НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Функція гешування

ДСТУ 7564:2014

Видання офіційне

БЗ № 12–2014/459

Київ
МІНЕКОНОМРОЗВИТКУ УКРАЇНИ
2015

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: Приватне акціонерне товариство «Інститут інформаційних технологій»

РОЗРОБНИКИ: **А. Бойко,** канд. техн. наук; **І. Горбенко,** д-р техн. наук (науковий керівник); **Ю. Горбенко,** канд. техн. наук; **О. Дирда,** канд. техн. наук; **В. Долгов,** д-р техн. наук; **О. Казимиров; О. Кузнецов,** д-р техн. наук; **Р. Олійников,** канд. техн. наук; **А. Пушкарьов; В. Руженцев,** канд. техн. наук

2 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ: наказ Мінекономрозвитку України від 2 грудня 2014 № 1431 з 2015–04–01

3 УВЕДЕНО ВПЕРШЕ

ЗМІСТ

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Функція гешування

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Функция хэширования

INFORMATION TECHNOLOGIES

CRYPTOGRAPHIC DATA SECURITY

Hash function

Чинний від 2015–04–01

1 СФЕРА ЗАСТОСУВАННЯ

Цей стандарт установлює алгоритм обчислення геш-значення для послідовностей двійкових символів, що застосовують у криптографічних методах захисту, для забезпечення цілісності та автентичності інформації під час її передавання, оброблення і зберігання, зокрема під час використання електронного цифрового підпису, що визначений у ДСТУ 4145.

Стандарт використовують під час розроблення засобів криптографічного захисту інформації в інформаційно-телекомунікаційних системах, а також під час модернізації діючих систем.

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому стандарті є посилання на такий нормативний документ:

ДСТУ 4145–2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті вжито такі терміни та визначення позначених ними понять:

3.1 байт

Впорядкована бітова послідовність, що складається з восьми бітів (елемент векторного простору V_8, який заданий над скінченним полем $GF(2)$)

3.2 біт

Двійковий розряд, що може приймати значення 0 або 1 (елемент скінченного поля $GF(2)$)

3.3 бітова послідовність

Впорядкована послідовність бітів (елемент векторного простору V_k, $k \in Z^+$)

3.4 вектор ініціалізації

Бітова послідовність фіксованої довжини (512 або 1024 біти), що використовують як початкове значення під час обчислення геш-значення

Видання офіційне

3.5 внутрішній стан

Бітова послідовність фіксованої довжини (512 або 1024 біти), що є проміжним значенням на кожній ітерації перетворення функції гешування, а також вхідним та вихідним значенням перетворень $T_l^{\oplus}$ і T_l^{+}

3.6 геш-значення; геш-вектор

Бітова послідовність фіксованої довжини ($n = 8 \cdot s$, $s \in \{1,2,...,64\}$), що є результатом роботи функції гешування

3.7 гешування

Обчислення геш-значення повідомлення (бітової послідовності)

3.8 довжина бітової послідовності

Кількість бітів, що складають бітову послідовність

3.9 доповнення

Вставка додаткових біт у кінець повідомлення для отримання кратності довжини бітової послідовності довжині внутрішнього стану функції гешування

3.10 многочлен *f*(*x*) степеня *m* над полем *GF*(2)

Многочлен $f(x) = x^m + q_{m-1}x^{m-1} + ... + q_0$, де коефіцієнти $q_1 \in GF(2)$, $i = 0, ..., m - 1$

3.11 незвідний многочлен над полем *GF*(2)

Многочлен ненульового степеня, що ділиться над полем $GF(2)$ без залишку тільки на самого себе і одиницю

3.12 повідомлення

Бітова послідовність довжини від 0 біт (порожній рядок) до $2^{96} - 1$ біт

3.13 просте поле *GF*(2)

Поле, що містить два елементи: 0 і 1

3.14 розширення простого поля *GF*(2)

Скінченне поле $GF(2^m)$, яке є розширенням степеня m поля $GF(2)$. За означенням це поле має характеристику 2

3.15 функція гешування

Криптографічне перетворення повідомлення M довжини від 0 біт (порожній рядок) до $2^{96} - 1$ біт у геш-значення (геш-вектор) $H(M)$, що є двійковим рядком фіксованої довжини n ($n = 8 \cdot s$, $s \in \{1,2,...,64\}$).

4 ПОЗНАКИ ТА СКОРОЧЕННЯ

У цьому стандарті використано такі познаки:

$\oplus$ — операція додавання за модулем 2 (XOR) бітових послідовностей однакової довжини $p = (p_1, p_2,..., p_k)$ і $q = (q_1, q_2,..., q_k)$, $k \in Z^+$, якщо кожен біт результуючої послідовності $r = (r_1, r_2,..., r_k)$ обчислюють за формулою $r_i = (p_i + q_i)(\text{mod}2)$;

$\otimes$ — операція скалярного добутку двох векторів над скінченним полем;

<< — операція зсуву ліворуч бітової послідовності фіксованої довжини (у бік старших розрядів; молодші розряди заповнюють 0), кількість розрядів, на котрі здійснюється зсув, визначають іншим аргументом;

$(a_0, a_1,..., a_k)^T$ — операція транспонування вектора, тобто подання вектора-рядка $(a_0, a_1,..., a_k)$ як вектора-стовпця $\begin{pmatrix} a_0 \\ a_1 \\ ... \\ a_k \end{pmatrix}$;

$v >>> i$ — операція циклічного зсуву праворуч послідовності фіксованої довжини (символи з молодших позицій займають місце старших);

0x — префікс числа, що записане у шістнадцятковій системі числення;

$a \bmod b$ — операція обчислення цілого невід'ємного числа, що дорівнює залишку від ділення цілого числа a на натуральне число b;

$\omega_j^{(\nu)}$, $\varsigma_j^{(\nu)}$ — константи ітерацій для ν-го циклу перетворень $T_l^{\oplus}$ та T_l^{+} відповідно;

$GF(2^8)$ — розширення простого поля степеня 8;

H — визначена у цьому стандарті функція гешування;

$H(IV, M)$ — результат обчислення функції гешування для повідомлення M (геш-значення);

IV — вектор ініціалізації;

n — довжина обчисленого геш-значення, $n = 8 \cdot s$, $s \in \{1,2,...,64\}$;

l — розмір внутрішнього стану функції гешування (у бітах), $l \in \{512,1024\}$;

M — повідомлення;

m_i — i-й блок доповненого повідомлення M;

N — довжина повідомлення M без доповнення;

$R_{l,n}(x)$ — функція, що повертає n старших бітів з вхідної послідовності x довжиною l біт;

$T_l^{\oplus}$, T_l^{+} — бієктивні відображення $T_l^{\oplus}$, $T_l^{+}: V_l \to V_l$, $l \in \{512,1024\}$ (перестановки), що виконують перетворення блоку довжиною l біт у вихідний такої самої довжини;

t — кількість ітерацій у перетвореннях $T_l^{\oplus}$ і T_l^{+};

k — кількість блоків, з яких складається повідомлення M, охоплюючи доповнення;

Z^+ — множина додатних цілих чисел;

V_k — k-мірний векторний простір, який заданий над полем $GF(2)$, $k \in Z^+$;

$+$ — операція додавання, яка визначена в адитивній групі найменших невід'ємних залишків $Z_{2^{64}}$;

$\Xi \circ \Lambda$ — композиція двох операцій Ξ і Λ, при цьому операція Λ виконується першою;

$\prod_{i=1}^{t} \Lambda^{(i)}$ — послідовне виконання t операцій $\Lambda^{(1)}$, $\Lambda^{(2)}$, ..., $\Lambda^{(t)}$, операція $\Lambda^{(1)}$ виконується першою;

Купина-n — режим використання функції гешування з формуванням геш-значення довжиною n біт.

5 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Під функцією гешування H розуміють залежне від вектора ініціалізації $IV \in V_l$, $l \in \{512,1024\}$ відображення повідомлення $M \in V_N$, $N \in \{0,1,...,2^{96} - 1\}$ у геш-значення $H(IV, M) \in V_n$, $n \in \{8 \cdot s \mid s = 1,2,...,64\}$, таке що $H^{(IV)}: V_N \to V_n$.

Режим роботи функції гешування для $n \in \{8 \cdot s \mid s = 1,2,...,64\}$ позначають «Купина-n». Основними режимами роботи функції гешування, рекомендованими до застосування, є «Купина-256», «Купина-384» і «Купина-512».

Для формування кодів автентифікації застосовують режими «Купина-256(КАП)», «Купина-384(КАП)» і «Купина-512(КАП)» відповідно.

6 СТРУКТУРА ПЕРЕТВОРЕННЯ

Під час формування геш-значення повідомлення M завжди доповнюється (див. розділ 7) до довжини, кратної розміру блоку, та поділяється на блоки m_1, m_2,..., m_k, кожен з яких має довжину l біт. Вибір l здійснюють відповідно до розміру геш-значення n:

$$l = \begin{cases} 512 \text{ для } 8 \le n \le 256, \\ 1024 \text{ для } 256 < n \le 512, \end{cases}$$

де $n \in \{8 \cdot s \mid s = 1,2,...,64\}$.

Обчислюють геш-значення за такою ітеративною процедурою:

$h_0 = IV$,

$h_\nu = T_l^{\oplus}(h_{\nu-1} \oplus m_\nu) \oplus T_l^{+}(m_\nu) \oplus h_{\nu-1}$, $\nu = 1,2,...,k$,

$H(IV, M) = R_{l,n}(T_l^{\oplus}(h_k) \oplus h_k)$,

де $IV = \begin{cases} 1 << 510 \text{ для } l = 512, \\ 1 << 1023 \text{ для } l = 1024 \end{cases}$ — вектор ініціалізації довжиною l біт;

$T_l^{\oplus}$, T_l^{+} — бієктивні перетворення, що виконують відображення вхідного блоку довжиною l біт у вихідний такої самої довжини (див. розділ 8),

$R_{l,n}(x)$ — функція, що повертає n старших біт з вхідного блоку x довжиною l біт ($n < 1$), де результат записується в молодші n біт обчисленого значення.

Структурну схему функції гешування «Купина» наведено на рисунку 1.

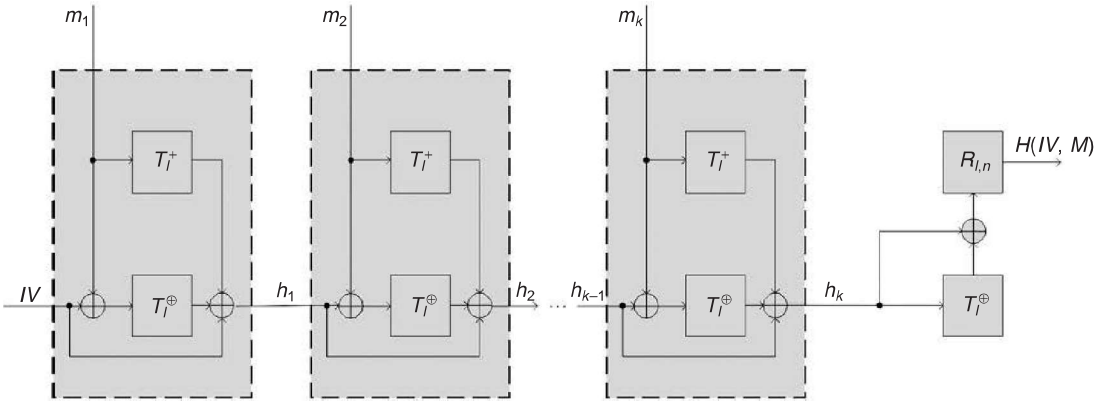

Рисунок 1 — Структурна схема функції гешування «Купина»

7 ДОПОВНЕННЯ ПОВІДОМЛЕННЯ

На вхід функції гешування подається повідомлення (бітова послідовність) M довжини N, $N \in \{0,1,...,2^{96} - 1\}$, яку задано в бітах. Кожне повідомлення доповнюється, незалежно від його довжини. У кінець повідомлення додається допоміжна інформація, яка містить одиничний біт, необхідну кількість нульових бітів (див. нижче) та довжину повідомлення на вході функції гешування так, щоб доповнена бітова послідовність мала довжину, кратну розміру внутрішнього стану l, $l \in \{512,1024\}$.

Під час доповнення спочатку у кінець повідомлення додають одиничний біт «1», потім додають d нульових бітів, де $d = (-N - 97) \bmod l$. Після цього додають ще 96 біт, в яких записано значення N (найменше значущі байти мають менший номер, тобто використовують формат little endian). Максимальна довжина повідомлення, що може бути оброблено, становить $(2^{96} - 1)$ біт.

8 ПЕРЕТВОРЕННЯ $T_l^{\oplus}$ та T_l^{+}

8.1 Загальна структура

Перетворення $T_l^{\oplus}$ та T_l^{+} є бієктивними відображеннями $T_l^{\oplus}$, $T_l^{+}: V_l \to V_l$, $l \in \{512,1024\}$, кожне з яких реалізоване у вигляді ітеративного застосування низки функцій, що обробляють вхідний аргумент $x \in V_l$ як матрицю розміром $8 \times c$ байтів, що містить елементи поля $GF(2^8)$.

Залежність розміру внутрішнього стану (l), кількості ітерацій (t) та кількості колонок матриці (c) від розміру геш-значення n наведено в таблиці 8.1.

Таблиця 8.1

Розмір геш-значення	Розмір внутрішнього стану (l)	Кількість ітерацій перетворення (t)	Кількість колонок у матриці (c)
$8 \le n \le 256$	512	10	8
$256 < n \le 512$	1024	14	16

Матрицю внутрішнього стану позначають як $G = (g_{i,j})$, $g_{i,j} \in GF(2^8)$, де $i = \overline{0,7}$, $j = \overline{0,c-1}$. Записують байти $B_1, B_2, \ldots, B_{l/8}$ перетворень $T_l^{\oplus}$ та T_l^{+} до матриці і зчитують з неї за колонками (приклад для $l = 512$ та $c = 8$, див. рисунок 2).

Вхідна послідовність							
B_1	B_9	B_{17}	B_{25}	B_{33}	B_{41}	B_{49}	B_{57}
B_2	B_{10}	B_{18}	B_{26}	B_{34}	B_{42}	B_{50}	B_{58}
B_3	B_{11}	B_{19}	B_{27}	B_{35}	B_{43}	B_{51}	B_{59}
B_4	B_{12}	B_{20}	B_{28}	B_{36}	B_{44}	B_{52}	B_{60}
B_5	B_{13}	B_{21}	B_{29}	B_{37}	B_{45}	B_{53}	B_{61}
B_6	B_{14}	B_{22}	B_{30}	B_{38}	B_{46}	B_{54}	B_{62}
B_7	B_{15}	B_{23}	B_{31}	B_{39}	B_{47}	B_{55}	B_{63}
B_8	B_{16}	B_{24}	B_{32}	B_{40}	B_{48}	B_{56}	B_{64}

↓

Внутрішній стан функції гешування							
$g_{0,0}$	$g_{0,1}$	$g_{0,2}$	$g_{0,3}$	$g_{0,4}$	$g_{0,5}$	$g_{0,6}$	$g_{0,7}$
$g_{1,0}$	$g_{1,1}$	$g_{1,2}$	$g_{1,3}$	$g_{1,4}$	$g_{1,5}$	$g_{1,6}$	$g_{1,7}$
$g_{2,0}$	$g_{2,1}$	$g_{2,2}$	$g_{2,3}$	$g_{2,4}$	$g_{2,5}$	$g_{2,6}$	$g_{2,7}$
$g_{3,0}$	$g_{3,1}$	$g_{3,2}$	$g_{3,3}$	$g_{3,4}$	$g_{3,5}$	$g_{3,6}$	$g_{3,7}$
$g_{4,0}$	$g_{4,1}$	$g_{4,2}$	$g_{4,3}$	$g_{4,4}$	$g_{4,5}$	$g_{4,6}$	$g_{4,7}$
$g_{5,0}$	$g_{5,1}$	$g_{5,2}$	$g_{5,3}$	$g_{5,4}$	$g_{5,5}$	$g_{5,6}$	$g_{5,7}$
$g_{6,0}$	$g_{6,1}$	$g_{6,2}$	$g_{6,3}$	$g_{6,4}$	$g_{6,5}$	$g_{6,6}$	$g_{6,7}$
$g_{7,0}$	$g_{7,1}$	$g_{7,2}$	$g_{7,3}$	$g_{7,4}$	$g_{7,5}$	$g_{7,6}$	$g_{7,7}$

Рисунок 2 — Заповнення внутрішнього стану

$T_l^{\oplus}$ та T_l^{+} визначено так:

$$T_l^{\oplus} = \prod_{\nu=0}^{t-1}\left(\psi \circ \tau^{(l)} \circ \pi' \circ \kappa_\nu^{(l)}\right),$$

$$T_l^{+} = \prod_{\nu=0}^{t-1}\left(\psi \circ \tau^{(l)} \circ \pi' \circ \eta_\nu^{(l)}\right),$$

де $\kappa_\nu^{(l)}$ — функція додавання констант ітерацій за модулем 2;

$\eta_\nu^{(l)}$ — функція додавання констант ітерацій за модулем 2^{64};

π' — шар нелінійного бієктивного відображення, який виконує байтову підстановку елементів матриці внутрішнього стану $G = (g_{i,j})$;

$\tau^{(l)}$ — перестановка елементів $g_{i,j} \in GF(2^8)$ внутрішнього стану (циклічний зсув у разі матричного подавання);

ψ — лінійне перетворення (множення вектора на матрицю над скінченним полем).

У функціях $\kappa_\nu^{(l)}$, $\eta_\nu^{(l)}$, π', $\tau^{(l)}$ і ψ вхідний аргумент $x \in V_l$ та вихідне значення $\chi(x) \in V_l$, $\chi \in \{\kappa_\nu^{(l)}, \eta_\nu^{(l)}, \pi', \tau^{(l)}, \psi\}$ розглядають як матрицю розміром $8 \times c$ байтів (див. таблицю 8.1).

8.2 Додавання констант ітерацій

Функція $\kappa_\nu^{(l)}$ здійснює додавання за модулем 2 до кожної колонки G_j матриці внутрішнього стану $G = (g_{i,j})$ вектора $\omega_j^{(\nu)} \in V_{64}$, де ν — номер ітерації, $\omega_j^{(\nu)} = ((j<<4)\oplus\nu,0,0,0,0,0,0,0)^T$.

Функція $\eta_\nu^{(l)}$ здійснює додавання за модулем 2^{64} до кожної колонки G_j матриці внутрішнього стану $G = (g_{i,j})$ вектора $\varsigma_j^{(\nu)} \in V_{64}$, де ν — номер ітерації, $\varsigma_j^{(\nu)} = (0xF3,0xF0,0xF0,0xF0,0xF0,0xF0,0xF0,0xF0, ((c - 1 - j)<<4) \oplus \nu)^T$, при цьому під час операції додавання $0xF3$ — молодші 8 біт вектора $\varsigma_j^{(\nu)}$, $g_{0,j}$ — молодші 8 біт вектора G_j.

8.3 Шар нелінійного бієктивного відображення

Функція π' виконує заміну кожного елемента $g_{i,j}$ матриці внутрішнього стану $G = (g_{i,j})$ на $\pi_{i \bmod 4}(g_{i,j})$, де $\pi_s : V_8 \to V_8$, $s \in \{0,1,2,3\}$ — підстановки, які наведені у додатку А.

Наприклад, нехай $g_{0,0} = 0x23$, тоді $\pi_0(0x23) = 0x4F$.

8.4 Перестановка елементів

Функція $\tau^{(l)}$ виконує циклічний зсув праворуч рядків матриці стану $G = (g_{i,j})$. Рядки з номерами $i = 0,1,2,..,6$ матриці зсуваються на i елементів, а рядок з номером 7 зсувається на 7 елементів для $l = 512$ і на 11 елементів для $l = 1024$.

8.5 Лінійне перетворення

Під час обчислення результату функції ψ кожен елемент $g_{i,j}$ матриці внутрішнього стану $G = (g_{i,j})$ розглядають як елемент скінченного поля $GF(2^8)$, що утворене незвідним поліномом $\vartheta(x) = x^8 + x^4 + x^3 + x^2 + 1$, або $0x11d$ у шістнадцятковому поданні.

Кожен елемент результуючої матриці стану $U = (u_{i,j})$ отримують як результат множення векторів довжини 8 над скінченним полем $GF(2^8)$за формулою:

$$u_{i,j} = (\upsilon >>> i) \oplus G_j,$$

де $\upsilon = (0x01,0x01,0x05,0x01,0x08,0x06,0x07,0x04)$ — вектор, що утворює циркулянтну матрицю МДР-коду і складається з послідовності байтових констант у шістнадцятковому поданні, які інтерпретують як елементи поля $GF(2^8)$, при цьому циклічний зсув виконується відносно елементів вектора;

G_j — j-а колонка матриці стану $G = (g_{i,j})$.

ДОДАТОК А
(обов'язковий)

ТАБЛИЦІ ЗАМІНИ ДЛЯ ШАРУ НЕЛІНІЙНОГО БІЄКТИВНОГО ВІДОБРАЖЕННЯ

(шістнадцяткове подання)

Підстановка π_0:

```
A8 43 5F 06 6B 75 6C 59 71 DF 87 95 17 F0 D8 09
6D F3 1D CB C9 4D 2C AF 79 E0 97 FD 6F 4B 45 39
3E DD A3 4F B4 B6 9A 0E 1F BF 15 E1 49 D2 93 C6
92 72 9E 61 D1 63 FA EE F4 19 D5 AD 58 A4 BB A1
DC F2 83 37 42 E4 7A 32 9C CC AB 4A 8F 6E 04 27
2E E7 E2 5A 96 16 23 2B C2 65 66 0F BC A9 47 41
34 48 FC B7 6A 88 A5 53 86 F9 5B DB 38 7B C3 1E
22 33 24 28 36 C7 B2 3B 8E 77 BA F5 14 9F 08 55
9B 4C FE 60 5C DA 18 46 CD 7D 21 B0 3F 1B 89 FF
EB 84 69 3A 9D D7 D3 70 67 40 B5 DE 5D 30 91 B1
78 11 01 E5 00 68 98 A0 C5 02 A6 74 2D 0B A2 76
B3 BE CE BD AE E9 8A 31 1C EC F1 99 94 AA F6 26
2F EF E8 8C 35 03 D4 7F FB 05 C1 5E 90 20 3D 82
F7 EA 0A 0D 7E F8 50 1A C4 07 57 B8 3C 62 E3 C8
AC 52 64 10 D0 D9 13 0C 12 29 51 B9 CF D6 73 8D
81 54 C0 ED 4E 44 A7 2A 85 25 E6 CA 7C 8B 56 80
```

Підстановка π_1:

```
CE BB EB 92 EA CB 13 C1 E9 3A D6 B2 D2 90 17 F8
42 15 56 B4 65 1C 88 43 C5 5C 36 BA F5 57 67 8D
31 F6 64 58 9E F4 22 AA 75 0F 02 B1 DF 6D 73 4D
7C 26 2E F7 08 5D 44 3E 9F 14 C8 AE 54 10 D8 BC
1A 6B 69 F3 BD 33 AB FA D1 9B 68 4E 16 95 91 EE
4C 63 8E 5B CC 3C 19 A1 81 49 7B D9 6F 37 60 CA
E7 2B 48 FD 96 45 FC 41 12 0D 79 E5 89 8C E3 20
30 DC B7 6C 4A B5 3F 97 D4 62 2D 06 A4 A5 83 5F
2A DA C9 00 7E A2 55 BF 11 D5 9C CF 0E 0A 3D 51
7D 93 1B FE C4 47 09 86 0B 8F 9D 6A 07 B9 B0 98
18 32 71 4B EF 3B 70 A0 E4 40 FF C3 A9 E6 78 F9
8B 46 80 1E 38 E1 B8 A8 E0 0C 23 76 1D 25 24 05
F1 6E 94 28 9A 84 E8 A3 4F 77 D3 85 E2 52 F2 82
50 7A 2F 74 53 B3 61 AF 39 35 DE CD 1F 99 AC AD
72 2C DD D0 87 BE 5E A6 EC 04 C6 03 34 FB DB 59
B6 C2 01 F0 5A ED A7 66 21 7F 8A 27 C7 C0 29 D7
```

Підстановка π_2:

```
93 D9 9A B5 98 22 45 FC BA 6A DF 02 9F DC 51 59
4A 17 2B C2 94 F4 BB A3 62 E4 71 D4 CD 70 16 E1
49 3C C0 D8 5C 9B AD 85 53 A1 7A C8 2D E0 D1 72
A6 2C C4 E3 76 78 B7 B4 09 3B 0E 41 4C DE B2 90
25 A5 D7 03 11 00 C3 2E 92 EF 4E 12 9D 7D CB 35
10 D5 4F 9E 4D A9 55 C6 D0 7B 18 97 D3 36 E6 48
56 81 8F 77 CC 9C B9 E2 AC B8 2F 15 A4 7C DA 38
1E 0B 05 D6 14 6E 6C 7E 66 FD B1 E5 60 AF 5E 33
87 C9 F0 5D 6D 3F 88 8D C7 F7 1D E9 EC ED 80 29
27 CF 99 A8 50 0F 37 24 28 30 95 D2 3E 5B 40 83
B3 69 57 1F 07 1C 8A BC 20 EB CE 8E AB EE 31 A2
73 F9 CA 3A 1A FB 0D C1 FE FA F2 6F BD 96 DD 43
52 B6 08 F3 AE BE 19 89 32 26 B0 EA 4B 64 84 82
6B F5 79 BF 01 5F 75 63 1B 23 3D 68 2A 65 E8 91
F6 FF 13 58 F1 47 0A 7F C5 A7 E7 61 5A 06 46 44
42 04 A0 DB 39 86 54 AA 8C 34 21 8B F8 0C 74 67
```

Підстановка π_3:

```
68 8D CA 4D 73 4B 4E 2A D4 52 26 B3 54 1E 19 1F
22 03 46 3D 2D 4A 53 83 13 8A B7 D5 25 79 F5 BD
58 2F 0D 02 ED 51 9E 11 F2 3E 55 5E D1 16 3C 66
70 5D F3 45 40 CC E8 94 56 08 CE 1A 3A D2 E1 DF
B5 38 6E 0E E5 F4 F9 86 E9 4F D6 85 23 CF 32 99
31 14 AE EE C8 48 D3 30 A1 92 41 B1 18 C4 2C 71
72 44 15 FD 37 BE 5F AA 9B 88 D8 AB 89 9C FA 60
EA BC 62 0C 24 A6 A8 EC 67 20 DB 7C 28 DD AC 5B
34 7E 10 F1 7B 8F 63 A0 05 9A 43 77 21 BF 27 09
C3 9F B6 D7 29 C2 EB C0 A4 8B 8C 1D FB FF C1 B2
97 2E F8 65 F6 75 07 04 49 33 E4 D9 B9 D0 42 C7
6C 90 00 8E 6F 50 01 C5 DA 47 3F CD 69 A2 E2 7A
A7 C6 93 0F 0A 06 E6 2B 96 A3 1C AF 6A 12 84 39
E7 B0 82 F7 FE 9D 87 5C 81 35 DE B4 A5 FC 80 EF
CB BB 6B 76 BA 5A 7D 78 0B 95 E3 AD 74 98 3B 36
64 6D DC F0 59 A9 4C 17 7F 91 B8 C9 57 1B E0 61
```

ДОДАТОК Б
(довідковий)

ПРИКЛАДИ ДЛЯ ПЕРЕВІРКИ

Нижче наведені тестові приклади для перевірки правильності реалізації функції гешування, що вказують вхідні та вихідні значення складових перетворень, а також проміжні значення під час обчислень. Застосовані скорочення наведено у таблиці Б.1.

Таблиця Б.1 — Скорочення, застосовані у прикладах для перевірки

`INPUT`	вхідна послідовність
`round[v]`	v-та ітерація перетворення $T_l^{\oplus}$ чи T_l^{+}
`add_c`	результат виконання перетворення $\kappa_v^{(l)}$ або $\eta_v^{(l)}$
`s_box`	результат виконання перетворення π'
`s_byt`	результат виконання перетворення $\tau^{(l)}$
`m_col`	результат виконання перетворення ψ
`padded`	результат виконання операції доповнення повідомлення до довжини, кратної розміру внутрішнього стану
`block[i].f`	внутрішній стан після оброблення i-го блоку вхідного повідомлення
`final`	результат роботи функції гешування перед виконанням перетворення $R_{l,n}(x)$
`HASH`	обчислене геш-значення

Внутрішні стани функції гешування подано як бітові послідовності у шістнадцятковій нотації.

Приклади для перевірки перетворень $T_{512}^{\oplus}$ та T_{512}^{+} геш-функції у режимі «Купина-256»:

```
ТЕСТ ПЕРЕТВОРЕННЯ T⊕512
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
round[ 0].add_c:
    000102030405060718090A0B0C0D0E0F301112131415161728191A1B1C1D1E1F
    602122232425262778292A2B2C2D2E2F503132333435363748393A3B3C3D3E3F
round[ 0].s_box:
    A8BB9A4D6BCB452A793ADFB31790511F92152B3DC91CBB831F5C71D56F5716BD
    34F6C002B4F4AD118E0F7A5E496DD1662E26C445D15DB7949C140E1A5810B2DF
round[ 0].s_byt:
    A814C45EB457BB1F79BB0E4549F41683923A9A1AD16DADBD1F15DF4D585DD111
    345C2BB36B10B7668EF6713D17CBB2942E0FC0D5C99045DF9C267A026F1C512A
round[ 0].m_col:
    4DA74F33C3485F0C9560F6400144488E65E3C69CD3B296FBA3F3430A2E154FE2
    E4B32BB503DFED48860D18AEBC3E135CCF4853EB8CAFB6B622BE8F7562D01010
round[ 1].add_c:
    4CA74F33C3485F0C8460F6400144488E44E3C69CD3B296FB92F3430A2E154FE2
    A5B32BB503DFED48D70D18AEBC3E135CAE4853EB8CAFB6B653BE8F7562D01010
round[ 1].s_box:
    8FA035458CD148545CE754B543BD922742D019FB0D8037C969F00326931C356B
    681EC85006AD06E91A90624294D8C218A2D19EAD3FF90D015A2429A6FC504A22
round[ 1].s_byt:
    8F249E42061C37275CA029AD94AD35C942E735A63FD8066B69D05445FCF9C2E9
    68F019B58C500D181A1E03FB43D14A01A290C8260DBD48225AD1625093809254
round[ 1].m_col:
    544AB381EA8ACA3449A9DD1F7D9FB4484E6AB7B5F93A61B18D05B4760C023FB9
    FA5FA01A21EEBF29E1662942BAB4A85A779BEF260345DD8873D6AE28FF1D16FC
```

```
round[ 2].add_c:
    564AB381EA8ACA345BA9DD1F7D9FB4486C6AB7B5F93A61B1BF05B4760C023FB9
    B85FA01A21EEBF29B3662942BAB4A85A159BEF260345DD8801D6AE28FF1D16FC
round[ 2].s_box:
    23683A7E519CB0400F4065BD9F981AE93879C15025C8819026CB1AA817EB9047
    1CCAB3B7DDDB433EBDFCA16EF13820414D6A449E06336505436131F28057BB57
round[ 2].s_byt:
    2361446EDDEB81E90F68319EF1DB909038403AF20638434726796 57E8033203E
    1CCBC1BD51576541BDCA1A509F9CBB054DFCB3A82598B057436AA1B717C81A40
round[ 2].m_col:
    A0300FB45ACD67409A4E457890710BA22D03F6C8225FB5760B6000E3C802A414
    EA43E88D78918717A4BEBB0777229A9D68FA1DF664A6F860E813B96D0824F4F4
round[ 3].add_c:
    A3300FB45ACD6740894E457890710BA20E03F6C8225FB576386000E3C802A414
    A943E88D78918717F7BEBB0777229A9D0BFA1DF664A6F8609B13B96D0824F4F4
round[ 3].s_box:
    E57C596F6652E2B57D910067EBDC02F8D8925496A3CAFBA8F4E79376FBEB072D
    02F3C5BF8E938D832A246F2A3B6495FF958A704C6A708C72DEB4FA9C719E3959
round[ 3].s_byt:
    E5B4702A8EEBFBF87D7CFA4C3B9307A8D891599C6A648D2DF492006F71709583
    02E75467669E8CFF2AF39396EB5239729524C576A3DCE259DE8A6FBFFBCA02B5
round[ 3].m_col:
    8E82F73EACEABC1D7FB49E09302FA6BCF7FEC0A4B7D9B599618AC29160896FD0
    B777D734C91726542AA8EE9DF72E7B105FD5AED8CBFB3246C806918CFDC79269
round[ 4].add_c:
    8A82F73EACEABC1D6BB49E09302FA6BCD3FEC0A4B7D9B599558AC29160896FD0
    F377D734C91726547EA8EE9DF72E7B103BD5AED8CBFB3246BC06918CFDC79269
round[ 4].s_box:
    21C9AAE12DC6BD79DB384052924D8A690D2952F63135FB8B169C089F34D538E7
    ED9763400543ADC808E446FF2A73E522ADB331815E27C4F99413CF218BA39988
round[ 4].s_byt:
    211331FF05D5FB69DBC9CF812A43388B0D38AA215E73ADE7162940E18B27E5C8
    ED9C52522DA3C422089708F692C699F9ADE4639F314DBD8894B3464034358A79
round[ 4].m_col:
    B64341B3BA32E14923FC775349AB3AE10EA4690FE40BE29EFBFB2C8C0A580613
    524A6B51FD522A7620FE164DB81B77960C85019D96D5160F4F2AC5946BDE71F5
round[ 5].add_c:
    B34341B3BA32E14936FC775349AB3AE12BA4690FE40BE29ECEFB2C8C0A580613
    174A6B51FD522A7675FE164DB81B77966985019D96D5160F3A2AC5946BDE71F5
round[ 5].s_box:
    BDF3A58EF12EFF4FFAC77EEECCC30EBBE1EFB81FD0B213C13D272D218781453D
    AF6815148B8E7AA8C729BBCF1CBA7EEBF9A2D9FFD3B3BB1FD502BE29DBAC0BA9
round[ 5].s_byt:
    BD02D9CF8B8113BBFAF3BEFF1C8E45C1E1C7A529D3BA7A3D3DEF7E8EDBB37EA8
    AF27B8EEF1ACBBEBC7682D1FCC2E0B1FF9291521D0C3FFA9D5A2BB1487B20E4F
round[ 5].m_col:
    485A33BD4DFF6F128C403A6B4A0CB5FAE69451A0D0D3A4F421A5FB9B9336E9A0
    9D86EF638819CECDAEDB0FAF7E4251AC979C4B601C590AAFC284D0C41789CCA5
round[ 6].add_c:
    4E5A33BD4DFF6F129A403A6B4A0CB5FAC09451A0D0D3A4F417A5FB9B9336E9A0
    DB86EF638819CECDF8DB0FAF7E4251ACF19C4B601C590AAFB484D0C41789CCA5
round[ 6].s_box:
    047BE3A26ED73846B51A0EABABD2FBB82FC4D597F7740759AF3B8B1D3A44A797
    B85544FDCD5C841285CD59C70869D5B9540712726F49DFC7AE7E6B0AAFD54B75
round[ 6].s_byt:
    047E12C7CD4407B8B57B6B72085CA7592F1AE30A6F698497AFC40EA2AF49D512
    B83BD5AB6ED5DFB985558B97ABD74BC754CD441DF7D23875AE0759FD3A74FB46
round[ 6].m_col:
    8B4A39DA56E2B90AD8EC2A4A1395C5A59E9AEAF2BD04442E1C3B1BA379ECE26D
    E471847832076001F494C9348E3E06EA9142DB5133095DBF42A0712072B03B17
round[ 7].add_c:
    8C4A39DA56E2B90ACFEC2A4A1395C5A5B99AEAF2BD04442E2B3B1BA379ECE26D
    A371847832076001A394C9348E3E06EAF642DB5133095DBF35A0712072B03B17
```

```
round[ 7].s_box:
    3F683BDE23DDFA2682347AD6CB47BE75EC9DE7DCAAEA113CE1AED4657734139C
    E5DC6D679EC1568DE5C4264089D845E3A7696814613A367A63180B58248B4183
round[ 7].s_byt:
    3F1868409E34117582680B1489C1133CEC343B5861D8569CE19D7ADE243A458D
    E5AEE7D6238B36E3E5DCD4DCCBDD417AA7C46D65AA47FA836369266777EABE26
round[ 7].m_col:
    30C2B6D3279468CBD0044D9343B36CE06748C856619FF079442BE20CC9300A0C
    F07BCBA7EDF577B78BBDF012FCBFB5DE9EC3BC253F06C0698F1DDD2BE0DBB6ED
round[ 8].add_c:
    38C2B6D3279468CBC8044D9343B36CE04F48C856619FF0797C2BE20CC9300A0C
    B87BCBA7EDF577B7D3BDF012FCBFB5DEF6C3BC253F06C069F71DDD2BE0DBB6ED
round[ 8].s_box:
    F4940DF70EC4ACAFFBEA7DD7371EA4CB27D132D34898422014B11354057CDF54
    1C06EA04D6ED7EC50D2542467C05FB80A728BD51A11352882A57655EACCD0D98
round[ 8].s_byt:
    F457BD46D67C42CBFB9465517CEDDF2027EA0D5EA1057E5414D17DF7AC13FBC5
    1CB132D70ECD52800D0613D337C40D88A725EA54481EAC982A2842040598A4AF
round[ 8].m_col:
    A59533213B91202CE66D8FF39EB95505FF6101404E519ECE2D859F05A3AA4388
    FD213991C053733FB971AB5E2CD340BEB4E86DE386286B83D3F2354742FBD234
round[ 9].add_c:
    AC9533213B91202CFF6D8FF39EB95505D66101404E519ECE14859F05A3AA4388
    B4213991C053733FE071AB5E2CD340BEDDE86DE386286B83AAF2354742FBD234
round[ 9].s_box:
    2D47E32FAD9349D1808C29F0910CA94B502BD9B504634084C9A2834BE5FF0305
    AEF63B9F2F5BD6DFACDC8E2C497425E262EC7C76187515F1A601788683277940
round[ 9].s_byt:
    2D017C2C2FFF404B80477876495B0384508CE3861874D605C92B292F837525DF
    AEA2D9F0AD2715E2ACF683B5919379F162DC3B4B040C4940A6EC8E9FE563A9D1
round[ 9].m_col:
    20A066016C8DAA5AA2ACA450D21F2796FBDC2E0CC452AF0AAF67E27A0755CB32
    718C2C7909201D3E7A3F256234C80B70D51AE3936DB26CF56E1F1BA8A0A7E1C0
OUTPUT:
    20A066016C8DAA5AA2ACA450D21F2796FBDC2E0CC452AF0AAF67E27A0755CB32
    718C2C7909201D3E7A3F256234C80B70D51AE3936DB26CF56E1F1BA8A0A7E1C0
```

ТЕСТ ПЕРЕТВОРЕННЯ T^{+}_{512}

```
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
round[ 0].add_c:
    F3F1F2F3F4F5F677FBF9FAFBFCFDFE6F030203040506076 80B0A0B0C0D0E0F60
    13121314151617581B1A1B1C1D1E1F5023222324252627482B2A2B2C2D2E2F40
round[ 0].s_box:
    EDC2A0F04EED54ECCA7F21C97CC0746006EBB5737513FC9B95D60254F0175972
    CB56C22D4D88A3A1FD36D4254B67E1314F64D8EDB62285E9E102C8D1D27372B5
round[ 0].s_byt:
    ED02D8254D17FC60CAC2C8ED4B88599B067FA0D1B667A37295EB21F0D222E1A1
    CBD6B5C94E738531FD5602737CED72E94F36C25475C054B5E164D42DF01374EC
round[ 0].m_col:
    2602D1E580D3126B9B293B34018A690EBF72F15BBDB2A1811A50B37E8F01D33D
    8AFDAA4350CFC93381F67A9B52273EC3AA3EC141D6E37358747938EF0A1C18EB
round[ 1].add_c:
    19F3C1D671C403DD8E1A2C25F27A5A70B263E24CAEA392D30D41A46F80F2C37F
    7DEE9B3441C0BA6574E76B8C43182FE59D2FB232C7D4646A676A29E0FB0C09ED
round[ 1].s_box:
    E0F0B687339AB5FC89362D51C02D18EACEFD1323A24B99F7F06B07609B01F35B
    9FDBD240F2F1F2BE36A6152137C5725A304DCAF37F53CCD85379A1CBCAD26A98
round[ 1].s_byt:
    E079CA21F20199EA89F0A1F337F1F3F7CE36B6CB7FC5F25BF0FD2D87CA5372BE
    9F6B135133D2CC5A36DB0723C09A6AD830A6D260A22DB598534D15409B4B18FC
```

```
round[ 1].m_col:
    DF966E4B4E7C751A3454F48BA48A74B789CCAAAC5847444A7BD211C382457BF6
    82D2CBDCABDDB107AC9C0D5C89135D92AAE80BC0BB6A059F8B33AC57338C4915
round[ 2].add_c:
    D2875F3C3F6D668D2745E57C957B651A7CBD9B9D4938359D6EC302B473366C39
    75C3BCCD9CCEA23A9F8DFE4C7A044EB59DD9FCB0AC5BF6B17E249D48247D3A18
round[ 2].s_box:
    0ABF483AA18CB9BF0E334728D7069CB71425D2FFCC9F78FFC3289A6F2844A408
    C728BD125DF257CEB10A7423BAEACB503035F86C2DD95490089E5BE9B4A50E13
round[ 2].s_byt:
    0A9EF8235D4478B70EBF5B6CBAF2A4FF143348E92DEA5708C325473AB4D9CBCE
    C728D228A1A55450B1289AFFD78C0E90300ABD6FCC06B91308357412289F9CBF
round[ 2].m_col:
    4C89AD984649A973D85C308B5DE1AB6110B8C06AB5B852B3EB7995ABCBF63E97
    0EE1E8736FD610600758E25FD64370EB588D7CC4AA2EE8BD9BEAAC98393C4BF2
round[ 3].add_c:
    3F7A9E89373A9AE7CB4D217C4ED29CC503A9B15BA6A94307DE6A869CBCE72FDB
    01D2D96460C70194FA48D350C734610F4B7E6DB59B1FD9D18EDB9D892A2D3CF6
round[ 3].s_box:
    A12D409AEEC895785E953C28042F3E060640F9B19840032AE37988FB94A672B4
    432F233734A3D929E6D1BF317F08811F4A837C50DE8D23B089CD5B9A156D4C4C
round[ 3].s_byt:
    A1CD7C3134A603065E2D5B507FA3722A0695409ADE08D9B4E3403C9A158D8129
    4379F928EE6D231FE62F88B104C84CB04AD123FB982F954C8983BF3794403E78
round[ 3].m_col:
    938F5067C36E9871D0F74E6EB4F38788055C36B91E76A72850E86E853E6543CB
    ED2FA7FF6FEA65B443DF0C66FD7A24DB78AAD41F941C01C84A96785EBD54A724
round[ 4].add_c:
    86804158B45F89E6C3E83F5FA5E478EDF84C27AA0F67987D43D95F762F563410
    E02098F060DB56E936D0FD56EE6B15006B9BC510850DF2DC3D87694FAE459829
round[ 4].s_box:
    182AA5A1AECAF77D8CEC907168876698851685E4094128DD373548A8C6197622
    AC31286434CD5595FA500CD373E5F468DB6ABE22DA90A0A5A4BFB899A233283E
round[ 4].s_byt:
    18BFBED3341928988C2AB82273CD76DD85ECA599DAE55522371690A1A290F495
    AC358571AE33A068FA3148E468CA28A5DB5028A80987F73EA46A0C64C641667D
round[ 4].m_col:
    613A348E2E0AD6C6C167BD5CBF7C35CD3F0C39640DF28FEBCCDDC66B1CADBAD6
    0A5B588D3DAE1DEFCD3F0FACF8109B10D1F623F7957C9A96B5F63A9798562BFC
round[ 5].add_c:
    542B257F1FFBC63CB458AE4DB06D263332FD2955FEE28041BFCEB75C0D9EAB1C
    FD4B497E2E9F0E25C030009DE9018C36C4E714E8866D8BACA8E72B8889471C02
round[ 5].s_box:
    96B19B5B3927193AAE8131CFB38CAD459EC0A14856DD873826F2C118F0B08E25
    8B4EEFAC939851512F7C93FF29BBECE835A6940B188CE9B9C5A6C8057DFACDCA
round[ 5].s_byt:
    96A694FF93B08745AEB1C80B29988E389E819B0518BB512526C0315B7D8CEC51
    8BF2A1CF39FAE9E82F4EC148B327CDB9357CEF18568C19CAC5A693ACF0DDAD3A
round[ 5].m_col:
    E1FD96DFE05A58B494EAD147F39E9A5294E0F281D9BF05B86FD26F94AAD3F544
    78C5617E2066F7206F4C941A6F47E02DE06740831AF7804F8119AB35F5F75DDC
round[ 6].add_c:
    D4EE87D0D14B492B87DBC238E48F8BB987D1E372CAB0F60E62C360859BC4E68B
    6BB6526F1157E857623D850B6038D154D35831740BE87166740A9C26E6E84EE3
round[ 6].s_box:
    7EDB8DE7EA4EEF5E46CD0856D051E947467A5862C18B5419FC28568FDE9A0A77
    DBB84F60F3A1C530FC103FB3349FF5C80D812C2495EC0B5F36D63E9E13ECCB76
round[ 6].s_byt:
    7ED62CB3F39A544746DB3E2434A10A1946CD8D9E959FC577FC7A08E713ECF530
    DB285856EAEC0BC8FCB85662D04ECB5F0D104F8FC151EF7636813F60DE8BE95E
round[ 6].m_col:
    8720106F1C351FF17172DD876EAE8C1C8F7CE256D316C976B24D3C8EF8115207
    E789CE875F53539D685410A82F53F386339612416C96D3E577A22BE8CDF35624
```

```
round[ 7].add_c:
    7A1101600D2610696463CE785F9F7D84826DD347C407BACEA53E2D7FE902434F
    DA7ABF78504444D55B4501992044E4AE268703325D87C4FD6A931CD9BEE4472C
round[ 7].s_box:
    BA15D972F0224A886AFD84674198AF7BFE8CBF8635C1F28468D8E05B29EB0399
    572D43672EBD119D0F33D98B3EBDF1429ABFB5F3A9BFAE1B5BFECD35F6872ED1
round[ 7].s_byt:
    BAFEB58B2EEBF27B6A15CDF33EBD0384FEFDD935A9BD1199688C8472F6BFF19D
    57D8BF67F087AE420F2DE08641222E1B9A33435B35984AD15BBFD96729C1AF88
round[ 7].m_col:
    AC4B595D1E3D82D9357B3DF0B35D0F350DBC8CF6AED7DAA4DD9DFD54C0626EB7
    0F6C3FA9EACD3000BBBCB2DDC0D719E4EA25FAD3A8A0547180C4AEA9BA568761
round[ 8].add_c:
    9F3C4A4E0F2E7352286C2EE1A44E009E00AD7DE79FC8CBFDD08EEE45B1535F00
    025D309ADBBE2139AEADA3CEB1C80A0DDD16EBC49991458A73B59F9AAB47786A
round[ 8].s_box:
    B1544E320973D6AE1F89D1BB009193C1A8E6AF78B14FEA1BF73D46F4BE5B4868
    5F37A68CB8243C08A2E61F84BE4FDF1E6288610A4093004328E1838C74FA66D8
round[ 8].s_byt:
    B1E16184B85BEAC11F54830ABE24481BA8894E8C404F3C68F7E6D1327493DF08
    5F3DAFBB09FA001EA23746780073664362E6A6F4B191D6D828881F8CBE4F93AE
round[ 8].m_col:
    CDB1F03FCA83EBA33CE6E1556F47B9AC4A5421936E1556905C6E0FDF2B7F705A
    E64EF39D1DD1417CA76458F52ABCD46A8B671489AA220A98356D4DC5A7EFF63A
round[ 9].add_c:
    C0A2E130BB74DC1D2FD7D2466038AA163D4512845F0647EA4F5F00D01C7061A4
    D93FE48E0EC232B69A5549E61BADC5947E58057A9B13FBB1285E3EB698E0E744
round[ 9].s_box:
    2F71FF70994A2A79C6AF79F9349FCE53A4332B7B41132EE327CA93E76F3081F6
    07BCF127D894C401B53CEF7DFDE6BE29088122DBDEB48B901F60B20167727FE5
round[ 9].s_byt:
    2F60227DD8302E53C671B2DBFD9481E3A4AFFF01DEE6C4F62733797067B4BE01
    07CA2BF999728B29B5BC937B344A7F90083CF1E7419F2AE51F81EF276F13CE79
round[ 9].m_col:
    2D6F3A8E12F162AEC3F76E0402575068671824EF72FEA1CD7D71FD4D8E6A27A1
    0C2BA7EBF31C277F91DD384731025A8DF3013049279CF47251B2434F2632F00A
OUTPUT:
    2D6F3A8E12F162AEC3F76E0402575068671824EF72FEA1CD7D71FD4D8E6A27A1
    0C2BA7EBF31C277F91DD384731025A8DF3013049279CF47251B2434F2632F00A
```

Приклади для перевірки геш-функції у режимі «Купина-256»:

```
ТЕСТ ГЕШУВАННЯ (N = 512)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    800000000000000000000000000000000000000000000000000000000000000
    000000000000000000000000000000000000000000000200000000000000000
block[ 0].f:
    332851203C1F0C904DEED6410B7531CB1BAFE41FF27C23BD7448E40F7DF16FBB
    A6FEB5CFA65C0CBFC723F896F23C3408EE529641899E84A5CB1ADF3A82884883
block[ 1].f:
    56C926AFF9CDE45340DFB15C75941BEB6A6500DE35319B4A4905B56585F6B1F2
    933E3737FC1A0BDC9F94B3254066917E00FC289D027EF13871320FA9A545304C
final:
    86A9D24E23F4B103B72B8C69D1F1BBB5117EC3017604DCDF6BF04F3DA95C0268
    08F4EE6F1BE6903B324C4E27990CB24EF69DD58DBE84813EE0A52F6631239875
HASH-256:
    08F4EE6F1BE6903B324C4E27990CB24EF69DD58DBE84813EE0A52F6631239875
```

```
ТЕСТ ГЕШУВАННЯ (N = 1024)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
    800000000000000000000000000000000000000000000000000000000000000000
    000000000000000000000000000000000000000000000400000000000000000000
block[ 0].f:
    332851203C1F0C904DEED6410B7531CB1BAFE41FF27C23BD7448E40F7DF16FBB
    A6FEB5CFA65C0CBFC723F896F23C3408EE529641899E84A5CB1ADF3A82884883
block[ 1].f:
    07E2BB60A9FAC6D9BE26B5B3A364230C98B6BD27D590D428A96A85454CB8BBD2
    980EFD5F9C74C2D3AD70D656F110262BB959719C2C80F1E05C257D8F67E30831
block[ 2].f:
    CC6E6452EDCEADD9636F4BFFE1A8029E3B85207111785C27DA1C1AEE9900C3B3
    898265156847F0F286CFBBF96731A752F27EBD215B04B3E32AAD7BB3DFC49517
final:
    E85748C52E31639147671CEA466CEA0AE72C4A2CC96C7A21DE2BA48AE6EF2464
    0A9474E645A7D25E255E9E89FFF42EC7EB31349007059284F0B182E452BDA882
HASH-256:
    0A9474E645A7D25E255E9E89FFF42EC7EB31349007059284F0B182E452BDA882


ТЕСТ ГЕШУВАННЯ (N = 2048)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
    808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9F
    A0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF
    C0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
    E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
    808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9F
    A0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF
    C0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
    E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
    800000000000000000000000000000000000000000000000000000000000000000
    000000000000000000000000000000000000000000008000000000000000000000
block[ 0].f:
    332851203C1F0C904DEED6410B7531CB1BAFE41FF27C23BD7448E40F7DF16FBB
    A6FEB5CFA65C0CBFC723F896F23C3408EE529641899E84A5CB1ADF3A82884883
block[ 1].f:
    07E2BB60A9FAC6D9BE26B5B3A364230C98B6BD27D590D428A96A85454CB8BBD2
    980EFD5F9C74C2D3AD70D656F110262BB959719C2C80F1E05C257D8F67E30831
block[ 2].f:
    0063E75C51D37AFE0A8B0C11478495F89D7599B7A33114AA21F06DF9A2BAADEF
    EF495481B102E51ED8B92776DD9B52BF5C8A91B9A4ACB3298905FC7B2731694A
block[ 3].f:
    FB34558370FFAC9FFE3728C557898745DBE1E0D64C5A50D305E038AF99073A04
    FA51A6C83DE587055990F99485C4567E565303E97487C8BE943DF24C5F206035
```

```
block[ 4].f:
    70FC7FE3D71FF6D0DBD93B0AE682280F28EC42E90BCB9415ACAB8BDC4875AFE4
    5FF55807CFAEDE93F269A4625FF2C318EC9C8C67CC02E763ECEE76F45DF255A3
final:
    321D1CC888C40E2C31FB4431F619D891FC2EEDF506023A7F651A5DBA3754C52C
    D305A32B963D149DC765F68594505D4077024F836C1BF03806E1624CE176C08F
HASH-256:
    D305A32B963D149DC765F68594505D4077024F836C1BF03806E1624CE176C08F


ТЕСТ ГЕШУВАННЯ (N = 8)
INPUT:
    FF
padded:
    FF80000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000800000000000000000000
block[ 0].f:
    620E3130D80F88DE6EF30B037537D927F4EDA40FBA53E97BAEE4D14F5636F7A1
    A85152444AFF1F0971A7AB621CE1155FDA2730FB94CA3B128AA5252F1BC8312E
final:
    68F8A3B662FFC6525D1049070D5EF8AC95EFDCF81E09F986C78B8671EB79569C
    EA7677CA4526555680441C117982EA14059EA6D0D7124D6ECDB3DEEC49E890F4
HASH-256:
    EA7677CA4526555680441C117982EA14059EA6D0D7124D6ECDB3DEEC49E890F4


ТЕСТ ГЕШУВАННЯ (N = 760)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E80
    0000000000000000000000000000000000000000F802000000000000000000000
block[ 0].f:
    332851203C1F0C904DEED6410B7531CB1BAFE41FF27C23BD7448E40F7DF16FBB
    A6FEB5CFA65C0CBFC723F896F23C3408EE529641899E84A5CB1ADF3A82884883
block[ 1].f:
    7A183DFBCCE5E32342988748D4F3D8574D34E445B28AF92AFF0EAE12A48187BB
    2FBCABD5A9E8A83827A1A15210B7AFD884C0F2F00F57249EDE3D98408B43116C
final:
    E976DD1E81FE86DB875211722D72BA5AB8F02B6B16DA3A2A56358AFF6C196614
    1075C8B0CB910F116BDA5FA1F19C29CF8ECC75CAFF7208BA2994B68FC56E8D16
HASH-256:
    1075C8B0CB910F116BDA5FA1F19C29CF8ECC75CAFF7208BA2994B68FC56E8D16


ТЕСТ ГЕШУВАННЯ (N = 0)
INPUT:
    ""
padded:
    8000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
block[ 0].f:
    A338CA99EA4A6CCE4EA4364AE9E392CDA9980E490D457A7B27171F4F73F9BB4C
    3F4D28BFCA519D66D1B30410144B4F2FE7D10AA89F21355030107C5F36D6D535
final:
    C59962A2DBB880A700B82C52215FD3F1F94AA22419122B4C9D0288F6F157BC7A
    CD5101D1CCDF0D1D1F4ADA56E888CD724CA1A0838A3521E7131D4FB78D0F5EB6
HASH-256:
    CD5101D1CCDF0D1D1F4ADA56E888CD724CA1A0838A3521E7131D4FB78D0F5EB6
```

```
ТЕСТ ГЕШУВАННЯ (N = 510)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3C
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3E
    000000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000FE0100000000000000000000
block[ 0].f:
    B6E487CF9382F4F04EB562CC4075E82ABD1FA4842005E7383B85D3AD8523D96B
    63976C8C04A9D73982727352354BABF523EBF6A5EFC37BC3029D92BF55D3251B
block[ 1].f:
    2B6FFE010BC3B81C5D6C1DE01ACBDEB947A32156AE4F18B4789A9A5896413337
    69CCCD9774F9E8B11B050BF72F21EF7A89ACBA7ED103AF355D1EF139C3378FB6
final:
    363AF5B88D2153253971DEB32CD99BE390E86B8BBC383D3D1D41B7FE2B88CD1A
    875C0023DAA0C077809FDD6A9672B49E03903BFF98EBE48740AE998C7BE3851E
HASH-256:
    875C0023DAA0C077809FDD6A9672B49E03903BFF98EBE48740AE998C7BE3851E


ТЕСТ ГЕШУВАННЯ (N = 655)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F5050
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505100000000000000000000000000000
    00000000000000000000000000000000000000000008F020000000000000000000
block[ 0].f:
    332851203C1F0C904DEED6410B7531CB1BAFE41FF27C23BD7448E40F7DF16FBB
    A6FEB5CFA65C0CBFC723F896F23C3408EE529641899E84A5CB1ADF3A82884883
block[ 1].f:
    028D7BE0E6D9D437C96B870C0587F40C928DF4BD39126022F28A6782AD24B8AB
    79E6C2B3A41376EF1EDD0967E561D01080633045F7A87708A51311C3252B679D
final:
    F6B9D1DBDABA127293A870FBA2D4D4F3BAD91B134CA304D328BE5B47BD8185FE
    4237D7DE1A00C4CC8037EDE9C54BA60D1C705CD1495DE19E5245BF3509DB59CE
HASH-256:
    4237D7DE1A00C4CC8037EDE9C54BA60D1C705CD1495DE19E5245BF3509DB59CE
```

Приклади для перевірки геш-функції у режимі «Купина-48»:

```
ТЕСТ ГЕШУВАННЯ (N = 512)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    800000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000200000000000000000000
block[ 0].f:
    332851203C1F0C904DEED6410B7531CB1BAFE41FF27C23BD7448E40F7DF16FBB
    A6FEB5CFA65C0CBFC723F896F23C3408EE529641899E84A5CB1ADF3A82884883
block[ 1].f:
    56C926AFF9CDE45340DFB15C75941BEB6A6500DE35319B4A4905B56585F6B1F2
    933E3737FC1A0BDC9F94B3254066917E00FC289D027EF13871320FA9A545304C
```

```
final:
    86A9D24E23F4B103B72B8C69D1F1BBB5117EC3017604DCDF6BF04F3DA95C0268
    08F4EE6F1BE6903B324C4E27990CB24EF69DD58DBE84813EE0A52F6631239875
HASH-48:
    2F6631239875
```

Приклади для перевірки перетворень $T^{\oplus}_{1024}$ та T^{+}_{1024} геш-функції у режимі «Купина-512»:

```
ТЕСТ ПЕРЕТВОРЕННЯ T⊕1024
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
round[ 0].add_c:
    000102030405060718090A0B0C0D0E0F301112131415161728191A1B1C1D1E1F
    602122232425262778292A2B2C2D2E2F503132333435363748393A3B3C3D3E3F
    C041424344454647D8494A4B4C4D4E4FF051525354555657E8595A5B5C5D5E5F
    A061626364656667B8696A6B6C6D6E6F907172737475767788797A7B7C7D7E7F
round[ 0].s_box:
    A8BB9A4D6BCB452A793ADFB31790511F92152B3DC91CBB831F5C71D56F5716BD
    34F6C002B4F4AD118E0F7A5E496DD1662E26C445D15DB7949C140E1A5810B2DF
    2F6BD70E4233C386C49B4E858F95CB9981634FEE963C5530124918B1BC37E671
    782B8FFD6A45B9AA1C0D2FAB388CDA60EBDC050C36B56CECCD62B17C14A55E5B
round[ 0].s_byt:
    A86205AB6A37556679BBB10C3845E694923A9A7C368CB9DF1F15DF4D14B5DA86
    345C2BB36BA56C998EF6713D17CB5E302E0FC0D5C99045719C267A026F1C51AA
    2F14C45EB457BB60C46B0E4549F416EC819BD71AD16DAD5B12634E0E585DD12A
    78494F854210B71F1C2B18EE8F33B283EB0D8FB19695C3BDCDDC2FFDBC3CCB11
round[ 0].m_col:
    86C37798D2C341A03D40B8B9E2D021B8EDF7EC7C7624852BE454C7EE3A2AAD4E
    9D55309ED99527D09204D40B63DC5B6F4D2590F2228318181819A801E26A9090
    2BE1E2D9F05181F4596EFABC35F984EB0CCB22FCB22ADC5C98D3ED8395CD50D4
    CE5A52168ED88C03081D60B9B28BAE4DFEA83FFB07F135B57178E6C89B206AD3
round[ 1].add_c:
    87C37798D2C341A02C40B8B9E2D021B8CCF7EC7C7624852BD554C7EE3A2AAD4E
    DC55309ED99527D0C304D40B63DC5B6F2C2590F2228318186919A801E26A9090
    AAE1E2D9F05181F4C86EFABC35F984EBADCB22FCB22ADC5C29D3ED8395CD50D4
    0F5A52168ED88C03D91D60B9B28BAE4D1FA83FFB07F135B58078E6C89B206AD3
round[ 1].s_box:
    46287EA40A28A597491AFE4764503CDA90665A28B29E3F5EF8CC893BD502EE32
    3C3CA6C1074785E78CEA01B3B71F976049F427DCA3006213F95C208D647927C3
    A62C13358163C959FBE32169637F6DAD0B85C057CE022A18BF7406F1D75210FE
    097B4F538939EC4D07575647CECF31CF39E490C959C278509BD40A96DE312FF7
round[ 1].s_byt:
    46D4904789522A6049280AC9CE391013901A7E9659CFECC3F866FEA4DEC23159
    3CCC5A470A3178AD8C3C892864282F1849EAA63BB250A5FEF9F401C1D59E3C4D
    A65C27B307023FCFFB2C20DCB747EE500BE3138DA31F85F7BF85213564009797
    0974C069817962DA077B06576363275E39574FF1CE7FC9329BE45653D7026DE7
round[ 1].m_col:
    B9E5BA2127BC6B0D1ED38309030433AF78A43B45832ED290FDE5108E000662BB
    95D68362E659424455A4268E634AC0AD1B939F279A3E6639D1F3947877C45839
    605EC85186651D6E180A5F1D052A6E7B4EC25AC6BF8E15250970509799457634
    F8434CD47B869D03CD7ED85D89BA63A85DED54EA60BA9E7460DDDD36D6EDC9B4
round[ 2].add_c:
    BBE5BA2127BC6B0D0CD38309030433AF5AA43B45832ED290CFE5108E000662BB
    D7D68362E659424407A4268E634AC0AD79939F279A3E6639A3F3947877C45839
    E25EC85186651D6E8A0A5F1D052A6E7BECC25AC6BF8E1525BB70509799457634
    3A434CD47B869D031F7ED85D89BA63A8BFED54EA60BA9E7492DDDD36D6EDC9B4
round[ 2].s_box:
    99BEF22F0E1D151E17745D5206EAE3C766EF41F4607379C382BE4A27A8138FCD
    1A615D151349D7E559EFAD27B76852D077FE8311B5D8B908E5F050673B9AD008
    64603214184570FA21D648797502DA7CCF9418E6263DF451993010C040336C40
    D5F39DFEF5555B4D39831BC47D23774926FB4DE334234024699965E850FB266F
```

```
round[ 2].s_byt:
    99994DC4F533F4D017BE65E37D556C086674F2E834235B0882EF5D2F502377FA
    1ABE41520EFB407C59614AF4061D265177EF5D2760EA1540E5FEAD15A873E34D
    64F0832713137949216050l1B7498F24CFD63267B568D76F999448143BD8521E
    D5301879189AB9C739F310E67545D0C326839DC0260270CD69FB1BFE403DDAE5
round[ 2].m_col:
    6001234411173B7C7B36D974877A6C9452CA2ED9F64D54D1691B5D7D1318BC3E1
    CEE175B328A9D21366C160CB410A38969C089BFC5E45BE9E89385F84AB8AD7B4
    BF276AF9E639A2763DDDF7C2F218A9519613C7C7F92AE9C398D83F95AC8CFB6C
    6CB95B52D5D5397A5190356C4EAE8C13C933168E976D5C8A20AAB60ADCD4DB65
round[ 3].add_c:
    630123441173B7C7A06D974877A6C9450FA2ED9F64D54D16A2B5D7D1318BC3E1
    8DE175B328A9D21335C160CB410A3896FF089BFC5E45BE9EFA385F84AB8AD7B4
    3C276AF9E639A276AEDDF7C2F218A9513513C7C7F92AE9C32BD83F95AC8CFB6C
    AFB95B52D5D5397A8290356C4EAE8C132A33168E976D5C8AD3AAB60ADCD4DB65
round[ 3].s_box:
    B7BBD8E5F36CC12B788C24E93B7026F4097106B26AB37D5301E163B072CFF3BB
    1B2C6E8E1F40793D636E56AFF2D609EB80E9D2574733DDC1E69F487B749C636F
    58AA2F91131457A8A299AA93C0C5EB1463B4892B2502A70FE13990C22D0E8B89
    760C97AEF8B33BDBFE7D78890478EC3D15F7BB27708CD3430DFF0D263C5368BE
round[ 3].s_byt:
    B7FFBB89F80EA7EB78BB0D2704B38BC1098CD82670783B6F017124E53C8CECA8
    1BE106E9F353D314632C63B23B6C680F806E6EB06A70C189E6E9568E72B326DB
    589FD2AF1FCF7D3DA2AA4857F240F34363992F7B47D679BEE1B4AA917433092B
    76398993139CDDF4FE0C902BC0146353157D97C225C557BB0DF778AE2D02EB3D
round[ 3].m_col:
    C2E3EB6FED37A859C565BE940ED824CC96D3A4455D551FB1F702BB461F55D7C2
    620CE8B439DE9F8F86A2AB5A9CAB0154BC99241F910A9A4A11E00A8736497192
    2F9043B4646FA783864AC58EEF8066336E02E276DD9379A4424474938A53315A
    6215C6E01A62E1F06057700E855A3903A4F99C811B90620DF75910BBE512F736
round[ 4].add_c:
    C6E3EB6FED37A859D165BE940ED824CCB2D3A4455D551FB1C302BB461F55D7C2
    260CE8B439DE9F8FD2A2AB5A9CAB0154D899241F910A9A4A65E00A8736497192
    AB9043B4646FA783124AC58EEF806633CA02E276DD9379A4F64474938A53315A
    A615C6E01A62E1F0B457700E855A390340F99C811B90620D035910BBE512F736
round[ 4].s_box:
    D4D06160D63E2092EA45DD29D8395C6ACE7407F4A93CE1908CEB6FF9393C6393
    9AD2C56F19AC83090A718E415DC3D9C8C48F5CBD84D695D68872DFA0FA9B0BB6
    747D036F6A20BCF11D68BE278D2AB945C1EB13A862FEFDF6A7BD14D7215B2C41
    981C19CB9748FF64AEA11E19DA7B3B4DDC7F3E7EFD7D8F1E06494ACDD956AAE8
round[ 4].s_byt:
    D4493E19975BFDC8EAD04A7EDA482CD6CE4561CDFD7BFFB68C74DD60D97D3BF1
    9AEB0729D6568F450AD26FF4D83EAAF6C471C5F9A9392041888F8E6F393C5C64
    74725C41193CE14D1D7DDFBD5DAC631EC16803A084C383E8A7EBBE6FFAD6D992
    98BD13276A9B956AAE1C14A88D200B90DCA119D7622ABC93067F1ECB21FEB909
round[ 4].m_col:
    877E938FB162D780B3DE917A0F603DA527FA985D80DD5EE0C13FCDC007D51F50
    D7AC34BD19B67A9A6680543A49873B1FF4DF0B4486C5358DBDE5065E4DFA01FB
    82DD302C0C1199B108FC3B2E0FFE72E8CB0F28E982EE8EEC550C269D893FE4C9
    2EDBEC4D98E2975EC9C51DBDBD86D8AA791D47B1D6129EF2D3B5EA36CF389941
round[ 5].add_c:
    827E938FB162D780A6DE917A0F603DA502FA985D80DD5EE0F43FCDC007D51F50
    92AC34BD19B67A9A3380543A49873B1F91DF0B4486C5358DC8E5065E4DFA01FB
    07DD302C0C1199B19DFC3B2E0FFE72E86E0F28E982EE8EECE00C269D893FE4C9
    EBDBEC4D98E2975E1CC51DBDBD86D8AA9C1D47B1D6129EF226B5EA36CF389941
round[ 5].s_box:
    FE83A809BE48633498ACCFDB09E7DE755F8A28C49B99E6CB4EBC64A759B3E131
    69A976A2E0B8B18C612A4DCECCBF41BD84AD02E5188478BFFBBE452C6E8AD9C9
    5999A6D11715309030C7413C0929050BC3F85395FEDB8074ACD2ADFF7DBCF1A3
    B9CD5ACF67DD242C6F8470A2AA551BE45D572E90505640DC9AE1E7E8829F3038
round[ 5].s_byt:
    FEE12EA267BC80BD9883E790AADDF1BF5FACA8E8505524C94E8ACF0982561B90
    69BC28DBBE9F400B61A964C409483074842A76A79BE763A3FBAD4DA25999DE2C
    59BE02CEE0B3E6E4309945E5CCB8E1DCC3C7A62C18BFB138ACF841D16E844134
    B9D2533C178A78756FCDAD950915D9CB5D845AFFFE2930319A5770CF7DDB058C
```

```
round[ 5].m_col:
    F2DD68A97BC6993031DE35B6B68C01908F55A3A08DC5F8D0AFC85A4411588639
    8B23D87C2411C1EE5D25D9A12D86B23BFC9E3A5E7C757BE183E455F263A21ABC
    C2ED6920AE3D7E06537DA445734BA62B9976745CCB349968BFACF1E91C2D78FB
    4AFB0DA04E36E5C11C3C05BA8C642215080F3234BB3C071291D7772D26C30C7A
round[ 6].add_c:
    F4DD68A97BC6993027DE35B6B68C0190A955A3A08DC5F8D099C85A4411588639
    CD23D87C2411C1EE0B25D9A12D86B23B9A9E3A5E7C757BE1F5E455F263A21ABC
    44ED6920AE3D7E06C57DA445734BA62B3F76745CCB34996809ACF1E91C2D78FB
    8CFB0DA04E36E5C1CA3C05BA8C642215EE0F3234BB3C071267D7772D26C30C7A
round[ 6].s_box:
    4E99AC33F5E830700EAC78018A0ED9C3023C1F971B848CE7404F18E5F3818808
    20581B28B415B63B95F4232ED255CA1AB5B00E2C14B5E5BB4487A9DCB7717169
    42FBB858A2105E4E03A507F4284E8A5EA13F14185E08309BDFA904956F6D66C9
    3F27DC97044447C6C154223F3F96C04A73F8C4409954FC4653AF7E169A289FDB
round[ 6].s_byt:
    4EAFC43F046D301A0E997E403F4466BB02ACAC1699964769403C78339A54C04E
    204F1F01F528FC5E955818978AE89F9BB5F41BE51B0E30C944B02328F384D9C6
    42870E2EB4818C4A03FBA92CD2158846A1A5B8DC1455B6DBDF3F0758B7B5CA70
    3FA914F4A271E5C3C1270418281071E77354DC955E4E5E0853F822976F088A3B
round[ 6].m_col:
    862032FB967FB79AD5E867C858C588F0009606B6C4F97FE4D4EB0DEE6C840ED2
    ADC89B06533BE20CE0C5BFED1F552400BCD94DFD1D0593AF8D3584ECFFF0DA5E
    8326BFD8747897FFD9605272E32CA3069706A2930E5AA94B7AFB4380EB893827
    CE5869E7E95E7E3E2664A2239F29BB00ED57CF6F398AF52984EFAE32C43A23EC
round[ 7].add_c:
    812032FB967FB79AC2E867C858C588F0279606B6C4F97FE4E3EB0DEE6C840ED2
    EAC89B06533BE20CB7C5BFED1F552400DBD94DFD1D0593AFFA3584ECFFF0DA5E
    0426BFD8747897FF4E605272E32CA3063006A2930E5AA94BCDFB4380EB893827
    095869E7E95E7E3EF164A2239F29BB000A57CF6F398AF52973EFAE32C43A23EC
round[ 7].s_box:
    4C31C4C9D35FC18CE8ECE296C284C7640E094501357F33BA1003DC3B387E5182
    514FD24E5AAE135431844398393C5C68B8357D1B4BCBA8C7E65D6D7480B63D2C
    6B22438136D4246104E74F6210DF1F4E921357D7D87BEB8520270334B9D50911
    DF81B87829605EE154965702B10F6F6887A18260199C863E285931F335C8D874
round[ 7].s_byt:
    4C59820229D5EB68E8313160B16009C70EECC4F3190F5E2C1009E2C9359C6F61
    51034596D3C8864E314FDC01C25FD885B884D23B3584C111E635434E387FC7E1
    6B5D7D985A7E336804226D1B39AE513E92E743744B3C137420134F8180CB5C8C
    DF27576236B6A864548103D710D43DBA8796B834D8DF248228A15778B97B1F54
round[ 7].m_col:
    20763E14C4D47FFAF4B5F84A848DF5543F74DA57AED5A548CE85069A27B45954
    44F2F8BDED41862169046E7887855A7F09F1898A3C5FD336C170FC8076299824
    ED71390D2BA81A94BD49A7ED3FE661870DE2AEB2C9987B21ABA3C6114F8CACC1
    40C5BAE39F09DC6B2E1291A97EFCC826FFF30A02F174E9A95166483F0C701462
round[ 8].add_c:
    28763E14C4D47FFAECB5F84A848DF5541774DA57AED5A548F685069A27B45954
    0CF2F8BDED41862131046E7887855A7F61F1898A3C5FD336B970FC8076299824
    6571390D2BA81A942549A7ED3FE66187A5E2AEB2C9987B2113A3C6114F8CACC1
    88C5BAE39F09DC6BF61291A97EFCC82617F30A02F174E9A9A966483F0C701462
round[ 8].s_box:
    1F3FB22D355333B8CFE18CD65C0A86C8AF4A3D30A2B31CE9A7A2458C0E387BC8
    17018CA2D66B882F72EADA6746A2185B48C2F74358CABFE8EC30F834B20F28ED
    88DC3B1EE1E47129B69BBC98A15E81A068DD3100050BE52FCB4B1903270EABC6
    CD84F276B13A2AABA756CF3308C7329EAFF0DFCA544AA73302FC92DF17309415
round[ 8].s_byt:
    1FFCDF33B10EE55BCF3F92CA083AABE8AFE1B2DF54C72AEDA74A8C2D174A3229
    17A23DD63530A7A0720145305C53942F48EA8C8CA20A33C6ECC2DAA20EB386AB
    8830F767D6381C9EB6DCF843466B7B33689B3B3458A28815CBDDBC1EB2CA18B8
    CD4B3198E10FBFC8A7841900A1E428E9AF56F203055E71C802F0CF76270B812F
round[ 8].m_col:
    61999B6493F2352DF7C99AFF85F31A68A63663CCF386842665F7BC3649A8FA59
    57705B123BA19EEC550D66A06950779B4BED5B4A24B51062C725F537B92D3D31
    AB85DD8DF6B27C18CB33B45B7C0CBAA0CAA4913B16C489A893FF47BB31DA4616
    8FD59747133AA16D06BC8BEB05BD7B3E5B9BB4D72BCE71DE53177E6F249392BF
```

```
round[ 9].add_c:
    68999B6493F2352DEEC99AFF85F31A688F3663CCF38684265CF7BC3649A8FA59
    1E705B123BA19EEC0C0D66A06950779B22ED5B4A24B51062BE25F537B92D3D31
    2285DD8DF6B27C185233B45B7C0CBAA063A4913B16C489A82AFF47BB31DA4616
    46D59747133AA16DDFBC8BEB05BD7B3EB29BB4D72BCE71DEAA177E6F249392BF
round[ 9].s_box:
    868FD2373A01781673779561DAF0719BFF44776AED556D9EBC66BDE8CCE42192
    45309746AD3240741790B997F94C7E1DA3FB97D6B4E14A15F6F48694EC6DDE5D
    A3A265BFA7806013E2F71AB114D2F297B7EFCF1A2C9AF74915D72ECD72DEC353
    7AB32486CBC8699CC81DE9AD7525E5E1CE6A1A5CE1F20B80A6435E60B4FE997A
round[ 9].s_byt:
    86431AADCBDEF71D738F5E5C75C8C315FF77D260E125695DBC449537B4F2E513
    456677613AFE0B971730BD6ADA019949A39097E8EDF07853F6FBB946CC55719C
    A3F49797ADE46DE1E2A286D6F9322180B7F76594B44C407A15EF1ABFECE17E16
    7AD7CFB1A76D4A9BC8B32E1A1480DE9ECE1D24CD2CD26092A66AE986729AF274
round[ 9].m_col:
    7976A8771FD70089B9911C5510ACB521BBB26F845450EDDF269A01E31FD86E1E
    508174D0EEAB0B19774FF172EC8F73DB2F49D594B8B976DDE168827863E62014
    EF144D22BB8227FCD8374C9D8CDAD93C6C8201154ABDCA0B47146C7EF03EAED6
    570D0531B868C5BD128B99E2AA495B6D4E8EEF850E453C46C51454323E2CD19F
round[10].add_c:
    7376A8771FD70089A3911C5510ACB52191B26F845450EDDF1C9A01E31FD86E1E
    1A8174D0EEAB0B192D4FF172EC8F73DB4549D594B8B976DD9B68827863E62014
    65144D22BB8227FC42374C9D8CDAD93CC68201154ABDCA0BFD146C7EF03EAED6
    9D0D0531B868C5BDC88B99E2AA495B6DA48EEF850E453C463F1454323E2CD19F
round[10].s_box:
    283F20EC39AF939AE593CD486DA9FB2F8480387B964C06EF6F9DD9763939DAF5
    97DA14E773C3028AD2EE0462CF51D6B4E49B5F291C0C6CFCDE12F067B75E492D
    88657D0D99C98557833E9DFF3FDE233AD4C9D94AAB25B0B38B65A4AC81D83187
    3090225D1C12BEA2FBCF306BA69B979C003D448FD8334CF9A1654DF3BBDFF5B2
round[10].s_byt:
    2865446B1CD8B0B4E53F4D8FA61231FC849320F3D89BBE2D6F80CDECBB339757
    979D384839DF4C3AD2DAD97B6DAFF5B3E4EE147696A99387DE9B04E7394CFBA2
    88125F627339069C8365F029CFC3DAF9D43E7D671C5102B28BC99D0DB70CD69A
    3065D9FF995E6C2FFB90A44A3FC949EF00CF22ACABDE85F5A13D305D8125238A
round[10].m_col:
    B865BC4A54E887CB44160E01BC93EED21E956D4C00B0C7694544769769855303E
    A62A38358DDB9EA064A0F4928B6A3838D5B6FF8AD9197BCCBF96643583A6897A
    B7E12E5685CC29A6A1845BA30171AA97FE4952197061A0282F83DDE2E833B8E0
    F0B3039119EBE5DA3FA56F80CB1350CE49162E27D75254D968685DF897DAF156
round[11].add_c:
    B365BC4A54E887CB5F160E01BC93EED235956D4C00B0C7697E4476769855303E
    ED2A38358DDB9EA03FA0F4928B6A3838BEB6FF8AD9197BCCC496643583A6897A
    3CE12E5685CC29A63A845BA30171AA97554952197061A0289483DDE2E833B8E0
    3BB3039119EBE5DAE4A56F80CB1350CEA2162E27D75254D993685DF897DAF156
round[11].s_box:
    BD45BDD696EC8DAF4188518D94FE468263477C23A88B898808BD6CA8673CA6E1
    D60209CC1BCD4097A11839B6B0790956F6B86743075CE56A3509CCCC6070F7DB
    582CD1D3DAE2A107D57E976543DCCEC0169B4F8A222BB3F29D00656B12F7FECB
    AD1EB59FE00347DED03B38345EB410840188D1111A8E4D353A12367F70DE04D3
round[11].s_byt:
    BD12D134E0F7B356414536115E03FE6A6388BD7F1AB447DB084751D6708E1007
    D6BD7C8D96DE4DC0A1026C2394EC04F2F61809A8A8FE8DCB35B839CC678B46DE
    580967B61B3C8984D52CCC43B0CDA635167ED1CC077940D39D9B97D3605C09AF
    AD004F65DA70E582D01E658A43E2F788013BB56B22DCA1E13A88389F122BCE97
round[11].m_col:
    09D01155348D9BAE4E4C0E4C61D7C9D62B5DC8ECEE95D43E599E0FA3B3B14B16
    94DCE5AEDCD0CD5F3424234966B23AC1F39569D80856687C0E6C3D9BCB99B842
    E30B28CF320D1CBF9D2F4E290D9E84EE935A12AD43DE1BDC6F1CCA73F686A24E
    B69DFB7B065EA4771913D14E9B64B98716A05E710FE661A1A98A01EB4B386929
round[12].add_c:
    05D01155348D9BAE524C0E4C61D7C9D6075DC8ECEE95D43E659E0FA3B3B14B16
    D8DCE5AEDCD0CD5F6824234966B23AC19F9569D80856687C726C3D9BCB99B842
    6F0B28CF320D1CBF012F4E290D9E84EE3F5A12AD43DE1BDCD31CCA73F686A24E
    7A9DFB7B065EA477C513D14E9B64B987FAA05E710FE661A1558A01EB4B386929
```

```
round[12].s_box:
    75501748D10AD242E216512348AF268759373274734701E188B05965BD461253
    C41F47423C506471869ED84FA5800EC6B147B8817119AC282489DE1D5E8FFE6E
    1EB253399E90CD7A434DCB3EF0B06D3BA17B2BD037ACD4A50DF5B00CA7555732
    BAB98B7C6C6007EC03B4F532DE96FAA0E618E6BC095E812E169CD9AD4A9FB83E
round[12].s_byt:
    759CE6326C55D4C6E250D9BCDE605728591617AD0996076E883751484A5EFA7A
    C4B03223D19F813B861F5974480AB8A5B19E476573AFD2322447D842BD4726EC
    1E89B84F3C4601A043B2DE81A550122EA14D531D7180643E0D7BCB395E190E42
    BAF52B3E9E8FAC8703B9B0D0F090FEE1E6B48B0C37B0CD531618F57CA7AC6D71
round[12].m_col:
    0F1D1C87FCC4ADBA6F9E3F0DC147F61502938AF58781738065D4F9FF4A2DB4DB
    42C7463231C2F59A2A2ECBF0DC60BCDFBAE12F1D90CAB225D58D2CFB3DCB3385
    7350D65E10C8E9908B7B56A7369E4293A2338C1124AC94512C38E367F3F86D75
    3225882F24C18C9ED715EF9759E40AE9E9526F4D50B508962DB352F042747C12
round[13].add_c:
    021D1C87FCC4ADBA729E3F0DC147F6152F938AF58781738058D4F9FF4A2DB4DB
    0FC7463231C2F59A772ECBF0DC60BCDFD7E12F1D90CAB225A88D2CFB3DCB3385
    FE50D65E10C8E990167B56A7369E42930F338C1124AC94519138E367F3F86D75
    FF25882F24C18C9E0A15EF9759E40AE904526F4D50B50896D0B352F042747C12
round[13].s_box:
    5F57CDA07C9AEE3F24B0901EEFFA544AC6FE1DA946DAD634C2533461AB6D1AB4
    09A3C3F37294868C3B73EA643CE7BDEF1A2C7279EBD3CA51C50A2DC9A485E38F
    564C752C6D4FA7C32C065504FAB0D7D709F7EC03B4A95014849F58AAED217CA6
    80F4C766B46EECC1871C44C06587DF956B8E38CF2EE1BAEBF71E4F64834A6046
round[13].s_byt:
    5F1E38C0B42150EF24574FCF656E7C51C6B0CD642E87EC8FC2FE90A083E1DFC3
    09531D1E7C4ABAD73BA334A9EF9A60141A73C36146FAEEA6C52CEAF3ABDA54C1
    560A7264726DD6952C4C2D793C941AEB090675C9EBE7864684F7552CA4D3BD3F
    809FEC046D85CA4A87F45803FA4FE3346B1CC7AAB4B0A7B4F78E4466EDA9D78C
round[13].m_col:
    604B9DCF7EAA578594D183EEF2DD97A32C111C8170C0A5086A08C9E428811132
    31BEC7B71D0EE31DE8363B4AA6AF890BDEEE5C96663A44383A40093060E76515
    2DEBECD25B8342C4EF4E750FC3F4814FA9E1D11FE7F6F8CF3272E7E1614F91AD
    6F01F728D8DBBE1F2AC197771E378F8DD7D131327BF1A943A955F1F7C832ADF3
OUTPUT:
    604B9DCF7EAA578594D183EEF2DD97A32C111C8170C0A5086A08C9E428811132
    31BEC7B71D0EE31DE8363B4AA6AF890BDEEE5C96663A44383A40093060E76515
    2DEBECD25B8342C4EF4E750FC3F4814FA9E1D11FE7F6F8CF3272E7E1614F91AD
    6F01F728D8DBBE1F2AC197771E378F8DD7D131327BF1A943A955F1F7C832ADF3
```

ТЕСТ ПЕРЕТВОРЕННЯ T^{+}_{1024}

```
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
round[ 0].add_c:
    F3F1F2F3F4F5F6F7FBF9FAFBFCFDFEEF03020304050607E80B0A0B0C0D0E0FE0
    131213141516 17D81B1A1B1C1D1E1FD023222324252627C82B2A2B2C2D2E2FC0
    33233334353637B83B3A3B3C3D3E3FB043424344454647A84B4A4B4C4D4E4FA0
    535253545556 57985B5A5B5C5D5E5F9063626364656667886B6A6B6C6D6E6F80
round[ 0].s_box:
    EDC2A0F04EED5417CA7F21C97CC0743606EBB5737513FC0B95D60254F01759CB
    CB56C22D4D88A381FD36D4254B67E1E74F64D8EDB6228596E102C8D1D27372A7
    612EE3406344B4DAADC8413AA4D8906C376903E5E4AB2E494A6812236E913597
    5A8E9EC81619C6A40F7B9718A96048C3B748773788FCE205DB7915897BE33834
round[ 0].s_byt:
    ED79771816912EE7CAC21537A9193596067FA0898860C6A795EB21F07BFC48DA
    CBD6B5C94EE3E26CFD5602737CED38494F36C25475C05497E164D42DF01374A4
    6102D8254D17FCC3AD2EC8ED4B88590537C8E3D1B667A3344A694140D222E117
    5A68033A637385360F8E12E5A444720BB77B9E23E4D8B4CBDB4897C86EAB9081
```

```
round[ 0].m_col:
    BA64F543FEDE1D21E02989B4D829A24B4D03A3A5C01B7AB64CEA7C00B4622629
    8CC8F61C7B0C8938D010F7B88D77D45622D00D4CF449517A499C9595426950A3
    1C46BF9B374A374452B9E741D202FD8C6E8D4AC42F8687E4E886E5DB6384C36D
    6BAB761BEB18954A9D481FC5FA5D660A8A12AC510ED9DAD7C9E3EC1450970EC3
round[ 1].add_c:
    AD55E634EFCF0E13D31A7AA5C91A932D40F49396B10C6B883FDB6DF1A45317EB
    7FB9E70D6CFD79EAC301E8A97E68C5F815C1FE3CE53A420C3C8D8686335A4125
    0F37B08C283B28B645AAD832C3F3EDEE617E3BB520777836DB77D6CC5475B4AF
    5E9C670CDC09867C903910B6EB4E572C7D039D42FFC9CBE9BCD4DD054188FFC4
round[ 1].s_box:
    0B3C0A408D82513D0D36B1750536A816DC5AA8EBBED21505A1CD7C6D005BA3AD
    550C7F1E38C0FDE38CBBC5330812BE7F4D6E743AD9C8D754580A8863617BA551
    093E73211FAE5301E4FF1BF38CF0063B488341503E9766E8B897756A96B51AC7
    4707E2543C3A8828EB144A01B991C6D19F925B6E8077EA959453654BF211670A
round[ 1].s_byt:
    0B535B013CB5667F0D3C656EB93A1A54DC360A4B80918851A15AB140F277C601
    55CDA8758D11EA3B8C0C7CEB058267E84DBB7F6DBE3651C7586EC51E00D2A828
    090A7433385B15D1E43E883A08C0A39548FF7363D912FD0AB8831B2161C8BE3D
    479741F31F7BD716EB0775508CAEA5059F14E26A3EF053AD94924A54969706E3
round[ 1].m_col:
    D9F54B3022D4D304853FB096C643DDD870D05346CF8A4AE674CCD64EF04CDB75
    E57273A272D0CA665696E2EC57CCAB19B9AE6A4E61A420AFD761E0BF52038610
    9B0CA73F1AF91753A8B40C68C800EC0E7D0821F6786EE86B219824B1A94F41E5
    C3858655B86D9E6F9F83E5E13E4DB4F671117FB7B43A4CDC057684CDC5DBA5CE
round[ 2].add_c:
    CCE63C2113C5C4F77830A187B734CEBB63C14437C07B3BB967BDC73FE13DCC38
    D863649363C1BB194987D3DD48BD9CBCAC9F5B3F52951142CA52D1B043F47693
    8EFD97300BEA08C69BA5FD58B9F1DC7170F911E7695FD9BE148915A29A403228
    B6767746A95E8FA29274D6D22F3EA519640270A8A52B3DEFF86675BEB6CC96D1
round[ 2].s_box:
    905E4C2FCB84AE178E7C69A0310884CDB76E11942F064147532589DF52104B56
    C4FDCCD7B76E6F8ACCBFBFFC9C253E692D9897DFE247176EC18EF56C375A6CD7
    89C0247095C6BAE6DE3B0CA1ECC22ABC227F1778F9CA23E2C9D5F4F8B51AC4F2
    8A3F7EF9026029F8694A7582C6D81C8A6AEB1E4968B1DE3685FC6EE28AE237B0
round[ 2].s_byt:
    90FC1E82021A23698E5E6E49C660C46EB77C4CE268D829D7536E692F8AB11CE6
    C42511A0CBE2DEBCCCFD8994318437E22DBFCCDF2F08AEF2C198BFD7520684F8
    898E97FCB710418ADEC0F5DF9C6E4B36223B246CE2256FB0C97F0C7037473E17
    8AD517A1955A17CD693FF478ECC66C476A4A7EF8F9C2BA5685EB75F9B5CA2A8A
round[ 2].m_col:
    9432E24F702FE16EB21641C0C88F71636194F11B78B1BD058C6EE0CCD4447429
    9E7C706C69913FFAB2DE323A54972D9C410B82562C0E4184352730195227E47B
    731199845F394E571E00431910326905B6C9FA447F89060A3609EB5B419D4569
    DE9BD97C72A37709A8D807224A80BB692A1D10B373637E24A84C7CDCFEEE60FC
round[ 3].add_c:
    8723D3406120D262A50732B1B98062475485E20C69A2AED97F5FD1BDC53565ED
    916D615D5A8230AEA5CF232B45881E4034FC72471DFF31182818210A4318D5FF
    66028A75502A3FCB11F1330A01235A69A9BAEB35707AF75D29FADB4C328E36AD
    D18CCA6D6394683D9BC9F8123B71AC8D1D0E01A464546F389B3D6DCDEFDF5100
round[ 3].s_box:
    4658BFB54831791568C1C490EC2A8F8696A21354F971313555CAF5A2035D9C98
    848C81C466C9A6426882D85EE41116B5D1C705864BD72C131FC53C2637C55F61
    A5EB1DA62E0290AFF3C2E32643581888022361CC222DAAC4BF8A68239E3DB7D0
    EA0EB09CB7C4ACD2DE778C46ADDCABBF4B17D9F66ACC3856DE107C128DADD568
round[ 3].s_byt:
    4610D946B73DAAB568587CF6ADC4B71396C1BF126ADCAC6155A2C4B58DCCABAF
    84CA139048AD3888688CF554EC31D5C4D18281A2F92A79D01FC7D8C403718FD2
    A5C5055E665D31BFF3EB3C86E4C99C5602C21D264B11A668BF23E3A637D71615
    EA8A61262EC52C86DE0E68CC43025F354B77B02322589098DE178C9C9E2D1842
round[ 3].m_col:
    4A3ADCE95DCF95C49ABFAE9217DDB38843771A98DB3659FFCF60CEC422E2DE2E
    805F25C8641D60070506A0EB6B492CF33CC539257CFA734A453DDE547CAA05C1
    BA5DBA20EACAF7201BAA35F5B03472D0635C45F55BB392C529DC2164D1C31F4A
    91CFE4D84B92478DB3E59006C230CC631829CF05FE38B5F3E47ACC388CBAFE0F
```

```
round[ 4].add_c:
    3D2BCDDA4EC086B98DB09F8308CEA46D36680B89CC274AD4C251BFB513D3CFF3
    735016B9550E51BCF8F690DC5C3A1D982FB62A166DEB64DF382ECF456D9BF645
    AD4EAB11DBBBE8950E9B26E6A1256335564D36E64CA4831A1CCD1255C2B4108F
    84C0D5C93C8338C2A6D681F7B221BD880B1AC0F6EE29A608D76BBD297DABEF14
round[ 4].s_box:
    A4B164DE04F188471B8B83F171F2079CFA12029A90AA4EFEE8634350CB7482F0
    284CBB471617D56985A727A5BCC870A4C6B87A537B03CCEFF47382F47B6A54F4
    0B918E03B876C5C2D86AAD7D11F477CC2395B77D8FEF5DB76F522B48E8384A09
    5CF15FA3580009939861C917CEF696059536524C730F8AD41AE5963E9FC3442D
round[ 4].s_byt:
    A4E5521758385DA41BB1964CCE004AEFFA8B643E73F609F4E81283DE9F0F96C2
    286302F104C38ACC854C439A71F144B7C6A7BB5090F28809F4B82747CBAA0793
    0B737AA516744E05D8918253BC1782D4236A8EF47BC8D52D6F95AD037B037047
    5C52B77DB86ACC9C98F12B7D117654FE95615F488FF4C5F01A36C9A3E8EF7769
round[ 4].m_col:
    1F5B9DA8225DBFB05CF286EBEF7142DCDFB68E831B047BF1D55713B828477D67
    A6C4DB75747496B695E49EBD1194E46F05553F3729AAAB761E1053CE59045CCD
    241D51E7B69ABE978F6F5AC0F857843BE1196C2326D4409A63007138FCB717B5
    FEB25FD275A74B145CB7DD1E10907DE40A1743D047A0BD78EF6C80FA4FBA8819
round[ 5].add_c:
    124C8E99134EB0A64FE377DCE06233C2D2A77F740CF56BC7C84804A919386E2D
    99B5CC666565876C88D58FAE0285D515F84530281A9B9C0C110144BF4AF54C53
    170E42D8A78BAF0D82604BB1E94875A1D40A5D1417C531F056F16129EDA808FB
    F1A350C366983C4A4FA8CE0F01816E0AFD0734C13891AE8EE25D71EB40AB791F
round[ 5].s_box:
    1D16808BCB91730727D07EA5AC48E3930AA0332417ED152BFBD19833E09FDA16
    40E14B5F88458D89CDB329425FA25F4A8533A6F2976A3E54F3BB117AABED9DEE
    AF17D781A0CFA21EFEE7129029D16E2E7ED6362DAF842C6423C2813ED6E4BAC9
    544B100FA50B4CD627E4841F43DADA268BC176C6F493312764370BADDCC3FDBD
round[ 5].s_byt:
    1D37761FA5E42C4A27160BC6430BBA540AD080ADF4DA4CEEFBA07E8BDC93DA1E
    40D133A5CBC3312ECDE19824AC91FD6485B34B33174873C9F333295FE0EDE3D6
    AFBBA642889F1526FE1711F25F45DA277EE7D77A97A28DBD23D61281AB6A5F07
    54C23690A0ED3E93274B812D29CF9D2B8BE4103EAFD1A21664C1840FD6846E89
round[ 5].m_col:
    5483D5A1EED506FD8469651E2B7C4D3CBE34A1AF029754C1EC04561AD965C6CE
    42055A86021F8F99C69B0FCE5212D7822D360212C5E73281F97C76F14C009D59
    F044294A9C10B0D1AF9A4801E181DC1622A9971C5E9CCBADE2E1820873A95354
    19926FD5CCE5484E6B684C0888D6106DDDC4FAEABE99C049CC98E2372C328B23
round[ 6].add_c:
    4774C692DFC6F7F3775A560F1C6D3E23B12592A0F3874598DFF5460BCA56B795
    35F64A77F30F8050B98C00BF4303C8292027F302B6D82318EC6D67E23DF18DE0
    E3351A3B8D01A148A28B39F2D172CD7D159A880D4F8DBC04D5D273F9639A449B
    0C8360C6BDD639855E593DF978C70194D0B5EBDBAF8AB160BF89D3281D237C2A
round[ 6].s_box:
    324A19B6C8E8AAF03B7B551F6F8CB202BEF49997EDBF00A4C8EDC3B3C119C1C2
    63A74EECEDF88731EC0E937A3792323E3EAADBCA8A39D813CF8CE26BA4C2EDCB
    105D711A1BBB69E901CF3BDCEAB764DD4D9DC71E270ABD73F82FD691B79D111D
    170056E6AA613B8F4749DE918EA3D929F7E161B4769CF97226D5BFF24B586055
round[ 6].s_byt:
    32D56191AA9DBD3E3B4ABFB48E611113BE7B19F276A33BCBC8F455B64B9CD9E9
    63ED991FC858F9DDECA7C3976FE860733E0E4EB3ED8CAA1DCFAA93ECC1BFB28F
    108CDB7AED190029015DE2CA37F8C1724DCF716B8A928755F89D3B1AA43932F0
    172FC7DC1BC2D8024700D61EEABBEDA4F749569127B769C226E1DEE6B70A6431
round[ 6].m_col:
    32B6BD9C772BFDD6D8F990FC3DF2855C9A6B5207F76EC0AE2D647ADCFCE3ACB9
    13B1D91D885CFA7DCD677A63DA445BD1D98CFA118C150BEFB0081B7515A2468C
    BF624A179C98BF88FC2522931FAB6CF8D5A05A29DD5752260E241DB0A40E46A8
    4C9EF566268854865DE51ACDE904CF16A1E2D47F031336A6A8CB9394AB76D0C6
round[ 7].add_c:
    25A7AE8D681CEECECBEA81ED2EE376448D5C43F8E75FB18620556BCDEDD49D81
    06A2CA0E794DEB35C0586B54CB354C79CC7DEB027D06FC86A3F90B6606933714
    B2533B088D89B000EF161384109C5D60C8914B1ACE48437E01150EA195FF36F0
    3F8FE657177945BE50D60BBEDAF5BF3E94D3C570F40327BE9BBC84859C67C1CE
```

```
round[ 7].s_box:
    B6A031BF86F546845EC6C99893D06CE51B6F037F0CCAF9633E3C1512D6535B7E
    6C71B019779561CC2F8115C85E5D9D2090A561CA9F13F863E57F025F6CFEB42D
    CE5B41D41BD573688D88C27B6D073672FB9312B73DD103AC431C512ED7D7B764
    A1510A30AF6200E22E6102E257ED43E19D74BEEA4E9285E2DE1D6D8F5D41B684
round[ 7].s_byt:
    B61DBEE2AFD703205EA06DEA5762B7631BC6318F4EED002D3E6FC9BF5D924368
    6C3C0398864185722F71157F93F5B6AC9081B0120CD04664E5A51519D6CA6CE2
    CE7F61C87753F9E18D5B02CA5E955BE2FB88415F9F5D61844393C2D46C139D84
    A11C127B1BFEF8E52E5151B76DD5B4639D610A2E3D07737EDE740230D7D136CC
round[ 7].m_col:
    65BF2BFD729B94D4B00C48F5BB8E6B730DA4A83C691868F2D40C84B1E49ADDDB
    719EFAB98235C9A227DE78A94A8D62BFB17BE8F5515A8F4CD6577149B20194FE
    9FAA1A78E3211A96B64307EAD9C91E3D3B914B679900231C1AC5C5484482114C
    1B29273F996D1798F1C9FAE05F7F5A4DB6E621D7AF5FA4362F229DEA7182C329
round[ 8].add_c:
    58B01CEE638C85CDA3FD38E6AC7F5C5C0095992D5A0959CBC7FD74A2D58BCEA4
    648FEBAA7326BA5B1ACF699A3B7E5368A46CD9E6424B80E5C948623AA3F28487
    929B0B69D4120B0FA934F8DACABA0FA62E823C588AF113750DB6B63935730295
    0E1A18308A5E08D1E4BAEBD150704B76A9D712C8A050954F22138EDB6273B432
round[ 8].s_box:
    C28BCD3BB70E3F12E5C0097D2D5FD318A8473016663A7BAF7FC014F8F8CF84F6
    6A5161E42822F2B19782B88CAD839E9B0089237D834E875A05D18FCEE5016DA0
    696A02887E56021F02088CDEC123590793C94CA121C2C2A6F0B80D08636C9AC2
    D83662702160BAB0D02361B02E3012A802AF2B96784C0F99A3B480B4FC6C1AF3
round[ 8].s_byt:
    C2B42BB0216CC29BE58B80962E609A5AA8C0CDB47830BAA07F47093BFC4C121F
    6AC0307DB76C0F07975114162D0E1AA6008261F8665F3FC20589B8E4F83AD3B0
    69D1238C28CF7BA8026A8F7DAD228499930802CE8383F2F3F0C98C88E54E9E12
    D8B84CDE7E018718D0360DA1C1566DAF02236208212302F6A3AF617063C259B1
round[ 8].m_col:
    03CCEF0FD1218835E6A512FD7F466DEDFED0CA51A034E4A42AEFE6BF7600E569
    B21636E75B7416C521392DE1F49B3331D88E44F1EEE534B5FCA40DA84B6C0A0E
    B8ABA1C895C01B12B40E6D43AAF18E0911B7D7BC23D0FA1840821D5DA35FF541
    DC39FC2A59FF7F68491140631B22F257F0B1701737C2B15E61139A5863E15BA7
round[ 9].add_c:
    F6BCE000C212792FD99603EE70375ED7F1C1BB429125D57E1DE0D7B067F1D533
    A50727D84C65077F142A1ED2E58C24DBCB7F35E2DFD6254FEF95FE983C5DFB97
    AB9C92B986B10C8CA7FF5D349BE27F7304A8C8AD14C1EB7233730E4E9450E68B
    CF2AED1B4AF070A23C0231540C13E381E3A2610828B3A27854048B4954D24CB1
round[ 9].s_box:
    A71DF668E856FD660709B53B223EE65C546E6F6E84F45FAC4B72636C53C25F45
    68C185818F45FC5BC9021682D90E5CB45E5F786BC8619B998D4774A458378BC0
    7407994718469F21A0D73640DEDD330C6BE432D0C96E6162616C51329D4C0A77
    820206D5ABB61EF858EB2CC817B4587E107181D41F1E576796EAE94F962F9D90
round[ 9].s_byt:
    A7EA81C8AB4C61B4071DE9D417B60A995409F64F1FB41EC04B6EB568961E5821
    68726F3BE82F570CC9C1636E22569D625E02856C843EFD778D5F168153F4E6F8
    744778828FC25F7EA007746BD9455F676BD799A4C80EFC9061E4364758615C66
    826C324018379B5C580251D0DE468BAC10EB0632C9DD9F4596712CD59D6E335B
round[ 9].m_col:
    6E8355CD1B229344E75180E3BE92CB8F0134B17B78D3251C8773428B06017C07
    96316EF877C227AF11985A95EE7B1940432662B53431D9B7F2E4CD7599E7009F
    EB2B3A7842D2B640712F16815E0EF99C41AC7F7488A858F081802BA9A0CD08FA
    AD7840082C499F94A9333855920D4D46D69BD72B929CEB5DA3651AFB1FF9051D
round[10].add_c:
    617446BE0C13843FDA4271D4AF83BC7AF424A26C69C416F77A64337CF7F16CD2
    89225FE968B3186A04894B86DF6C0AEB361753A62522CA52E5D5BE668AD8F129
    DE1C2B6933C3A7BB642007724FFFE907349D70657999494B74711C9A91BEF944
    A06931F91C3A90CF9C24294683FE3D71C98CC81C838DDC7896560BEC10EAF627
round[10].s_box:
    484AC3E217B46DDF57690BFE7600BDDB4E9E5789F99ABB17BA96E3282AC2A482
    7D644895861E62D86BD51263C889DFADFA439E07B664B0AED9B3DD5F2139043E
    E3F5C8886128BCCD6A31FC6227D7A72AD1B91EBE778FEF8536DCCD8C842434E5
    780D2C916FC827395D9EA1F96029DEBC050E3225600A2A67D31902746DC65411
```

```
round[10].s_byt:
    481932F96F24EFAD574A022560C834AE4E69C3746029273EBA9E0BE26D0ADECD
    7D9657FE17C62A2A6B64E38976B45485FAD54828F9006DE5D94312952A9ABD39
    E3B39E6386C2BBBC6AF5DD07C81EA467D131C85FB689621136B9FC882164DFDF
    78DC1E626139B0DB5D0DCDBE27280417059E2C8C77D7BC82D30EA191848FA7D8
round[10].m_col:
    EC4242E6E3B00F299103E1AB5B87327E676B8CC35395F1FAA1904E3F6F33FDF9
    6B4A99E082A4E4E559474F44E90A809744D1DECDDA9137299361AC6FFB0910AF
    D102E0363F68B52A8669F5D1F92B6794CF08D2D89A121AA100F6A742D68199FA
    65C096A313214D0FA5D2084E6B47FA3DFDA73ADCD1F0E099176491F11E0F5473
round[11].add_c:
    DF3333D7D4A1002584F4D19C4C78236A5A5C7DB44486E2D694813F306024EEC5
    5E3B8AD17395D5A14C384035DAFB704337C2CFBECB8228C586529D60ECFA003B
    C4F3D0273059A6A6795AE6C2EA1C5800C2F9C2C98B030BFDF3E69833C7728A46
    58B1879404123E4B98C3F93E5C38EB69F0982BCDC2E1D1B50A5582E20F00457F
round[11].s_box:
    C8F7E35C7E3293515C5AF5FB8FD4D8D8666FAF6F425513879DDA9070349E4606
    47AE1DB028475F2E8F9F25CC57271E0EEE9482E25EC95306188E5B72CF8A931A
    35F06B1192498A07777B0A9351F5D068E87F08A3B092021BED5E28457FB71DF9
    C2468D296B56B285672834E1BC9F6188810BC812E82CF550873CF06B09CE005B
round[11].s_byt:
    C83CC8E16BB7020E5CF7F012BC561D06665AE36BE89FB21A9D6FF55C092C6107
    47DAAFFB7ECEF5688FAE906F8F32001BEE9F1D7042D493F9189425B03455D885
    358E82CC289E138877F05BE257474650E87B6B725E275F5BED7F0A11CFC91E51
    C25E0893928A53D8674628A35149938781288D45B0F58A06870B34297F92D02E
round[11].m_col:
    062DC290BF1067D4855A4C5DF54C3452384F8741D928D98D2EDFC01AA53D7B10
    4A0510F39BCC482468B516D01F82F5EC9D84D8494209F585CF6BB113E5D3C6E6
    9A5A5E1E69FB98DCD056A0BBB5BA7D0AD20853ADD10445A8189455A467BD2C05
    3BEFA8550BD2FE4EEB263E7D82F197950B9547BEDA8840F4671FA5DF2A8D0D4E
round[12].add_c:
    F91DB381B00158D1784B3D4EE63D253F2B407832CA19CA6A21D0B10B962E6CDD
    3DF600E48CBD39E15BA607C11073E6999075C93A33FAE522C25CA204D6C4B773
    8D4B4F0F5AEC8959C34791ACA6AB6E77C5F9439EC2F535050B85469558AE1D52
    2EE09946FCC2EF8BDE172F6E73E288C2FE8538AFCB7931115A1096D01B7EFE5A
round[12].s_box:
    25573A7EB3BBD0B08E4EDE3213109BDFE11A66F3C15CB0D8DD50F9B3D373A4FC
    A4A793BA3F253BBB0F70FCC66D6C0A8BEBB526CE618A470DE86F5773509AC10C
    1B4E351F6634F7928CFACFB998C3DAEC037F03C1E8ED784B95A2C3C2C27870AE
    937230F97C944477E34372FA28DDC79356A209C75E622C03664237E7FD837441
round[12].s_byt:
    254209FA7C78788B8E5737C72894700DE14E3AE75EDD440CDD1ADE7EFD62C792
    A4506632B3832CEC0FA7F9F313BB744BEB7093B3C110D0AEE8B5FCBAD35C9B77
    1B6F26C63F73B0938C4E57CE6D25A40303FA3573616C3B41957FCF1F508A0AB0
    93A203B9669A47DFE372C3C19834C1D8564330C2E8C3F7FC66A272F9C2EDDABB
round[12].m_col:
    19EA0E7E5E95FAEE8E7CA96E49AC193255D2B1703978352ACFB790BACE023A08
    AAEFBBFC13EB2D3D24114528E9688FD663DBA990D6F03221E88A6DEDA300508E
    9F0514D5FF22D422DC6C9D174F5EF9AF89074AD8FFEC9A534CC2AD16A018F5C8
    78DA55EEB5340B578E531EEABCA9F6C1ACA3297B7938F9547A7635FB7D8E5C64
round[13].add_c:
    0CDBFF6E4F86EBEC816D9A5F3A9D0A2048C3A2612A692608C2A881ABBFF32AD6
    9DE0ACED04DC1EFB17023619DA59808456CC9A81C7E123BFDB7B5EDE94F1401C
    92F604C6F013C5A0CF5D8E08404FEA1D7CF83AC9F0DD8BB13FB39E079109E616
    6BCB46DFA625FC9481440FDBAD9AE7EF9F941A6C6A29EA726D6726EC6E7F4D72
round[13].s_box:
    17CD67FA275561744C8C9571D5B9DF589C285744150DADD4E8E4C9D926F07A87
    3072AB986B1F16C9AFEBB78A5749877B23E2957E7F2CD87AB806E6809DC22525
    69A798E681B4BE97823780D4DCEEE77914210EA38199E990A11E402A843A0A53
    DB85C3EF98F4F8294CBD59B40B9D7F36B1C471895B0FE7627B41AD74C35F7D62
round[13].s_byt:
    174171B4983AE97B4CCDAD890BF40A7A9C8C67745B9DF825E82895FAC30F7F97
    30E45771275FE779AF72C944D5557D9023EBABD915B96153B8E2B798260DDF29
    6906958A6BF0AD3682A7E67E571F7A62143798807F491662A12180E69D2C8774
    DB1E0ED481C2D8584C8540A3DCB425D4B1BDC32A81EEBE877BC459EF8499E7C9
```

```
round[13].m_col:
    36575D993036AFDEB2654C1E13660A9D4F0E105CA2336F2BB3690045259A1A9D
    3F248507C342A70B42F74981ECE46DD05E1D309F774E1ED213247CC821461673
    C7419AE12B9361F32C7538C15909B197E20F9E09DD28CDD4D7C234DBDB479318
    A258A7180B1833178A20FCFE05A6064FD7B1EA9607995E98D90D2D55DCF72F5F
OUTPUT:
    36575D993036AFDEB2654C1E13660A9D4F0E105CA2336F2BB3690045259A1A9D
    3F248507C342A70B42F74981ECE46DD05E1D309F774E1ED213247CC821461673
    C7419AE12B9361F32C7538C15909B197E20F9E09DD28CDD4D7C234DBDB479318
    A258A7180B1833178A20FCFE05A6064FD7B1EA9607995E98D90D2D55DCF72F5F
```

Приклади для перевірки геш-функції у режимі «Купина-512»:

```
ТЕСТ ГЕШУВАННЯ (N = 512)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    80000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000020000000000000000000
block[ 0].f:
    F667151F2565C5C03B16CA22CFA299146CA8D5365FD4735691E5D6577C1AF901
    7A617F1BA0B4B1D01F0C497D5C9443C305F7F69C1D81AD6D268174D31B7B03F4
    51D6CBF8D066C586502FD72695B91A71EE490C5E9294DC08093EFAD3A89698AA
    FD450BB8225784B0B1FDE9CCA657332B975B597F8FEC7400B3CCDB6B4C6E46C0
final:
    A831B6BA47C4F091DBC1E902A96A0B3BD8747F37DBC262FAEE2F37BB312BEF29
    1BA98C5A29FA3928938F784931C6C331BA80E96A6FF2C1DB9D897D0C07CDA57B
    3813E2109118CDFB5A6D5E72F7208DCCC80A2DFB3AFDFB02F46992B5EDBE536B
    3560DD1D7E29C6F53978AF58B444E37BA685C0DD910533BA5D78EFFFC13DE62A
HASH-512:
    3813E2109118CDFB5A6D5E72F7208DCCC80A2DFB3AFDFB02F46992B5EDBE536B
    3560DD1D7E29C6F53978AF58B444E37BA685C0DD910533BA5D78EFFFC13DE62A


ТЕСТ ГЕШУВАННЯ (N = 1024)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
    80000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000040000000000000000000
block[ 0].f:
    1628B5406F0224E7D9397A969D5D94591D5C8E42FE19E046C3FBC000ED826B61
    94990525FF2E5091A2909783A631B666072041844359727AE038693EA9EAA64C
    3DFB1074A253525F7A95BAD13C6F2F2EB9D98ACA307A2562335820C32402BACE
    DF516EA17EF173F1F11567BFE94DD3331F5D76107CC1B46D94E24A5C50DD0A7A
block[ 1].f:
    004C02A008A68BA14BA489FC4D2C5C58E28BAEF190DD9C8983C42834A68D0439
    41913C2C189C5EE8CAD6F247B572A20408CCF30DA3FC460AB0069EB8C7329C3A
    F1E8AA46A81141FC661890AD252997E047AD0B78FB321F85948981B856DD7B3F
    CA28646950624C04DE3775F05273EC475582D3EE8E42A8667834F760B29FBF11
```

```
final:
    6E1E4DF99CE48DE66D66278FA5BD366197FCC0BE35454C9E414BDF740DFBEF72
    DD45F428BE889F07BA59727410870D836CB622DBA8536CF85666B3E825B7ABCE
    76ED1AC28B1D0143013FFA87213B4090B356441263C13E03FA060A8CADA32B97
    9635657F256B15D5FCA4A174DE029F0B1B4387C878FCC1C00E8705D783FD7FFE
HASH-512:
    76ED1AC28B1D0143013FFA87213B4090B356441263C13E03FA060A8CADA32B97
    9635657F256B15D5FCA4A174DE029F0B1B4387C878FCC1C00E8705D783FD7FFE


ТЕСТ ГЕШУВАННЯ (N = 2048)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
    808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9F
    A0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF
    C0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
    E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
    808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9F
    A0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF
    C0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
    E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
    800000000000000000000000000000000000000000000000000000000000000000
    000000000000000000000000000000000000000000000000000000000000000000
    000000000000000000000000000000000000000000000000000000000000000000
    000000000000000000000000000000000000000000008000000000000000000000
block[ 0].f:
    1628B5406F0224E7D9397A969D5D94591D5C8E42FE19E046C3FBC000ED826B61
    94990525FF2E5091A2909783A631B666072041844359727AE038693EA9EAA64C
    3DFB1074A253525F7A95BAD13C6F2F2EB9D98ACA307A2562335820C32402BACE
    DF516EA17EF173F1F11567BFE94DD3331F5D76107CC1B46D94E24A5C50DD0A7A
block[ 1].f:
    BAF25AE07E75A55D1E95A8E5C2F922E48093F4E4C652A0DD735FEA527C9CE215
    6B4AEFA58C68C35414530BEEA704B3EBD0BF5DA0FB4E440372032E0C2DFD61E7
    289ECDBDD4DC40400B8E2E13D8BBC0686E570F87BE48AA301ADE433CBD17B8BA
    850DB6329174C9BA7B08CC51873CD57418C20A919D524298505A8EFEB7DD378D
block[ 2].f:
    3395B9E1D958A69958B38CE44C33C5BC6513FD513E8BFAAC6C56EBFBB2B11B13
    BAF60242A0F68EC0DE7450A45A8BDCF91CB8B0091ABCECF1B02C9302D3CB1BF0
    1B1ED5D9D7C612080F35041377D62F81D16E987A0073EFE9EBD40A635B512EB8
    5D7A9CA9FD2C63E04EE3E16BFD69B78A6E92649F651DDE6E17EF905CA7CB065E
final:
    CA34E77DEDE7AF95220C2820CD6083823E48A792C1D09D99431C220CE0F458AC
    01FF65E5E1C730AEA8B2D75B3135222AF0D23E90C54DBD3EFE8D1A03EFCAC4F3
    0DD03D7350C409CB3C29C25893A0724F6B133FA8B9EB90A64D1A8FA93B565566
    11EB187D715A956B107E3BFC76482298133A9CE8CBC0BD5E1436A5B197284F7E
HASH-512:
    0DD03D7350C409CB3C29C25893A0724F6B133FA8B9EB90A64D1A8FA93B565566
    11EB187D715A956B107E3BFC76482298133A9CE8CBC0BD5E1436A5B197284F7E
```

```
ТЕСТ ГЕШУВАННЯ (N = 8)
INPUT:
    FF
padded:
    FF80000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000800000000000000000000000
block[ 0].f:
    D63FF30DCE785B60764519513B0A1E43D8B2C3FD40CD84B66F9F7DCC6D183FC0
    565C4FA456C9C35FE83EC4D9DE063A62246EFB003BC96C09BDFC79D877E8438D
    9F1658C492C8FFBA4860F083974B09D9108C32724B74DC023D54EB8A6725130C
    C5B10143811728287D165CF2C3C939E6416671491CF3962BDDBDCE4B2111C231
final:
    EC7DD314D9978774267926DB439A2809410CFCBE581A9D555A428CF2B9910AD7
    C0B57A9BCB1400A3EA8E9FDF501FAAF209C34B2DCF06FA52D5A780C3D30CE0F5
    871B18CF754B72740307A97B449ABEB32B64444CC0D5A4D65830AE5456837A72
    D8458F12C8F06C98C616ABE11897F86263B5CB77C420FB375374BEC52B6D0292
HASH-512:
    871B18CF754B72740307A97B449ABEB32B64444CC0D5A4D65830AE5456837A72
    D8458F12C8F06C98C616ABE11897F86263B5CB77C420FB375374BEC52B6D0292


ТЕСТ ГЕШУВАННЯ (N = 1536)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
    808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9F
    A0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
    808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9F
    A0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF
    800000000000000000000000000000000000000000000000000000000000000
    000000000000000000000000000000000000000000000000600000000000000
block[ 0].f:
    1628B5406F0224E7D9397A969D5D94591D5C8E42FE19E046C3FBC000ED826B61
    94990525FF2E5091A2909783A631B6660720418443597 27AE038693EA9EAA64C
    3DFB1074A253525F7A95BAD13C6F2F2EB9D98ACA307A2562335820C32402BACE
    DF516EA17EF173F1F11567BFE94DD3331F5D76107CC1B46D94E24A5C50DD0A7A
block[ 1].f:
    DF9F1E7426AFCD67F61402A567EFDC1BB74EB9BA5B3F76DF88FC21C14C1B5129
    EB4816D9926D670EB2F40D646EF853E5A77FA01E71BAC2A28B313EF784520A87
    0E43573C01D062DAE01F85EE33C4FC879CE9FE8B7A44DDDFBFB15F5B1114F134
    7CE3C9E0D2479A7E854E15B3A7030A3475D31F0EB315D79034E2F02D8F85AAA9
final:
    F59A8CF72B529530D350367D15C6CD0702C5D48B2E7720DFD28AB41B76A6F35A
    293A5B05D848F60B7158835A208C0ADB565BB5F3034800D2683D42FC3818BFEC
    B189BFE987F682F5F167F0D7FA565330E126B6E592B1C55D44299064EF95B1A5
    7F3C2D0ECF17869D1D199EBBD02E8857FB8ADD67A8C31F56CD82C016CF743121
HASH-512:
    B189BFE987F682F5F167F0D7FA565330E126B6E592B1C55D44299064EF95B1A5
    7F3C2D0ECF17869D1D199EBBD02E8857FB8ADD67A8C31F56CD82C016CF743121
```

```
ТЕСТ ГЕШУВАННЯ (N = 0)
INPUT:
    ""
padded:
    8000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
block[ 0].f:
    6049885FBE371F32F439DAB60FA523B99444CDCC17732FE5DD60A93F275AF2E8
    22E0FC944148B971FBAEE46B68E4819EC75C60F47D8DCEC92A0858FF3470F9B1
    82BC2AE42B17F38551AC6458691F46B5DFA482B727F401A1E373DF8C321B0D58
    9325C32C67D0E1A30DC9858359849D521CBB50F40323C255315EA7D70BE1AF55
final:
    4A97F6D5B099CF28075FA89CE599C25AABCB59A04EF02530EFC9378CBC561AAB
    BB922BDB4F606A7DA322B73C802B9AB74C97D5947B3A9B0B8744A8BD35EED5BF
    656B2F4CD71462388B64A37043EA55DBE445D452AECD46C3298343314EF04019
    BCFA3F04265A9857F91BE91FCE197096187CEDA78C9C1C021C294A0689198538
HASH-512:
    656B2F4CD71462388B64A37043EA55DBE445D452AECD46C3298343314EF04019
    BCFA3F04265A9857F91BE91FCE197096187CEDA78C9C1C021C294A0689198538


ТЕСТ ГЕШУВАННЯ (N = 510)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3C
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3E
    0000000000000000000000000000000000000000000000000000000000000000
    000000000000000000000000000000000000000000FE0100000000000000000000
block[ 0].f:
    679DDAA7BC4723B7FDF9D517717A2CF2A890A28258834DAA9EF0BF420559FDAE
    4B6D8E9916F08B100B048EF4943F86D6E0611512B7ADD908AD9C35D7826B7346
    4BCD465DAB9A28B876828845D428942129E92DA36DA3B6AACF0D9FF6B0F0E728
    5139E0319CA688A2FA61042A327BB843E531E7446D4EB52FFA7988487A87D833
final:
    3082594858E2F22F466BDC75DA9A81B4AAE7AA80B8724D09FB6E762A1360658C
    45A922D9446C9F495D5E6281BE7144F922C57F0909955ABC026FDEC0526E7F8B
    2F3BBAC98E8771D6E3B8AA30153ABC4D0C2985E91DA1B5568FD1BDD705CCAB7E
    E8D95D2FC98BFA5322A241E09C896B58284C83F2488CF943E4B3DE43E05F0DEA
HASH-512:
    2F3BBAC98E8771D6E3B8AA30153ABC4D0C2985E91DA1B5568FD1BDD705CCAB7E
    E8D95D2FC98BFA5322A241E09C896B58284C83F2488CF943E4B3DE43E05F0DEA


ТЕСТ ГЕШУВАННЯ (N = 655)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F5050
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F5051000000000000000000000000000000
    000000000000000000000000000000000000000000008F020000000000000000000
block[ 0].f:
    B68F8C062E64F890FB2DC03D2BC00B1B444F74DC785C7F23D4F6E9B9AB2DB98F
    AC9D3789F93BE7D006C67822596BCC7A576A62B6FBFF732709EEBEFE9751C098
    B24BC55E52F3BD03F37C6F465149CBB3734CD4D5F95462CDAE1EE217C724F74A
    10516B93899727BD7FA53D0280BBA3EEFC5BD51161C1E3E9690B410229D7959E
```

```
final:
    2A0390223CB88B258A76712C2CE5FE54F340362D98F487B4D2F54D9479BC93AB
    CFEE04BE8BFC7EA9E14EADAD4DEED475F598FCDB2E8851A54256A10A5440E135
    01B7BDA1DBA77D7379F53C2A498A390DE5E688A12BC75FEE9E010CB6FEBED3B9
    C7023931C74A7B55168A15047D5E2CB78A8B5CA2F75E05E80CA398030E02C7AA
HASH-512:
    01B7BDA1DBA77D7379F53C2A498A390DE5E688A12BC75FEE9E010CB6FEBED3B9
    C7023931C74A7B55168A15047D5E2CB78A8B5CA2F75E05E80CA398030E02C7AA
```

Приклади для перевірки геш-функції у режимі «Купина-304»:

```
ТЕСТ ГЕШУВАННЯ (N = 1024)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F
    606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
    80000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000400000000000000000000
block[ 0].f:
    1628B5406F0224E7D9397A969D5D94591D5C8E42FE19E046C3FBC000ED826B61
    94990525FF2E5091A2909783A631B6660720418443597 27AE038693EA9EAA64C
    3DFB1074A253525F7A95BAD13C6F2F2EB9D98ACA307A2562335820C32402BACE
    DF516EA17EF173F1F11567BFE94DD3331F5D76107CC1B46D94E24A5C50DD0A7A
block[ 1].f:
    004C02A008A68BA14BA489FC4D2C5C58E28BAEF190DD9C8983C42834A68D0439
    41913C2C189C5EE8CAD6F247B572A20408CCF30DA3FC460AB0069EB8C7329C3A
    F1E8AA46A81141FC661890AD252997E047AD0B78FB321F85948981B856DD7B3F
    CA28646950624C04DE3775F05273EC475582D3EE8E42A8667834F760B29FBF11
final:
    6E1E4DF99CE48DE66D66278FA5BD366197FCC0BE35454C9E414BDF740DFBEF72
    DD45F428BE889F07BA59727410870D836CB622DBA8536CF85666B3E825B7ABCE
    76ED1AC28B1D0143013FFA87213B4090B356441263C13E03FA060A8CADA32B97
    9635657F256B15D5FCA4A174DE029F0B1B4387C878FCC1C00E8705D783FD7FFE
HASH-304:
    0A8CADA32B979635657F256B15D5FCA4A174DE029F0B1B4387C878FCC1C00E87
    05D783FD7FFE
```

Приклади для перевірки геш-функції у режимі «Купина-384»:

```
ТЕСТ ГЕШУВАННЯ (N = 760)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E
padded:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
    202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E80
    00000000000000000000000000000000000000000F80200000000000000000000
block[ 0].f:
    116536FD9CA815744AFC6E6D2E14BA758C4F8AAD46E65F3300A93FB7E9EADC7C
    A2C3442457E78575DE0DB88C53E00E13578A3CA26BDB2EC1F912F0B4C07258B1
    107B5522DF2501B92D391908ACAAA358EFA5F82BBC37169919247B7BDAE797C1
    6F136BF4C08E1D311D0B3562A55898742EF0BBBD0EEF36B2B37966A7B5F71908
```

```
final:
    42E71F192370F7E13871951B7A41A477971E124863C9E231875D95B358F1B76F
    F5C0AC0D495B238D18450B20E1E6557F557A0F254CD5B4F19359724F838C2358
    53BBB2B549CD4F31F1CC231651302242D9021692D84E5175735654846BA751E6
    D0ED0FAC36DFBC0841287DCB0B5584C75016C3DECC2A6E47C50B2F3811E351B8
HASH-384:
    D9021692D84E5175735654846BA751E6D0ED0FAC36DFBC0841287DCB0B5584C7
    5016C3DECC2A6E47C50B2F3811E351B8


ТЕСТ ГЕШУВАННЯ (N = 33)
INPUT:
    0000FF
padded:
    0000FF00400000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000210000000000000000000000
block[ 0].f:
    AA190B9E3BADED30E0189D49E4BDC2741B1DAB8827FA0B361123B2BC37C32DF9
    62E7023E2DC7BC4EB51B679B990E710EB17BA74AB8B30B1D6E554360A8AE82EE
    4099E2BCDBD4477A41EA6B7C7AC90E44877BEFA49B018A4F045E2E6AB497CACB
    DAC1E87F9CED6A45E352BD67F4B6D3C9D4E91282401786FB5D9089E451BA09EB
final:
    3A232A8D3814F067BD07AD151303D6EE837BA6449E39792E03AAF9F97564533A
    DEC744E711B113A4AC6A07B3432C16322AFA5AC98125E68589B6E88AA501CA68
    C1AD5FD0BFC1A249C0B9E9BD8AAFD51CB0331847CB0F28E0A7ECCBDF72386F49
    2B8A07BD6AE6B4AF8C279F1C1E8D771CD033917FCDFD22EB20A0C4F663C3611D
HASH-384:
    B0331847CB0F28E0A7ECCBDF72386F492B8A07BD6AE6B4AF8C279F1C1E8D771C
    D033917FCDFD22EB20A0C4F663C3611D


ТЕСТ ГЕШУВАННЯ (N = 1)
INPUT:
    80
padded:
    C0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000001000000000000000000000000
block[ 0].f:
    A331F74555D54E41E8A4663AFCFCAD373AE5336003BC573D0205022B0D4206C3
    7A58D0B5779CA55EFF104155223A74470BA2B567394615E805D1B0797F8BAB8B
    3534F73476DF10B2920D53018A0511B479DE6001AF6C6C1EAD6761C53E9BFA3D
    12E178680C78375E3CF3BC1C6D69D0734C86EB32AF7310472C463D2FDB9DF816
final:
    71BAFF87626BC5F81536076DFF363BA46EA259C75CD4C1B505EEEDE1950E0CDE
    CF457A3F0B7E689BF5ED9D4FF1E939D35CF429C4FBB22665724C1361F672C8C3
    7D2FA4206F3E18BDC6F7967759BB17D9801BA7ACEFFF771FC331690512D432EF
    031829EDF1705B487D90B8A333C29868F586B377BE9C92F08D63F79277C82221
HASH-384:
    801BA7ACEFFF771FC331690512D432EF031829EDF1705B487D90B8A333C29868
    F586B377BE9C92F08D63F79277C82221
```

ДОДАТОК В
(довідковий)

РЕЖИМ ЗАСТОСУВАННЯ ФУНКЦІЇ ГЕШУВАННЯ ДЛЯ ФОРМУВАННЯ КОДУ АВТЕНТИФІКАЦІЇ ПОВІДОМЛЕННЯ

В.1 Визначення

Код автентифікації повідомлення (КАП), або імітовставка — бітова послідовність фіксованої довжини, отримана внаслідок оброблення функцією гешування повідомлення і ключа автентифікації для забезпечення захисту повідомлення від його спотворення та модифікації.

В.2 Позначення

$V_1 || V_2$ — конкатенація (об'єднання) двох бітових послідовностей V_1 і V_2, що ліва (молодша) частина результуючої послідовності співпадає з V_1, а права (старша) — з V_2; довжина результуючої послідовності дорівнює сумі довжин V_1 і V_2;

$Pad(M)$ — бітова послідовність, отримана внаслідок застосування перетворення, описаного у розділі 7 цього стандарту, до повідомлення M;

~ — операція побітової інверсії (логічного заперечення) кожного біта у бітової послідовності фіксованої довжини;

$\phi(M, K)$ — код автентифікації повідомлення, вироблений для повідомлення M і ключа автентифікації K.

В.3 Параметри перетворення

Режим застосування функції гешування, визначений у цьому додатку, формує код автентифікації повідомлення довжиною від 0 біт (порожній рядок) до 2^{96} — 2048 біт і ключа автентифікації довжиною 256, 384 або 512 біт у режимах «Купина-256(КАП)», «Купина-384(КАП)» і «Купина-512(КАП)» відповідно.

Для режиму роботи «Купина-n (КАП)» (n = 256, 384 або 512) і як базове перетворення застосовують функцію гешування «Купина-n».

Довжина коду автентифікації повідомлення співпадає із довжиною ключа автентифікації.

В.4 Опис перетворення

Вироблення коду автентифікації повідомлення M і ключа автентифікації K здійснюється відповідно до формули:

$$\phi(M, K) = H(Pad(K) \,||\, Pad(M) \,||\, (\sim K).$$

Таким чином, здійснюється конкатенація доповнення ключа автентифікації, доповнення повідомлення та інверсії ключа, після чого виконується гешування результуючої бітової послідовності.

Вибір режиму роботи функції гешування H («Купина-256», «Купина-384» або «Купина-512») здійснюється відповідно до В.3 та відповідає довжині ключа автентифікації K.

В.5 Приклади для перевірки

Нижче наведені тестові приклади для перевіряння правильності реалізації перетворення для формування коду автентифікації повідомлення. Застосовані скорочення наведено у таблиці В.1.

Таблиця В.1 — Скорочення, застосовані у прикладах для перевіряння

INPUT	вхідне повідомлення, що обробляється для формування коду автентифікації повідомлення
KEY	ключ автентифікації для формування коду автентифікації повідомлення
K-MAC	обчислений код автентифікації повідомлення

Приклади для перевірки режиму «Купина-256(КАП)»:

```
ТЕСТ КАП (N = 248)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E
KEY:
    1F1E1D1C1B1A19181716151413121110F0E0D0C0B0A0908070605040302010 0
K-MAC:
B60594D56FA79BA210314C72C2495087CCD0A99FC04ACFE2A39EF669925D98EE
```

Приклади для перевірки режиму «Купина-384(КАП)»:

```
ТЕСТ КАП (N = 248)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E
KEY:
    2F2E2D2C2B2A292827262524232221201F1E1D1C1B1A19181716151413121110
    0F0E0D0C0B0A09080706050403020100
K-MAC:
    BEBFD8D730336F043ABACB41829E79A4D320AEDDD8D14024D5B805DA70C396FA
    295C281A38B30AE728A304B3F5AE490E
```

Приклади для перевірки режиму «Купина-512(КАП)»:

```
ТЕСТ КАП (N = 248)
INPUT:
    000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E
KEY:
    3F3E3D3C3B3A39383736353433323130 2F2E2D2C2B2A29282726252423222120
    1F1E1D1C1B1A19181716151413121110 0F0E0D0C0B0A09080706050403020100
K-MAC:
    F270043C06A5C37E65D9D791C5FBFB966E5EE709F8F54019C9A55B76CA40B701
    00579F269CEC24E347A9D864614CF3ABBF6610742E4DB3BD2ABC000387C49D24
```

Код УКНД 35.040

Ключові слова: інформаційна технологія, криптографічний захист інформації, функція гешування, геш-функція, цілісність повідомлення, код автентифікації повідомлення, імітозахист.

Редактор **О. Рождественська**
Технічний редактор **О. Марченко**
Коректор **О. Опанасенко**
Верстальник **Т. Шишкіна**

Підписано до друку 10.03.2015. Формат 60 × 84 1/8.
Ум. друк. арк. 4,18. Зам. Ціна договірна.

Виконавець
Державне підприємство «Український науково-дослідний і навчальний центр
проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»)
вул. Святошинська, 2, м. Київ, 03115

Свідоцтво про внесення видавця видавничої продукції до Державного реєстру видавців,
виготівників і розповсюджувачів видавничої продукції від 14.01.2006, серія ДК, № 1647

Код УКНД 35.040

ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функції ґешування

Місце поправки	Надруковано	Має бути
Титульний аркуш, по всьому тексту	ґешування ґеш-функція ґеш-значення ґеш-вектор	гешування геш-функція геш-значення геш-вектор

(ІПС № 11–2015)