \bmod 203 = 122 (< 168)$

$K_c = 122; \quad K_o = 5; \quad m = h(M) = 92$

$S = m^{K_c} \bmod r$

$S = m^{K_c} \bmod r = 92^{122} \bmod 203 = 141^{61} \bmod 203 = \left(190^{30} \cdot 141\right) \bmod 203 = \left(169^{15} \cdot 141\right) \bmod 203 =$

$= \left(141^8 \cdot 169\right) \bmod 203 = \left(190^4 \cdot 169\right) \bmod 203 = \left(165^2 \cdot 169\right) \bmod 203 =$

$= (141 \cdot 169) \bmod 203 = 78$

$S = 78$