Ежегодная международная научно-практическая конференция
«РусКрипто’2023»

Обобщенный параметризованный алгоритм восстановления прообраза хеш-функции MD5 методом полного опробования

Коновалов Никита
студент 3-го курса аспирантуры НИЯУ «МИФИ»

Актуальность работы

Протоколы с MD5 ✓

- Сетевой протокол IKE
- Протокол хранения паролей в Unix/Linux системах
- Протокол парольной защиты файлов MS Office
- Протокол парольной защиты файлов PKSC #8
- Сетевой протокол Kerberos

Исследование семейства хеш-функций MD ✓

Исследование семейства хеш-функций SHA ✓

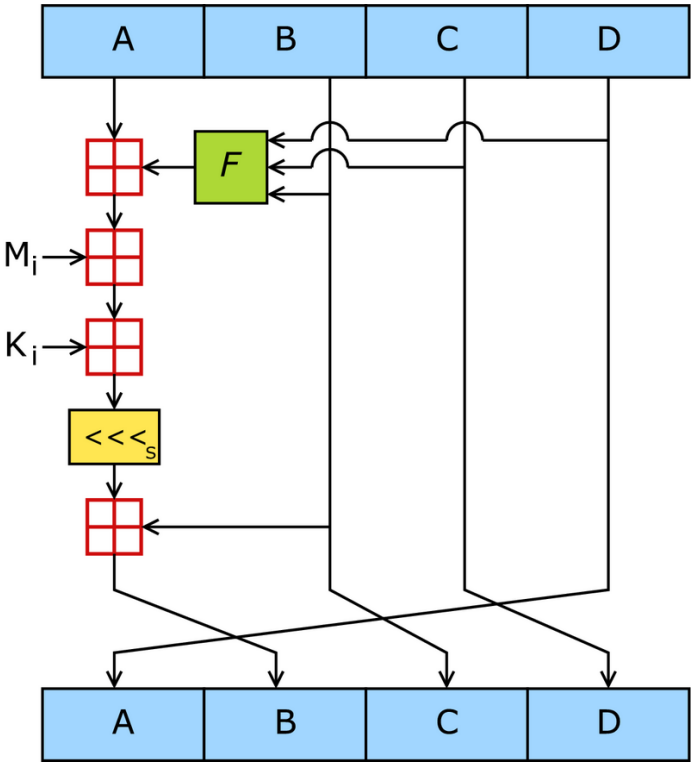
Хеш-функция MD5

Работа хеш-функции

$$\boldsymbol{C}\colon \{0,1\}^{(128)} \times \{0,1\}^{(512)} \to \{0,1\}^{(128)},$$
$$\boldsymbol{h_{i+1}} = C(h_i, M_i),$$
$$\boldsymbol{F}(\boldsymbol{M_0}, \dots, \boldsymbol{M_{p-1}}) = h_p, i = \{0, \dots, p-1\}.$$

Функции усложнения

$$\boldsymbol{W_0}(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}) = (x \wedge y) \vee (\bar{x} \wedge z),$$
$$\boldsymbol{W_1}(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}) = (x \wedge z) \vee (\bar{z} \wedge y),$$
$$\boldsymbol{W_2}(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}) = x \oplus y \oplus z,$$
$$\boldsymbol{W_3}(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}) = y \oplus (\bar{z} \vee y).$$



Константы

$$\boldsymbol{t_n} = int(2^{32} \cdot |\sin n|), n \in \{0, \dots, 63\}.$$

Начальные состояния

$$\boldsymbol{Q_{-4}} = 0x67452301,$$
$$\boldsymbol{Q_{-3}} = 0xefcdab89,$$
$$\boldsymbol{Q_{-2}} = 0x98badcfe,$$
$$\boldsymbol{Q_{-1}} = 0x10325476.$$

Обновление состояния

$$\boldsymbol{Q_0} = Q_{j-3} \boxplus \left(\left(Q_{j-4} \boxplus W_0(Q_{j-3}, Q_{j-2}, Q_{j-1}) \boxplus m_0 \boxplus t_0 \right) \lll s_0 \right),$$
$$\boldsymbol{Q_j} = Q_{j-3} \boxplus \left(\left(Q_{j-4} \boxplus W_f(Q_{j-1}, Q_{j-2}, Q_{j-3}) \boxplus m_{v_r(j)} \boxplus t_n \right) \lll s_j \right), j \in \{1, \dots, 63\}.$$

Хеш-функция MD5

Промежуточный результат

$$\boldsymbol{h_{i+1}^{(0)}} = Q_{-4} \boxplus Q_{60},$$
$$\boldsymbol{h_{i+1}^{(1)}} = Q_{-3} \boxplus Q_{61},$$
$$\boldsymbol{h_{i+1}^{(2)}} = Q_{-2} \boxplus Q_{62},$$
$$\boldsymbol{h_{i+1}^{(3)}} = Q_{-1} \boxplus Q_{63}.$$

Обновление состояний

$$\boldsymbol{Q_{-4}} = h_i^{(0)},$$
$$\boldsymbol{Q_{-3}} = h_i^{(1)},$$
$$\boldsymbol{Q_{-2}} = h_i^{(2)},$$
$$\boldsymbol{Q_{-1}} = h_i^{(3)}.$$

Результат работы

$$\boldsymbol{h} = \boldsymbol{h_p} = h_{p-1}^{(0)} \,||\, h_{p-1}^{(1)} \,||\, h_{p-1}^{(2)} \,||\, h_{p-1}^{(3)}.$$

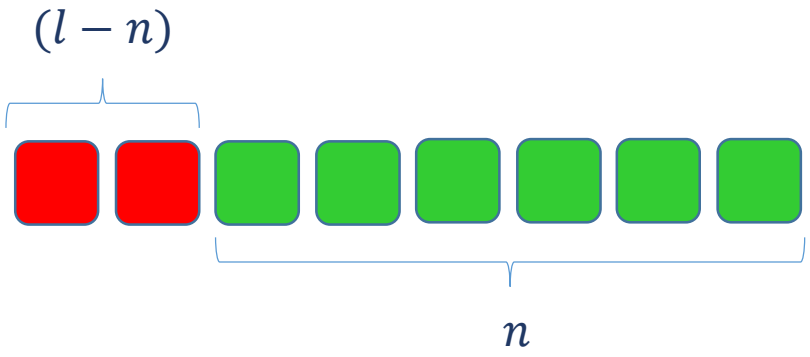
Операции над 32-х битными векторами	$\boxplus$	$\lll$	$\wedge$	$\vee$	$\oplus$	$\neg$
Количество операций	260	64	64	48	48	48

Алгоритм восстановления прообраза хеш-функции

Условия:

$\boldsymbol{H}$: $\{0,1\}^{(*)} \to \{0,1\}^{(n)}$,
$\bar{y} = H(\bar{x}), \bar{y} \in \bar{Y}, \bar{x} \in \bar{X}$;
$\bar{X} = \{0,1\}^{(K)}, \bar{Y} = \{0,1\}^{(n)}$.

$\bar{X} = \bar{X}^{(1)} \cup \cdots \cup \bar{X}^{(L)}, \bar{x}^{(l)} \in \bar{X}^{(l)}, l \in \{1, \ldots, L\}$;
$\bar{x}^{(l)} = \left(x_0^{(l)}, \ldots, x_{l-1}^{(l)}\right), x_q^{(l)} \in \{0,1\}$;
$\bar{X}^{(l)} = \bar{Z}^{(n)} \,||\, \bar{V}^{(l-n)}, n < l$.



Алгоритм 1

Вход: $\bar{y}, l, n, \bar{X}, H$.
Выход: $\bar{x}$ или $\emptyset$.
Алгоритм:

1. Пока $l \le L$:
   1.1 Для $\bar{X}^{(l)}$ зафиксировать n.
   1.2 Для каждого $\bar{v}_q^{(l-n)} \in \bar{V}^{(l-n)}$ ***(внешний цикл)***:
      1.2.1 Сформировать фиксированную часть m.
      1.2.2 Для каждого $\bar{z}_p^{(n)} \in \bar{Z}^{(n)}$ ***(внутренний цикл)***:
         1.2.2.1 Сформировать переменную часть m.
         1.2.2.2 Вычислить $\bar{y}' = H(\bar{z}_p^{(n)} \,||\, \bar{v}_q^{(l-n)})$.
         1.2.2.3 Если $\bar{y} = \bar{y}'$: вернуть $\bar{x}^{(l)} = \bar{z}_p^{(n)} \,||\, \bar{v}_q^{(l-n)}$ и закончить работу.
   1.3 Увеличить l.
1. Вернуть $\emptyset$ и закончить работу.

Обратимость хеш-функции MD5

Обратное преобразование обновления состояния

$$\boldsymbol{Q_{j-4}} = \left((Q_j \boxminus Q_{j-3}) \ggg s_j\right) \boxminus W_f\left(Q_{j-1}, Q_{j-2}, Q_{j-3}\right) \boxminus m^r_{v_r(j)}, j \in \{1, \dots, 63\}.$$

Обратное преобразование последних состояний

$$\begin{aligned}
\boldsymbol{Q_{60}} &= h^0 \boxminus Q_{-4},\\
\boldsymbol{Q_{61}} &= h^1 \boxminus Q_{-3},\\
\boldsymbol{Q_{62}} &= h^2 \boxminus Q_{-2},\\
\boldsymbol{Q_{63}} &= h^3 \boxminus Q_{-1}.
\end{aligned}$$

Оптимизация алгоритма восстановления прообраза MD5

Фиксируем все подблоки сообщения, кроме $\boldsymbol{m_0}$, получаем последние состояния:

$$\boldsymbol{Q_{63}} = h^{(3)} \boxminus Q_{-1},$$
$$\boldsymbol{Q_{62}} = h^{(2)} \boxminus Q_{-2},$$
$$\boldsymbol{Q_{61}} = h^{(1)} \boxminus Q_{-3},$$
$$\boldsymbol{Q_{60}} = h^{(0)} \boxminus Q_{-4},$$

Применяя свойство обратимости, получаем промежуточные состояния:

$$\boldsymbol{Q_{59}} = ((Q_{63} \boxminus Q_{60}) \ggg 21) \boxminus W_3(Q_{62}, Q_{61}, Q_{60}) \boxminus m_{15}^{(63)},$$
$$\ldots,$$
$$\boldsymbol{Q_{48}} = ((Q_{52} \boxminus Q_{49}) \ggg 12) \boxminus W_3(Q_{62}, Q_{61}, Q_{60}) \boxminus m_{12}^{(52)},$$
$$\boldsymbol{Q_{47}} = ((Q_{51} \boxminus Q_{48}) \ggg 21) \boxminus W_3(Q_{62}, Q_{61}, Q_{60}) \boxminus m_{5}^{(51)},$$
$$\boldsymbol{Q_{46}} = ((Q_{50} \boxminus Q_{47}) \ggg 15) \boxminus W_3(Q_{62}, Q_{61}, Q_{60}) \boxminus m_{14}^{(50)},$$
$$\boldsymbol{Q_{45}} = ((Q_{49} \boxminus Q_{46}) \ggg 10) \boxminus W_3(Q_{62}, Q_{61}, Q_{60}) \boxminus m_{7}^{(49)}.$$

Оптимизация алгоритма восстановления прообраза MD5

$$Q_{j-4} = \left((Q_j \boxminus Q_{j-3}) \ggg s_j\right) \boxminus W_f(Q_{j-1}, Q_{j-2}, Q_{j-3}) \boxminus m^r_{v_r(j)}, j \in \{1, \dots, 63\}.$$

1

$m_0 \to Q_0$	$m_1 \to Q_1$	$m_2 \to Q_2$	$m_3 \to Q_3$
$m_4 \to Q_4$	$m_5 \to Q_5$	$m_6 \to Q_6$	$m_7 \to Q_7$
$m_8 \to Q_8$	$m_9 \to Q_9$	$m_{10} \to Q_{10}$	$m_{11} \to Q_{11}$
$m_{12} \to Q_{12}$	$m_{13} \to Q_{13}$	$m_{14} \to Q_{14}$	$m_{15} \to Q_{15}$

2

$m_1 \to Q_{16}$	$m_6 \to Q_{17}$	$m_{11} \to Q_{18}$	$m_0 \to Q_{19}$
$m_5 \to Q_{20}$	$m_{10} \to Q_{21}$	$m_{15} \to Q_{22}$	$m_4 \to Q_{23}$
$m_9 \to Q_{24}$	$m_{14} \to Q_{25}$	$m_3 \to Q_{26}$	$m_8 \to Q_{27}$
$m_{13} \to Q_{28}$	$m_2 \to Q_{29}$	$m_7 \to Q_{30}$	$m_{12} \to Q_{31}$

3

$m_5 \to Q_{32}$	$m_8 \to Q_{33}$	$m_{11} \to Q_{34}$	$m_{14} \to Q_{35}$
$m_1 \to Q_{36}$	$m_4 \to Q_{37}$	$m_7 \to Q_{38}$	$m_{10} \to Q_{39}$
$m_{13} \to Q_{40}$	$m_0 \to Q_{41}$	$m_3 \to Q_{42}$	$m_6 \to Q_{43}$
$m_9 \to Q_{44}$	$m_{12} \to Q_{45}$	$m_{15} \to Q_{46}$	$m_2 \to Q_{47}$

4

$m_0 \to Q_{48}$	$m_7 \to Q_{49}$	$m_{14} \to Q_{50}$	$m_5 \to Q_{51}$
$m_{12} \to Q_{52}$	$m_3 \to Q_{53}$	$m_{10} \to Q_{54}$	$m_1 \to Q_{55}$
$m_8 \to Q_{56}$	$m_{15} \to Q_{57}$	$m_6 \to Q_{58}$	$m_{13} \to Q_{59}$
$m_4 \to Q_{60}$	$m_{11} \to Q_{61}$	$m_2 \to Q_{62}$	$m_9 \to Q_{63}$

Оптимизация алгоритма восстановления прообраза MD5

Частный случай:

$0 < l \leq 160$ *бит;*

49 шагов.

Возможность восстановления при:

$0 < l \leq 448$ *бит.*

[1] *Steube, J. Optimizing computation of Hash-Algorithms as an attacker. 2013. WEB – https://hashcat.net/events/p13/js-ocohaaaa.pdf.*

[2] *Jie, W., Qiang, W. & Can-qun, Y. (2011). OpenCL-based MD5 Decryption Algorithm. Computer Engineering, vol.37, no.4, pp.119-121.*

[3] *Wang, F., Yang, C., Wu, Q., & Shi, Z. (2012, July). Constant memory optimizations in MD5 Crypt cracking algorithm on GPU-accelerated supercomputer using CUDA. In Computer Science & Education (ICCSE), 2012 7th International Conference on (pp. 638-642). IEEE.*

Алгоритм 2.1

Вход: $h, l, \bar{X}$.
Выход: $\bar{x}$ или $\emptyset$.
Алгоритм:

1. Пока $l \leq L$:
   1.1 Для $\bar{X}^{(l)}$ зафиксировать $n, n \leq 32$.
   1.2 Для каждого $\bar{v}_q^{(l-n)} \in \bar{V}^{(l-n)}$ ***(внешний цикл)***:
      1.2.1 Зафиксировать $m_1, \ldots, m_{15}; m_0 = 0$.
      1.2.2 Вычислить $Q_{45}, Q_{46}, Q_{47}, Q_{48}$.
      1.2.3 Для каждого $\bar{z}_p^{(n)} \in \bar{Z}^{(n)}$ ***(внутренний цикл)***:
         1.2.3.1 Зафиксировать m_0.
         1.2.3.2 Вычислить $Q'_{45}, Q'_{46}, Q'_{47}, Q'_{48}$.
         1.2.3.3 Если выполняются равенства

$$Q'_{45} = Q_{45},$$
$$Q'_{46} = Q_{46},$$
$$Q'_{47} = Q_{47},$$
$$Q'_{48} = Q_{48},$$

      вернуть $\bar{x}^{(l)}$ и закончить работу.
   1.3 Увеличить l.
2. Вернуть $\emptyset$ и закончить работу.

Обобщенный параметризованный алгоритм восстановления прообраза MD5

$$Q_{j-4} = \left((Q_j \boxplus Q_{j-3}) \ggg s_j\right) \boxplus W_f(Q_{j-1}, Q_{j-2}, Q_{j-3}) \boxplus m^r_{v_r(j)}, j \in \{1, \dots, 63\}.$$

1

$m_0 \to Q_0$	$m_1 \to Q_1$	$m_2 \to Q_2$	$m_3 \to Q_3$
$m_4 \to Q_4$	$m_5 \to Q_5$	$m_6 \to Q_6$	$m_7 \to Q_7$
$m_8 \to Q_8$	$m_9 \to Q_9$	$m_{10} \to Q_{10}$	$m_{11} \to Q_{11}$
$m_{12} \to Q_{12}$	$m_{13} \to Q_{13}$	$m_{14} \to Q_{14}$	$m_{15} \to Q_{15}$

2

$m_1 \to Q_{16}$	$m_6 \to Q_{17}$	$m_{11} \to Q_{18}$	$m_0 \to Q_{19}$
$m_5 \to Q_{20}$	$m_{10} \to Q_{21}$	$m_{15} \to Q_{22}$	$m_4 \to Q_{23}$
$m_9 \to Q_{24}$	$m_{14} \to Q_{25}$	$m_3 \to Q_{26}$	$m_8 \to Q_{27}$
$m_{13} \to Q_{28}$	$m_2 \to Q_{29}$	$m_7 \to Q_{30}$	$m_{12} \to Q_{31}$

3

$m_5 \to Q_{32}$	$m_8 \to Q_{33}$	$m_{11} \to Q_{34}$	$m_{14} \to Q_{35}$
$m_1 \to Q_{36}$	$m_4 \to Q_{37}$	$m_7 \to Q_{38}$	$m_{10} \to Q_{39}$
$m_{13} \to Q_{40}$	$m_0 \to Q_{41}$	$m_3 \to Q_{42}$	$m_6 \to Q_{43}$
$m_9 \to Q_{44}$	$m_{12} \to Q_{45}$	$m_{15} \to Q_{46}$	$m_2 \to Q_{47}$

4

$m_0 \to Q_{48}$	$m_7 \to Q_{49}$	$m_{14} \to Q_{50}$	$m_5 \to Q_{51}$
$m_{12} \to Q_{52}$	$m_3 \to Q_{53}$	$m_{10} \to Q_{54}$	$m_1 \to Q_{55}$
$m_8 \to Q_{56}$	$m_{15} \to Q_{57}$	$m_6 \to Q_{58}$	$m_{13} \to Q_{59}$
$m_4 \to Q_{60}$	$m_{11} \to Q_{61}$	$m_2 \to Q_{62}$	$m_9 \to Q_{63}$

Обобщенный параметризованный алгоритм восстановления прообраза MD5

Алгоритм 2.2

Вход: $h, l, \bar{X}$.
Выход: $\bar{x}$ или $\emptyset$.
Алгоритм:
1. Пока $l \leq L$:
 1.1 Для $\bar{X}^{(l)}$ зафиксировать $n, n \leq 32$.
 1.2 Для каждого $\bar{v}_q^{(l-n)} \in \bar{V}^{(l-n)}$ ***(внешний цикл)***:
  1.2.1 Зафиксировать $m_0, \ldots, m_{15}; m_4 = 0$.
  1.2.2 Вычислить Q_0, Q_1, Q_2, Q_3.
  1.2.3 Вычислить $Q_{57}, Q_{58}, Q_{59}, Q_{60}$.
  1.2.4 Для каждого $\bar{z}_p^{(n)} \in \bar{Z}^{(n)}$ ***(внутренний цикл)***:
   1.2.4.1 Зафиксировать m_4.
   1.2.4.2 Для состояний Q_0, Q_1, Q_2, Q_3 вычислить $Q_{57}', Q_{58}', Q_{59}', Q_{60}'$.
   1.2.4.3 Если выполняются равенства

$$Q_{57}' = Q_{57},$$
$$Q_{58}' = Q_{58},$$
$$Q_{59}' = Q_{59},$$
$$Q_{60}' = Q_{60},$$

   вернуть $\bar{x}^{(l)}$ и закончить работу.
  1.3 Увеличить l.
2. Вернуть $\emptyset$ и закончить работу.

Параметры:

$$\bar{X}^{(l)} = \bar{V}_0^{(128)} \,||\, \bar{Z}^{(n)} \,||\, \bar{V}_1^{(l-n-128)},$$

$$\bar{V}^{(l-n)} = \bar{V}_0^{(128)} \,||\, \bar{V}_1^{(l-n-128)},$$

$$160 < l \leq 288 \text{ бит},$$

57 шагов.

Обобщенный параметризованный алгоритм восстановления прообраза MD5

$$Q_{j-4} = \left((Q_j \boxplus Q_{j-3}) \ggg s_j\right) \boxplus W_f(Q_{j-1}, Q_{j-2}, Q_{j-3}) \boxplus m^r_{v_r(j)}, j \in \{1, \dots, 63\}.$$

1

$m_0 \to Q_0$	$m_1 \to Q_1$	$m_2 \to Q_2$	$m_3 \to Q_3$
$m_4 \to Q_4$	$m_5 \to Q_5$	$m_6 \to Q_6$	$m_7 \to Q_7$
$m_8 \to Q_8$	$m_9 \to Q_9$	$m_{10} \to Q_{10}$	$m_{11} \to Q_{11}$
$m_{12} \to Q_{12}$	$m_{13} \to Q_{13}$	$m_{14} \to Q_{14}$	$m_{15} \to Q_{15}$

2

$m_1 \to Q_{16}$	$m_6 \to Q_{17}$	$m_{11} \to Q_{18}$	$m_0 \to Q_{19}$
$m_5 \to Q_{20}$	$m_{10} \to Q_{21}$	$m_{15} \to Q_{22}$	$m_4 \to Q_{23}$
$m_9 \to Q_{24}$	$m_{14} \to Q_{25}$	$m_3 \to Q_{26}$	$m_8 \to Q_{27}$
$m_{13} \to Q_{28}$	$m_2 \to Q_{29}$	$m_7 \to Q_{30}$	$m_{12} \to Q_{31}$

3

$m_5 \to Q_{32}$	$m_8 \to Q_{33}$	$m_{11} \to Q_{34}$	$m_{14} \to Q_{35}$
$m_1 \to Q_{36}$	$m_4 \to Q_{37}$	$m_7 \to Q_{38}$	$m_{10} \to Q_{39}$
$m_{13} \to Q_{40}$	$m_0 \to Q_{41}$	$m_3 \to Q_{42}$	$m_6 \to Q_{43}$
$m_9 \to Q_{44}$	$m_{12} \to Q_{45}$	$m_{15} \to Q_{46}$	$m_2 \to Q_{47}$

4

$m_0 \to Q_{48}$	$m_7 \to Q_{49}$	$m_{14} \to Q_{50}$	$m_5 \to Q_{51}$
$m_{12} \to Q_{52}$	$m_3 \to Q_{53}$	$m_{10} \to Q_{54}$	$m_1 \to Q_{55}$
$m_8 \to Q_{56}$	$m_{15} \to Q_{57}$	$m_6 \to Q_{58}$	$m_{13} \to Q_{59}$
$m_4 \to Q_{60}$	$m_{11} \to Q_{61}$	$m_2 \to Q_{62}$	$m_9 \to Q_{63}$

Обобщенный параметризированный алгоритм восстановления прообраза MD5

Вход: $h, l, \bar{X}$.
Выход: $\bar{x}$ или $\emptyset$.
Алгоритм:

Алгоритм 2.3

1. Пока $l \leq L$:
   1.1 Для $\bar{X}^{(l)}$ зафиксировать $n, n \leq 32$.
   1.2 Для каждого $\bar{v}_q^{(l-n)} \in \bar{V}^{(l-n)}$ ***(внешний цикл)***:
      1.2.1 Зафиксировать $m_0, \ldots, m_{15}; m_8 = 0$.
      1.2.2 Вычислить Q_4, Q_5, Q_6, Q_7.
      1.2.3 Вычислить $Q_{53}, Q_{54}, Q_{55}, Q_{56}$.
      1.2.4 Для каждого $\bar{z}_p^{(n)} \in \bar{Z}^{(n)}$ ***(внутренний цикл)***:
         1.2.4.1 Зафиксировать m_8.
         1.2.4.2 Для состояний Q_4, Q_5, Q_6, Q_7 вычислить $Q'_{53}, Q'_{54}, Q'_{55}, Q'_{56}$.
         1.2.4.3 Если выполняются равенства

$$Q'_{53} = Q_{53},$$
$$Q'_{54} = Q_{54},$$
$$Q'_{55} = Q_{55},$$
$$Q'_{56} = Q_{56},$$

      вернуть $\bar{x}^{(l)}$ и закончить работу.
   1.3 Увеличить l.
2. Вернуть $\emptyset$ и закончить работу.

Параметры:

$$\bar{X}^{(l)} = \bar{V}_0^{(256)} \,||\, \bar{Z}^{(n)} \,||\, \bar{V}_1^{(l-n-256)},$$

$$\bar{V}^{(l-n)} = \bar{V}_0^{(256)} \,||\, \bar{V}_1^{(l-n-256)},$$

$$288 < l \leq 416 \text{ бит},$$

49 шагов.

Обобщенный параметризованный алгоритм восстановления прообраза MD5

$$Q_{j-4} = \left((Q_j \boxplus Q_{j-3}) \ggg s_j\right) \boxplus W_f(Q_{j-1}, Q_{j-2}, Q_{j-3}) \boxplus m^r_{v_r(j)}, j \in \{1, \dots, 63\}.$$

1

$m_0 \to Q_0$	$m_1 \to Q_1$	$m_2 \to Q_2$	$m_3 \to Q_3$
$m_4 \to Q_4$	$m_5 \to Q_5$	$m_6 \to Q_6$	$m_7 \to Q_7$
$m_8 \to Q_8$	$m_9 \to Q_9$	$m_{10} \to Q_{10}$	$m_{11} \to Q_{11}$
$m_{12} \to Q_{12}$	$m_{13} \to Q_{13}$	$m_{14} \to Q_{14}$	$m_{15} \to Q_{15}$

2

$m_1 \to Q_{16}$	$m_6 \to Q_{17}$	$m_{11} \to Q_{18}$	$m_0 \to Q_{19}$
$m_5 \to Q_{20}$	$m_{10} \to Q_{21}$	$m_{15} \to Q_{22}$	$m_4 \to Q_{23}$
$m_9 \to Q_{24}$	$m_{14} \to Q_{25}$	$m_3 \to Q_{26}$	$m_8 \to Q_{27}$
$m_{13} \to Q_{28}$	$m_2 \to Q_{29}$	$m_7 \to Q_{30}$	$m_{12} \to Q_{31}$

3

$m_5 \to Q_{32}$	$m_8 \to Q_{33}$	$m_{11} \to Q_{34}$	$m_{14} \to Q_{35}$
$m_1 \to Q_{36}$	$m_4 \to Q_{37}$	$m_7 \to Q_{38}$	$m_{10} \to Q_{39}$
$m_{13} \to Q_{40}$	$m_0 \to Q_{41}$	$m_3 \to Q_{42}$	$m_6 \to Q_{43}$
$m_9 \to Q_{44}$	$m_{12} \to Q_{45}$	$m_{15} \to Q_{46}$	$m_2 \to Q_{47}$

4

$m_0 \to Q_{48}$	$m_7 \to Q_{49}$	$m_{14} \to Q_{50}$	$m_5 \to Q_{51}$
$m_{12} \to Q_{52}$	$m_3 \to Q_{53}$	$m_{10} \to Q_{54}$	$m_1 \to Q_{55}$
$m_8 \to Q_{56}$	$m_{15} \to Q_{57}$	$m_6 \to Q_{58}$	$m_{13} \to Q_{59}$
$m_4 \to Q_{60}$	$m_{11} \to Q_{61}$	$m_2 \to Q_{62}$	$m_9 \to Q_{63}$

Обобщенный параметризированный алгоритм восстановления прообраза MD5

Алгоритм 2.4

Вход: $h, l, \bar{X}$.
Выход: $\bar{x}$ или $\emptyset$.
Алгоритм:
1. Пока $l \leq L$:
 1.1 Для $\bar{X}^{(l)}$ зафиксировать $n, n \leq 32$.
 1.2 Для каждого $\bar{v}_q^{(l-n)} \in \bar{V}^{(l-n)}$ ***(внешний цикл)***:
  1.2.1 Зафиксировать $m_0, \ldots, m_{15}; m_{12} = 0$.
  1.2.2 Вычислить $Q_9, Q_{10}, Q_{11}, Q_{12}$.
  1.2.3 Вычислить $Q_{49}, Q_{50}, Q_{51}, Q_{52}$.
  1.2.4 Для каждого $\bar{z}_p^{(n)} \in \bar{Z}^{(n)}$ ***(внутренний цикл)***:
   1.2.4.1 Зафиксировать m_{12}.
   1.2.4.2 Для состояний $Q_9, Q_{10}, Q_{11}, Q_{12}$ вычислить $Q'_{49}, Q'_{50}, Q'_{51}, Q'_{52}$.
   1.2.4.3 Если выполняются равенства

$$Q'_{49} = Q_{49},$$
$$Q'_{50} = Q_{50},$$
$$Q'_{51} = Q_{51},$$
$$Q'_{52} = Q_{52},$$

   вернуть $\bar{x}^{(l)}$ и закончить работу.
  1.3 Увеличить l.
2. Вернуть $\emptyset$ и закончить работу.

Параметры:

$$\bar{X}^{(l)} = \bar{V}_0^{(384)} \,||\, \bar{Z}^{(n)} \,||\, \bar{V}_1^{(l-n-384)},$$

$$\bar{V}^{(l-n)} = \bar{V}_0^{(384)} \,||\, \bar{V}_1^{(l-n-384)},$$

$$416 < l \leq 440 \text{ бит},$$

41 шаг.

Сравнение результатов

Параметр	*Количество шагов обновления состояния во внутреннем цикле*	*Сокращение количества шагов обновления состояния во внутреннем цикле в сравнении со классической реализацией*
$0 < l \leq 160$	*49*	*23%*
$160 < l \leq 288$	*57*	*11%*
$288 < l \leq 416$	*49*	*23%*
$\mathbf{416 < l \leq 440}$	***41***	***36%***

Контактная информация

Электронная почта:

nikitakonovalov2013@yandex.ru

Телефон:

+7-987-555-14-97

Спасибо за внимание!