



НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Алгоритм симетричного блокового перетворення

ДСТУ ____:2014

(проект)

Видання офіційне

Київ
Мінекономрозвитку України
2014

ПЕРЕДМОВА

1 РОЗРОБЛЕНО

Приватним акціонерним товариством «Інститут інформаційних технологій»

РОЗРОБНИКИ:

І. Горбенко, д-р техн. наук, проф. (науковий керівник)

Ю. Горбенко, канд. техн. наук

О. Дирда, канд. техн. наук

В. Долгов, д-р техн. наук

Д. Кайдалов

О. Казимиров, канд. техн. наук

О. Кузнецов, д-р техн. наук

Р. Мордвінов

Р. Олійников, д-р техн. наук (відповідальний виконавець)

А. Пушкарьов

В. Руженцев, канд. техн. наук

2 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ наказ Мінекономрозвитку України від
____.____.2014 № ____

3 УВЕДЕНО ВПЕРШЕ

**Право власності на цей документ належить державі.
Відтворювати, тиражувати і розповсюджувати його повністю чи частково
на будь-яких носіях інформації без офіційного дозволу
заборонено.**

**Стосовно врегулювання прав власності звертатися
до Мінекономрозвитку України.**

Мінекономрозвитку, 2014

ЗМІСТ

1 СФЕРА ЗАСТОСУВАННЯ	6
2 НОРМАТИВНІ ПОСИЛАННЯ	6
3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ	7
4 ПОЗНАКИ ТА СКОРОЧЕННЯ	10
5 ЗАГАЛЬНІ ПОЛОЖЕННЯ	12
5.1 Призначення	12
5.2 Режими роботи	12
6 ПРОСТА ЗАМІНА (БАЗОВЕ ПЕРЕТВОРЕННЯ)	13
6.1 Загальні параметри	13
6.2 Подання вхідних та вихідних даних, внутрішнього стану перетворення	14
6.3 Зашифрування	15
6.3.1 Структура перетворення	15
6.3.2 Функція додавання циклового ключа K_v за модулем 2^{64}	15
6.3.3 Шар нелінійного бієктивного відображення	16
6.3.4 Перестановка елементів	16
6.3.5 Лінійне перетворення	16
6.3.6 Функція додавання циклового ключа K_v за модулем 2	16
6.4 Розшифрування	17
6.4.1 Структура перетворення	17
6.4.2 Функція віднімання циклового ключа K_v за модулем 2^{64}	17
6.4.3 Шар оберненого нелінійного бієктивного відображення	18
6.4.4 Обернена перестановка елементів	18
6.4.5 Обернене лінійне перетворення	18
6.5 Формування циклових ключів	18
6.5.1 Допоміжний ключ K_σ	18
6.5.2 Циклові ключі з парними індексами	19
6.5.3 Циклові ключі з непарними індексами	20
7 ГАМУВАННЯ	20
7.1 Загальні параметри	20
7.2 Зашифрування	20
7.3 Розшифрування	20
8 ГАМУВАННЯ ЗІ ЗВОРОТНІМ ЗВ'ЯЗКОМ ЗА ШИФРТЕКСТОМ	21
8.1 Загальні параметри	21
8.2 Зашифрування	21
8.3 Розшифрування	21
9 ВИРОБЛЕННЯ ІМІТОВСТАВКИ	22
9.1 Загальні параметри	22
9.2 Обчислення	22
9.3 Перевірка	22
10 ЗЧЕПЛЕННЯ ШИФРБЛОКІВ	22
10.1 Загальні параметри	22

10.2	Зашифрування.....	23
10.3	Розшифрування.....	23
11	ГАМУВАННЯ ЗІ ЗВОРОТНІМ ЗВ'ЯЗКОМ ЗА ШИФРГАМОЮ.....	23
11.1	Загальні параметри.....	23
11.2	Зашифрування.....	24
11.3	Розшифрування.....	24
12	ВИБІРКОВЕ ГАМУВАННЯ ІЗ ПРИСКОРЕНИМ ВИРОБЛЕННЯМ ІМІТОВСТАВКИ	24
12.1	Загальні параметри.....	24
12.2	Вироблення імітовставки для відкритої частини повідомлення та шифртексту	25
12.3	Зашифрування та забезпечення цілісності.....	26
12.4	Перевірка цілісності та розшифрування	26
12.5	Вироблення імітовставки для відкритого повідомлення.....	27
12.6	Перевірка цілісності для відкритого повідомлення	27
13	ВИРОБЛЕННЯ ІМІТОВСТАВКИ І ГАМУВАННЯ	28
13.1	Загальні параметри.....	28
13.2	Вироблення імітовставки.....	29
13.3	Пряме перетворення.....	30
13.4	Обернене перетворення	31
14	ІНДЕКСОВАНА ЗАМІНА.....	31
14.1	Загальні параметри.....	31
14.2	Зашифрування без доповнення	32
14.3	Розшифрування без доповнення	32
14.4	Зашифрування із доповненням	32
14.5	Розшифрування із доповненням	33
15	ЗАХИСТ КЛЮЧОВИХ ДАНИХ.....	33
15.1	Загальні параметри.....	33
15.2	Зашифрування без доповнення	33
15.3	Розшифрування без доповнення	34
15.4	Зашифрування із доповненням	34
15.5	Розшифрування із доповненням	35
Додаток А (обов'язковий)	Нелінійні таблиці заміни	36
А.1	Таблиці заміни для шару нелінійного бієктивного відображення	36
А.2	Таблиці заміни для шару оберненого нелінійного бієктивного відображення.....	38
Додаток Б (обов'язковий)	Доповнення повідомлення.....	40
Б.1	Загальні положення.....	40
Б.2	Доповнення повідомлення	40
Б.3	Зняття доповнення повідомлення.....	40
Додаток В (довідковий).	Приклади для перевірки.....	41
В.1	Позначення	41
В.2	Базове перетворення.....	43
В.3	Гамування.....	139
В.4	Гамування зі зворотнім зв'язком за шифртекстом.....	148
В.5	Вироблення імітовставки.....	159
В.6	Зчеплення шифрблоків.....	162
В.7	Гамування зі зворотнім зв'язком за шифргамою	168
В.8	Вибіркове гамування із прискореним виробленням імітовставки.....	175

В.9 Вироблення імітовставки і гамування.....	186
В.10 Індексована заміна.....	196
В.11 Захист ключових даних.....	215
Додаток Г (довідковий) Вимоги до реалізації алгоритму симетричного блокового перетворення.....	236
Г.1 Загальні вимоги щодо захисту від витоку побічними каналами.....	236
Г.2 Обмеження на сумарну довжину повідомлень, що захищаються з використанням одного ключа	236
Г.3 Вимоги щодо синхропосилки	236
Г.4 Захист від повторного прийому повідомлення.....	237

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології **КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ** **Алгоритм симетричного блокового перетворення**

Информационные технологии **КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ.** **Алгоритм симметричного блочного преобразования**

Information technologies **CRYPTOGRAPHIC DATA SECURITY** **Symmetric block transformation algorithm**

Чинний від 201_ - _ - _

1 СФЕРА ЗАСТОСУВАННЯ

Цей стандарт встановлює криптографічний алгоритм симетричного блокового перетворення для забезпечення конфіденційності та цілісності (як додаткової послуги) інформації під час її обробки

Стандарт використовується під час розробки засобів криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, а також при модернізації діючих систем для заміни ДСТУ ГОСТ 28147:2009.

Для забезпечення конфіденційності і цілісності послідовностей двійкових символів можливо використання цього стандарту сумісно з ДСТУ ____ „Інформаційні технології. Криптографічний захист інформації. Функція гешування”, при цьому повинні використовуватись різні ключі шифрування і автентифікації.

2 НОРМАТИВНІ ПОСИЛАННЯ

У даному стандарті використовуються посилання на наступні стандарти:

ДСТУ ____ „Інформаційні технології. Криптографічний захист інформації. Функція гешування”.

ДСТУ ГОСТ 28147:2009. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования (Системы обработки информации. Захист криптографічний. Алгоритм криптографічного перетворення).

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

3.1 байт

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

3.2 базове перетворення

Бієктивне (взаємно однозначне) відображення, параметризоване ключем шифрування або ключем автентифікації K довжиною k бітів, $T_{l,k}^{(K)} : V_l \rightarrow V_l$ (пряме відображення), $U_{l,k}^{(K)} : V_l \rightarrow V_l$ (обернене відображення), $l \in \{128, 256, 512\}$, що виконує перетворення блоку довжиною l бітів у вихідний такої ж довжини (параметризована перестановка).

3.3 біт

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

3.4 бітова послідовність

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

3.5 відкритий текст

Повідомлення для зашифрування на вході криптографічного алгоритму симетричного блокового перетворення.

3.6 вибіркове гамування

Гамування заданої частини повідомлення, при якому інша частина повідомлення залишається незмінною.

3.7 внутрішній стан

Бітова послідовність фіксованої довжини (128, 256 або 512 бітів), що є проміжним значенням на кожній ітерації базового перетворення, а також вхідним та вихідним значенням перетворень $T_{l,k}^{(K)}$ і $U_{l,k}^{(K)}$.

3.8 гама шифра

Псевдовипадкова послідовність, що сформована відповідно до заданого алгоритму, для зашифрування або розшифрування.

3.9 довжина бітової послідовності

Кількість бітів, що складають бітову послідовність.

3.10 доповнення

Вставка додаткових бітів у кінець повідомлення для отримання кратності довжини бітової

послідовності довжині внутрішнього стану базового перетворення.

3.11 допоміжний ключ

Бітова послідовність фіксованої довжини (що дорівнює довжині внутрішнього стану), отримана з ключа шифрування або ключа автентифікації при виконанні процедури формування циклових ключів як проміжне значення.

3.12 зашифрування

Перетворення відкритого тексту в шифртекст.

3.13 імітовставка (код автентифікації повідомлення)

Бітова послідовність фіксованої довжини, отримана в результаті обробки повідомлення криптографічним алгоритмом симетричного блокового перетворення, параметризованого ключем автентифікації (та синхропосилкою для деяких режимів), для забезпечення цілісності повідомлення (захисту від його спотворення та модифікації).

3.14 ключ (шифрування, автентифікації)

Параметр криптографічного алгоритму симетричного блокового перетворення (двійкова послідовність довжиною 128, 256 або 512 бітів), який відомий тільки довіреним сторонам, що забезпечує вибір конкретного перетворення із множини всіх можливих перетворень алгоритму.

3.15 конфіденційність

Властивість інформації, що визначає унеможливлення доступу до її змісту для неуповноважених осіб або технічних засобів.

3.16 криптограма

Повідомлення, яке містить шифртекст та, у разі необхідності, іншу додаткову інформацію, що подається у відкритому вигляді.

3.17 многочлен $f(x)$ степеня m над полем $GF(2)$

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

3.18 незвідний многочлен над полем $GF(2)$

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

3.19 обробка інформації

Виконання однієї або декількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрацію, приймання, передавання, які

здійснюються в системі за допомогою технічних і програмних засобів.

3.20 повідомлення

Бітова послідовність ненульової довжини на вході криптографічного алгоритму симетричного блокового перетворення.

3.21 подання у форматі little endian

Спосіб запису бітових послідовностей, коли байти, що містять найменш значущі біти послідовності, мають менший індекс.

3.22 поле $GF(2)$

Поле, що містить два елементи: 0 і 1.

3.23 режим роботи криптографічного алгоритму симетричного блокового перетворення

Спосіб застосування базового перетворення для забезпечення конфіденційності та (або) цілісності повідомлення.

3.24 розширення поля $GF(2)$

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

3.25 розшифрування

Перетворення, обернене до зашифрування.

3.26 синхропосилка (вектор ініціалізації)

Бітова послідовність фіксованої довжини (що дорівнює довжині внутрішнього стану), відкритий параметр криптографічного алгоритму симетричного блокового перетворення.

3.27 цілісність

Властивість інформації, що визначає унеможливлення її спотворення або модифікації з боку неуповноважених осіб або технічних засобів.

3.28 цикловий ключ

Бітова послідовність фіксованої довжини, що дорівнює довжині внутрішнього стану, отримана з ключа шифрування або ключа автентифікації в результаті виконання низки перетворень.

3.29 шифртекст

Результат зашифрування відкритого тексту криптографічним алгоритмом симетричного блокового перетворення.

3.30 шифрування

Оборотне перетворення повідомлення з метою забезпечення послуги конфіденційності;

складається з зашифрування (прямого перетворення) та розшифрування (оберненого перетворення).

4 ПОЗНАКИ ТА СКОРОЧЕННЯ

У даному стандарті використовуються наступні позначення:

- \oplus – операція додавання за модулем 2 (XOR) бітових послідовностей однакової довжини $p = (p_1, p_2, \dots, p_k)$ і $q = (q_1, q_2, \dots, q_k)$, $k \in \mathbb{Z}^+$, коли кожен біт результуючої послідовності $r = (r_1, r_2, \dots, r_k)$ обчислюється за формулою $r_i = (p_i + q_i) \pmod{2}$;
- $\lfloor x \rfloor$ – ціла частина x , тобто для дійсного x найбільше ціле y таке, що $y \leq x$;
- $|X|$ – довжина бітової послідовності X ;
- $L_{l,r}(X)$ – функція, що повертає r молодших бітів з вхідної послідовності X довжиною l бітів;
- $R_{l,r}(X)$ – функція, що повертає r старших бітів з вхідної послідовності X довжиною l бітів;
- \gg – операція зсуву вправо послідовності фіксованої довжини (у бік молодших розрядів; старші елементи заповнюються 0), кількість елементів, на котрі здійснюється зсув, визначається другим аргументом;
- \ll – операція зсуву вліво послідовності фіксованої довжини (у бік старших елементів; молодші елементи заповнюються 0), кількість елементів, на котрі здійснюється зсув, визначається другим аргументом;
- $+$ – операція додавання, яка визначена в адитивній групі найменших невід'ємних залишків \mathbb{Z}_2^l ;
- \otimes – операція скалярного добутку двох векторів над скінченним полем;
- $T_{l,k}^{(K)}, U_{l,k}^{(K)}$ – базові перетворення зашифрування і розшифрування (параметризовані ключем K відображення $V_l \rightarrow V_l$, $l, k \in \{128, 256, 512\}$ при цьому $k = l$ або $k = 2 \cdot l$);
- $v \ggg i$ – операція циклічного зсуву вправо бітової послідовності фіксованої довжини (символи з молодших позицій займають місце старших);
- $v \lll i$ – операція циклічного зсуву вліво бітової послідовності фіксованої довжини (символи із старших позицій займають місце молодших);
- $V_1 \parallel V_2$ – конкатенація (об'єднання) двох бітових послідовностей V_1 і V_2 таким чином, 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 ;
- $\Xi \circ \Lambda$ – композиція двох операцій Ξ і Λ , при цьому операція Λ виконується першою;
- $\prod_{i=1}^t \Lambda^{(i)}$ – послідовне виконання t операцій $\Lambda^{(1)}, \Lambda^{(2)}, \dots, \Lambda^{(t)}$, операція $\Lambda^{(1)}$ виконується першою;

V_k	– k -мірний векторний простір, який заданий над полем $GF(2)$, $k \in Z^+$;
$\mathfrak{Z}_{l,k}^{(K)}$	– криптографічний алгоритм симетричного блокового перетворення у режимі забезпечення конфіденційності;
$\phi_{l,k}^{(K)}$	– криптографічний алгоритм симетричного блокового перетворення у режимі забезпечення цілісності;
0^r	– бітова послідовність довжиною r елементів, кожен з яких дорівнює 0.
$\mu_l^{(j)}$	– подання цілого j як бітової послідовності довжиною l бітів (формат little endian)
$0x$	– 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 ;
$GF(2^8)$	– розширення степеня 8 поля $GF(2)$;
$f(x)$	– многочлен над полем $GF(2)$;
$f_{128}(x)$	– $x^{128} + x^7 + x^2 + x + 1$;
$f_{256}(x)$	– $x^{256} + x^{10} + x^5 + x^2 + 1$;
$f_{512}(x)$	– $x^{512} + x^8 + x^5 + x^2 + 1$;
α_l^i	– l -бітова послідовність, що відповідає результату піднесення до степеня i примітивного елемента $\alpha = x$ поля $GF(2^l)$ (молодшим коефіцієнтам відповідають біти послідовності із молодшими індексами); поле задано незвідним многочленом $f_l(x)$ для $l \in \{128, 256, 512\}$.
$X \bullet_l Y$	– l -бітова послідовність, що відповідає результату множення двох елементів поля $GF(2^l)$, асоційованих з l -бітовими послідовностями X та Y (молодшим коефіцієнтам відповідають біти із молодшими індексами); поле задано незвідним многочленом $f_l(x)$ для $l \in \{128, 256, 512\}$.
S	– синхропосилка (вектор ініціалізації);
l	– розмір внутрішнього стану базового перетворення (у бітах), $l \in \{128, 256, 512\}$;
M	– повідомлення (або частина повідомлення), для якого (якої) буде забезпечена конфіденційність (або конфіденційність та цілісність у режимах GCM, CCM та KW);
m_i	– i -й блок повідомлення M ;
N	– довжина повідомлення M (у бітах) без доповнення;
n	– кількість блоків (або напівблоків для режиму KW) базового перетворення, достатніх для збереження повідомлення M , тобто n – найменше невід’ємне ціле, таке що $N \leq n \cdot l$ (або $N \leq \frac{n \cdot l}{2}$ для режиму захисту ключових даних);
O	– повідомлення (або його частина), для якого (якої) буде забезпечена тільки цілісність і не буде забезпечена конфіденційність;
o_i	– i -й блок повідомлення O ;

N_o	– довжина повідомлення O (у бітах) без доповнення;
n_o	– кількість блоків базового перетворення, достатніх для збереження повідомлення O (n_o – найменше невід’ємне ціле, таке що $N \leq n_o \cdot l$)
t	– кількість ітерацій у перетвореннях $T_{l,k}^{(K)}$ і $U_{l,k}^{(K)}$;
q	– параметр режиму роботи алгоритму симетричного блокового перетворення (залежить від режиму);
Z^+	– множина додатних цілих чисел;
Калина- l/k	– застосування базового перетворення $T_{l,k}^{(K)}$ або $U_{l,k}^{(K)}$ з блоком розміром l бітів та ключем довжиною k бітів.

5 ЗАГАЛЬНІ ПОЛОЖЕННЯ

5.1 Призначення

Під алгоритмом симетричного блокового перетворення $\mathfrak{S}_{l,k}^{(K)}$ у режимі шифрування розуміється пряме і обернене відображення відкритого тексту $M \in V_N$ у шифртекст $C \in V_N$ (і навпаки), що залежить від ключа шифрування $K \in V_k$ і (для деяких режимів) синхропосилки $S \in V_l$: $\mathfrak{S}_{l,k}^{(K)} : V_N \times V_k \rightarrow V_N$ або $\mathfrak{S}_{l,k}^{(K)} : V_l \times V_N \times V_k \rightarrow V_N$. Параметри l і k визначають розмір блоку та довжину ключа базового блокового алгоритму.

Під алгоритмом симетричного блокового перетворення $\phi_{l,k}^{(K)}$ у режимі забезпечення цілісності (вироблення імітовставки) розуміється відображення повідомлення $M \in V_N$ в імітовставку (код автентифікації повідомлення), що залежить від ключа автентифікації $K \in V_k$ і (для деяких режимів) синхропосилки $S \in V_l$: $\phi_{l,k}^{(K)}(S, M) \in V_q$, $64 \leq q \leq l$ таке що $\phi_{l,k}^{(K)} : V_l \times V_N \times V_k \rightarrow V_q$.

Криптографічний алгоритм, визначений у цьому стандарті, передбачає можливість одночасного забезпечення конфіденційності та цілісності повідомлення шляхом послідовного застосування відповідних перетворень.

5.2 Режим роботи

Криптографічний алгоритм симетричного блокового перетворення використовує базове перетворення як основний елемент при забезпеченні конфіденційності та (або) цілісності.

Режими роботи криптографічного алгоритму, визначеного в цьому стандарті, їх позначення та послуги безпеки, які забезпечує відповідний режим, визначені у таблиці 5.1. Додаткові параметри використання кожного режиму наведені при його описі.

Таблиця 5.1

№ режиму	Назва режиму	Позначення	Послуга безпеки
1	Проста заміна (базове перетворення)	ECB	Конфіденційність
2	Гамування	CTR	Конфіденційність
3	Гамування зі зворотнім зв'язком за шифртекстом	CFB	Конфіденційність
4	Вироблення імітовставки	CMAC	Цілісність
5	Зчеплення шифрблоків	CBC	Конфіденційність
6	Гамування зі зворотнім зв'язком за шифргамою	OFB	Конфіденційність
7	Вибіркове гамування із прискореним виробленням імітовставки	GCM, GMAC	конфіденційність і цілісність (GCM), тільки цілісність (GMAC)
8	Вироблення імітовставки і гамування	CCM	цілісність і конфіденційність
9	Індексованої заміни	XTS	конфіденційність
10	Захисту ключових даних	KW	конфіденційність і цілісність

Режим роботи криптографічного алгоритму, визначеного у цьому стандарті, позначається наступним чином: „Калина- l/k -позначення режиму-параметри режиму” (для деяких режимів параметри відсутні), де l – розмір блоку базового перетворення, k – довжина ключа.

Наприклад, Калина-256/512-CCM-32,128 визначає використання базового перетворення з розміром блоку 256 бітів, довжиною ключа 512 бітів, застосування у режимі вироблення імітовставки і гамування, довжина конфіденційної (та відкритої) частини повідомлення завжди менша 2^{32} байтів, довжина імітовставки дорівнює 128 бітам.

Режим простої заміни збігається з базовим перетворенням, тому крім позначення «Калина- l/k -ECB» може використовуватись позначення «Калина- l/k ».

6 ПРОСТА ЗАМІНА (БАЗОВЕ ПЕРЕТВОРЕННЯ)

6.1 Загальні параметри

Режим простої заміни є компонентом усіх інших режимів роботи криптографічного алгоритму симетричного блокового перетворення.

Без додаткових перетворень, визначених іншими режимами, використання простої заміни для захисту повідомлень не рекомендується.

Базове перетворення реалізує пряме перетворення (зашифрування) та обернене перетворення (розшифрування).

Базове перетворення зашифрування $T_{l,k}^{(K)}$ є параметризованим ключем шифрування K відображенням $T_{l,k}^{(K)}: V_l \rightarrow V_l$, $K \in V_k$, $l, k \in \{128, 256, 512\}$ при цьому $k = l$ або $k = 2 \cdot l$, що реалізоване у вигляді ітеративного застосування низки функцій, які обробляють вхідний аргумент $x \in V_l$ як матрицю внутрішнього стану розміром $8 \times c$ байтів, що містить елементи поля $GF(2^8)$.

Базове перетворення розшифрування $U_{l,k}^{(K)}$ є параметризованим ключем шифрування K відображенням, оберненим до $T_{l,k}^{(K)}$, також реалізованим у вигляді ітеративного перетворення.

Залежність кількості ітерацій (t) при реалізації перетворень $T_{l,k}^{(K)}$ та $U_{l,k}^{(K)}$, кількості стовпців матриці внутрішнього стану (c) від розміру блоку (l) і довжини ключа шифрування (k) наведено у таблиці 6.1

Таблиця 6.1

№ з/п	Розмір блоку (l)	Довжина ключа (k)	Кількість ітерацій перетворення (t)	Кількість стовпців в матриці (c)
1	128	128	10	2
2		256	14	
3	256	256	14	4
4		512	18	
5	512	512	18	8

6.2 Подання вхідних та вихідних даних, внутрішнього стану перетворення

Базове перетворення виконує обробку вхідного блоку даних довжиною l бітів (відкритий текст при зашифруванні або шифртекст при розшифруванні).

Матриця внутрішнього стану позначається як $G = (g_{i,j})$, $g_{i,j} \in GF(2^8)$, де $i = \overline{0,7}$, $j = \overline{0, c-1}$. Запис байтів $B_1, B_2, \dots, B_{l/8}$ для перетворень $T_{l,k}^{(K)}$ та $U_{l,k}^{(K)}$ до матриці і зчитування з неї здійснюється по стовпцях. Приклад запису байтів до внутрішнього стану для $l = 512$ ($k = 512$, $c = 8$) див. на рис. 1.

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 базового перетворення							
$g_{0,0}$	$g_{0,1}$	$g_{0,2}$	$g_{0,3}$	$g_{0,4}$	$g_{0,5}$	$g_{0,6}$	$g_{0,7}$
$g_{1,0}$	$g_{1,1}$	$g_{1,2}$	$g_{1,3}$	$g_{1,4}$	$g_{1,5}$	$g_{1,6}$	$g_{1,7}$
$g_{2,0}$	$g_{2,1}$	$g_{2,2}$	$g_{2,3}$	$g_{2,4}$	$g_{2,5}$	$g_{2,6}$	$g_{2,7}$
$g_{3,0}$	$g_{3,1}$	$g_{3,2}$	$g_{3,3}$	$g_{3,4}$	$g_{3,5}$	$g_{3,6}$	$g_{3,7}$
$g_{4,0}$	$g_{4,1}$	$g_{4,2}$	$g_{4,3}$	$g_{4,4}$	$g_{4,5}$	$g_{4,6}$	$g_{4,7}$
$g_{5,0}$	$g_{5,1}$	$g_{5,2}$	$g_{5,3}$	$g_{5,4}$	$g_{5,5}$	$g_{5,6}$	$g_{5,7}$
$g_{6,0}$	$g_{6,1}$	$g_{6,2}$	$g_{6,3}$	$g_{6,4}$	$g_{6,5}$	$g_{6,6}$	$g_{6,7}$
$g_{7,0}$	$g_{7,1}$	$g_{7,2}$	$g_{7,3}$	$g_{7,4}$	$g_{7,5}$	$g_{7,6}$	$g_{7,7}$

Рисунок 1. Заповнення внутрішнього стану

6.3 Зашифрування

6.3.1 Структура перетворення

Базове перетворення зашифрування $T_{l,k}^{(K)}$ визначено наступним чином:

$$T_{l,k}^{(K)} = \eta_l^{(K_t)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \left(\prod_{v=1}^{t-1} (\kappa_l^{(K_v)} \circ \psi_l \circ \tau_l \circ \pi'_l) \right) \circ \eta_l^{(K_0)},$$

де l – розмір внутрішнього стану блокового шифру (у бітах),

K – ключ шифрування,

k – довжина ключа шифрування (у бітах),

$\eta_l^{(K_v)}$ – функція додавання циклового ключа K_v ($v \in \{0, t\}$) за модулем 2^{64} ,

π'_l – шар нелінійного бієктивного відображення, який виконує обробку векторів, заданих над V_8 (байтова підстановка);

τ_l – перестановка елементів $g_{i,j} \in GF(2^8)$ внутрішнього стану (циклічний зсув рядків вправо при матричному поданні);

ψ_l – лінійне перетворення (множення матриці лінійного перетворення на матрицю внутрішнього стану над скінченним полем);

$\kappa_l^{(K_v)}$ – функція додавання циклового ключа K_v ($v \in \{1, 2, \dots, t-1\}$) за модулем 2 (інволютивне перетворення).

В функціях π'_l , τ_l і ψ_l вхідний аргумент $x \in V_l$ та вихідне значення $\chi(x) \in V_l$, $\chi \in \{\pi'_l, \tau_l, \psi_l\}$ розглядаються як матриці розміром $8 \times c$ байтів (див. табл. 6.1).

Функції $\eta_l^{(K_v)}$ і $\kappa_l^{(K_v)}$ залежать від параметра $K_v \in V_l$ (циклового ключа v -ї ітерації), мають вхідний аргумент $x \in V_l$ (внутрішній стан шифру), та вихідне значення $\chi(x, K_v) \in V_l$, $\chi \in \{\eta_l^{(K_v)}, \kappa_l^{(K_v)}\}$, при цьому вхідні аргументи та вихідне значення розглядаються як матриці розміром $8 \times c$ байтів.

6.3.2 Функція додавання циклового ключа K_v за модулем 2^{64}

$\eta_l^{(K_v)}$ здійснює додавання за модулем 2^{64} стовпців матриці внутрішнього стану $G = (g_{i,j})$ і стовпців матриці циклового ключа $K_v = (k_{i,j}^v)$, при цьому результат також є матрицею розміром $8 \times c$ байтів (внутрішнім станом після додавання).

При виконанні додавання менші значущі байти мають менші індекси, тобто використовується формат little endian.

6.3.3 Шар нелінійного бієктивного відображення

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

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

Для здійснення перетворення може використовуватися інший набір підстановок, відмінний від наведеного у додатку А. У цьому випадку набір підстановок має постачатися і застосовуватися в установленому порядку.

6.3.4 Перестановка елементів

Функція τ_l виконує циклічний зсув вправо рядків матриці стану $G = (g_{i,j})$. Кількість елементів зсуву залежить від номеру рядку $i \in \{0,1,\dots,7\}$, розміру блоку $l \in \{128,256,512\}$, та обчислюється за формулою $\delta_i = \left\lfloor \frac{i \cdot l}{512} \right\rfloor$.

Наприклад, 5-й рядок матриці стану шифра з 256-бітовим блоком зсувається вправо на 2 елемента.

6.3.5 Лінійне перетворення

При обчисленні результату функції ψ_l кожен елемент $g_{i,j}$ матриці внутрішнього стану $G = (g_{i,j})$ розглядається як елемент скінченного поля $GF(2^8)$, що утворене незвідним поліномом $\nu(x) = x^8 + x^4 + x^3 + x^2 + 1$, або $0x11d$ у шістнадцятковому поданні.

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

$$w_{i,j} = (v \ggg i) \otimes G_j,$$

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

G_j – j -й стовпець матриці стану $G = (g_{i,j})$.

6.3.6 Функція додавання циклового ключа K_v за модулем 2

Функція $\kappa_l^{(K_v)}$ має вхідний аргумент $x \in V_l$ (внутрішній стан шифру) і залежить від параметра $K_v \in V_l$ (циклового ключа v -ї ітерації), кожен з яких поданий як матриця розміром $8 \times c$ байтів.

$\kappa_l^{(K_v)}$ здійснює побітове додавання (за модулем 2) стовпців матриці внутрішнього стану $G = (g_{i,j})$ і стовпців матриці циклового ключа $K_v = (k_{i,j}^v)$, при цьому результат також є матрицею розміром $8 \times c$ байтів (внутрішнім станом після додавання).

6.4 Розшифрування

6.4.1 Структура перетворення

Базове перетворення розшифрування $U_{l,k}^{(K)}$ визначено наступним чином:

$$U_{l,k}^{(K)} = {}_{-1}\eta_l^{(K_0)} \circ \left(\prod_{v=t-1}^1 ({}_{-1}\pi'_l \circ {}_{-1}\tau_l \circ {}_{-1}\psi_l \circ \kappa_l^{(K_v)}) \right) \circ {}_{-1}\pi'_l \circ {}_{-1}\tau_l \circ {}_{-1}\psi_l \circ {}_{-1}\eta_l^{(K_t)},$$

де l – розмір внутрішнього стану блокового шифру (у бітах),

K – ключ шифрування,

k – довжина ключа шифрування (у бітах),

${}_{-1}\eta_l^{(K_v)}$ – функція віднімання циклового ключа K_v ($v \in \{0, t\}$) за модулем 2^{64} (обернена до $\eta_l^{(K_v)}$);

${}_{-1}\psi_l$ – обернене лінійне перетворення (множення матриці оберненого лінійного перетворення на матрицю внутрішнього стану над скінченним полем);

${}_{-1}\tau_l$ – обернена перестановка елементів $g_{i,j} \in GF(2^8)$ внутрішнього стану (циклічний зсув рядків вліво при матричному поданні);

${}_{-1}\pi'_l$ – шар оберненого нелінійного бієктивного відображення, який виконує обробку векторів, заданих над V_8 (обернена байтова підстановка);

$\kappa_l^{(K_v)}$ – інволютивна функція додавання циклового ключа K_v ($v \in \{1, 2, \dots, t-1\}$) за модулем 2 (однакова для зашифрування і розшифрування).

Як і при зашифруванні, в функціях ${}_{-1}\pi'_l$, ${}_{-1}\tau_l$ і ${}_{-1}\psi_l$ вхідний аргумент $x \in V_l$ та вихідне значення $\chi(x) \in V_l$, $\chi \in \{{}_{-1}\pi'_l, {}_{-1}\tau_l, {}_{-1}\psi_l\}$ розглядаються як матриці розміром $8 \times c$ байтів.

Функція ${}_{-1}\eta_l^{(K_v)}$ має два вхідних аргументи $x \in V_l$ (внутрішній стан шифру) і $K_v \in V_l$ (цикловий ключ v -ї ітерації) та вихідне значення ${}_{-1}\eta_l^{(K_v)}(x, K_v) \in V_l$, при цьому вхідні аргументи та вихідне значення розглядаються як матриці розміром $8 \times c$ байтів.

6.4.2 Функція віднімання циклового ключа K_v за модулем 2^{64}

${}_{-1}\eta_l^{(K_v)}$ є оберненою до $\eta_l^{(K_v)}$ і здійснює віднімання за модулем 2^{64} стовпців матриці

циклового ключа $K_v = (k_{i,j}^v)$ від стовпців матриці внутрішнього стану $G = (g_{i,j})$, при цьому результат також є матрицею розміром $8 \times c$ байтів (внутрішнім станом після віднімання).

При виконанні віднімання найменш значущі байти мають менший індекс, тобто використовується формат little endian.

6.4.3 Шар оберненого нелінійного бісктивного відображення

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

Наприклад, нехай $g_{0,0} = 0xA3$, тоді ${}_{-1}\pi_0(0xA3) = 0x22$.

У разі використання підстановок, відмінних від наведених у додатку А, застосовуються відповідні їм обернені.

6.4.4 Обернена перестановка елементів

Функція ${}_{-1}\tau_l$ виконує циклічний зсув вліво рядків матриці стану $G = (g_{i,j})$. Кількість елементів зсуву залежить від номеру рядку $i \in \{0,1,\dots,7\}$ розміру блоку $l \in \{128,256,512\}$, та обчислюється за формулою $\delta_i = \left\lfloor \frac{i \cdot l}{512} \right\rfloor$.

Наприклад, 4-й рядок матриці стану шифру з 128-бітовим блоком зсувається вліво на 1 елемент.

6.4.5 Обернене лінійне перетворення

При обчисленні результату функції ${}_{-1}\psi_l$ кожен елемент $g_{i,j}$ матриці внутрішнього стану $G = (g_{i,j})$ розглядається 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 ${}_{-1}W = ({}_{-1}w_{i,j})$ отримується як результат множення векторів довжини 8 над скінченним полем $GF(2^8)$ за формулою

$${}_{-1}w_{i,j} = ({}_{-1}v \ggg i) \otimes G_j,$$

де ${}_{-1}v = (0xAD, 0x95, 0x76, 0xA8, 0x2F, 0x49, 0xD7, 0xCA)$ – вектор, що утворює циркулянтну матрицю МДР-коду і складається з послідовності байтових констант у шістнадцятковому поданні, які інтерпретуються як елементи поля $GF(2^8)$, при цьому циклічний зсув виконується відносно елементів вектора над скінченним полем;

G_j – j -й стовпець матриці стану $G = (g_{i,j})$.

6.5 Формування циклових ключів

6.5.1 Допоміжний ключ K_σ

Допоміжний ключ K_σ має розмір внутрішнього стану шифру (l бітів), подається як матриця розміром $8 \times c$ байтів (див. табл. 6.1) і формується на основі ключа шифрування K за допомогою перетворення $\Theta^{(K)}$:

$$\Theta^{(K)} = \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(K_\alpha)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \kappa_l^{(K_\omega)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(K_\alpha)},$$

де $\eta_l^{(\cdot)}, \pi'_l, \tau_l, \psi_l, \kappa_l^{(\cdot)}$ – перетворення, описані у пп.6.3.2-6.3.6.

Коли довжина ключа і розмір блоку базового перетворення співпадають ($k = l$), $K_\alpha = K_\omega = K$ (другим аргументом функцій $\eta_l^{(\cdot)}$ і $\kappa_l^{(\cdot)}$ є ключ шифрування).

Якщо довжина ключа і розмір блоку базового перетворення не співпадають ($k = 2 \cdot l$), то $K_\alpha \parallel K_\omega = K$, тобто $K_\alpha = L_{l,l/2}(K)$ і $K_\omega = R_{l,l/2}(K)$.

Для обчислення значення допоміжного ключа K_σ на вхід перетворення $\Theta^{(K)}$ подається l -бітове значення $\left(\frac{l+k}{64} + 1\right)$, представлене у форматі little endian.

6.5.2 Циклові ключі з парними індексами

Кожен з циклових ключів K_0, K_1, \dots, K_t має розмір внутрішнього стану шифру (l бітів), подається як матриця розміром $8 \times c$ байтів і формується на основі ключа шифрування K , допоміжного ключа K_σ та власного індексу i .

Циклові ключі K_i з парними індексами ($i \in \{0, 2, \dots, t\}$) формуються за допомогою перетворення $\Xi^{(K, K_\sigma, i)}$:

$$\Xi^{(K, K_\sigma, i)} = \eta_l^{(\varphi_i(K_\sigma))} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \kappa_l^{(\varphi_i(K_\sigma))} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(\varphi_i(K_\sigma))},$$

де $\eta_l^{(\cdot)}, \pi'_l, \tau_l, \psi_l, \kappa_l^{(\cdot)}$ – перетворення, описані у пп.6.3.2-6.3.6,

$\varphi_i(K_\sigma)$ – параметризоване індексом парного циклового ключа (i) перетворення допоміжного ключа K_σ (аргументу перетворення), що визначене як $\varphi_i = \eta_l^{(\vartheta \ll (i/2))}$ для значення $\vartheta = \mu_l^{(0x00010001 \dots 0001)}$, яке має довжину внутрішнього стану шифру; тобто, перетворення $\varphi_i(K_\sigma)$ повертає внутрішній стан, до якого занесено K_σ із доданими за модулем 2^{64} константами, зсунутими відповідно до індексу циклового ключа.

Коли довжина ключа і розмір блоку базового перетворення співпадають ($k = l$), для формування циклового ключа K_i на вхід перетворення $\Xi^{(K, K_\sigma, i)}$ подається значення $(K \gg \gg 32 \cdot i)$, де K – ключ шифрування.

Якщо довжина ключа і розмір блоку базового перетворення не співпадають ($k = 2 \cdot l$), то для формування циклового ключа K_i на вхід перетворення $\Xi^{(K, K_\sigma, i)}$ подається значення:

$L_{k,l}(K \gg \gg 16 \cdot i)$ для формування циклових ключів K_i з індексами, кратними 4 ($i = 0, 4, 8, \dots$);

$R_{k,l} \left(K \ggg 64 \cdot \left\lfloor \frac{i}{4} \right\rfloor \right)$ для формування циклових ключів K_i з індексами, не кратними 4 ($i = 2, 6, \dots$),
де K – ключ шифрування.

6.5.3 Циклові ключі з непарними індексами

Кожен з циклових ключів з непарними індексами обчислюється із попереднього ключа з парним індексом відповідно до співвідношення: $K_i = \left(K_{i-1} \lll \left(\frac{3 \cdot l}{4} - 24 \right) \right)$, де l – розмір внутрішнього стану блокового шифру (у бітах), $i \in \{1, 3, \dots, t-1\}$.

7 ГАМУВАННЯ

7.1 Загальні параметри

Режим забезпечує конфіденційність повідомлення шляхом шифрування.

Шифрування виконує пряме відображення повідомлення M ($|M| \geq 1$) у шифртекст C , $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M .

Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються.

Параметрами режиму є ключ шифрування K , $|K| = k$ та синхропосилка S , $|S| = l$.

Додаткові вимоги щодо синхропосилки не накладаються.

Режим гамування позначається як Калина- l/k -CTR.

7.2 Зашифрування

Повідомлення M ($|M| \geq 1$) подається у вигляді послідовності блоків: $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$, $|m_i| = l$ для $i = 1, 2, \dots, n-1$, $1 \leq |m_n| \leq l$.

Початкове значення лічильника s_0 ($|s_0| = l$) обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків шифртекста обчислюється відповідно до співвідношення $c_i = m_i \oplus L_{l,|m_i|} \left(T_{l,k}^{(K)} \left(L_{l,l/2}(s_0 + i) \parallel R_{l,l/2}(s_0) \right) \right)$ для $i = 1, 2, \dots, n$, $|c_i| = |m_i|$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$.

7.3 Розшифрування

Шифртекст C ($|C| \geq 1$) подається у вигляді послідовності блоків: $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$, $|c_i| = l$ для $i = 1, 2, \dots, n-1$, $1 \leq |c_n| \leq l$.

Початкове значення лічильника s_0 обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків повідомлення обчислюється відповідно до співвідношення

$$m_i = c_i \oplus L_{l,|c_i|} \left(T_{l,k}^{(K)} \left(L_{l,l/2} (s_0 + i) \parallel R_{l,l/2} (s_0) \right) \right) \text{ для } i = 1, 2, \dots, n.$$

Результатом розшифрування є повідомлення $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$.

8 ГАМУВАННЯ ЗІ ЗВОРОТНІМ ЗВ'ЯЗКОМ ЗА ШИФРТЕКСТОМ

8.1 Загальні параметри

Режим забезпечує конфіденційність повідомлення шляхом шифрування.

Шифрування виконує пряме відображення повідомлення M ($|M| \geq 1$) у шифртекст C , $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M .

Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються.

Параметрами режиму є ключ шифрування K , $|K| = k$, синхропосилка S , $|S| = l$ та додаткове значення q , яке визначає кількість бітів повідомлення, що обробляються за допомогою одного застосування базового перетворення, $q \in \{1, 8, 64, 128, 256, 512 \mid q \leq l\}$. Рекомендованим значенням параметра є $q = l$.

Додатковою вимогою до синхропосилки в цьому режимі є випадковість, в тому числі непередбачуваність значення, яке буде застосовано для будь-якого повідомлення, до його формування.

Режим гамування позначається як Калина- l/k -CFB- q .

8.2 Зашифрування

Повідомлення M ($|M| \geq 1$) подається у вигляді послідовності блоків: $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$, $|m_i| = q$ для $i = 1, 2, \dots, n-1$, $1 \leq |m_n| \leq q$.

Встановлюється значення $c_0^\# = T_{l,k}^{(K)}(S)$, $|c_0^\#| = l$.

Кожен з блоків шифртексту c_i ($|c_i| = q$) обчислюється відповідно до співвідношення $c_i = m_i \oplus R_{l,|m_i|}(c_{i-1}^\#)$ для $i = 1, 2, \dots, n$ та $c_i^\# = T_{l,k}^{(K)}(L_{l,l-q}(c_{i-1}^\#) \parallel c_i)$ для $i = 1, 2, \dots, n-1$, $|c_i^\#| = l$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$.

8.3 Розшифрування

Шифртекст C ($|C| \geq 1$) подається у вигляді послідовності блоків: $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$, $|c_i| = q$ для $i = 1, 2, \dots, n-1$, $1 \leq |c_n| \leq q$.

Встановлюється значення $c_0^\# = T_{l,k}^{(K)}(S)$.

Кожен з блоків повідомлення обчислюється відповідно до співвідношення $m_i = c_i \oplus R_{l,|c_i|}(c_{i-1}^\#)$ для $i = 1, 2, \dots, n$ та $c_i^\# = T_{l,k}^{(K)}(L_{l,l-q}(c_{i-1}^\#) \parallel c_i)$ для $i = 1, 2, \dots, n-1$.

Результатом розшифрування шифртексту є повідомлення $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$.

9 ВИРОБЛЕННЯ ІМІТОВСТАВКИ

9.1 Загальні параметри

Режим забезпечує цілісність повідомлення шляхом обчислення та перевірки імітовставки.

Якщо довжина повідомлення не є кратною розміру блоку базового перетворення, то застосовується алгоритм, наведений у додатку Б.

Режим виконує відображення повідомлення O ($|O|=l \cdot n_o$, де n_o – додатне ціле) в імітовставку h , $|h| \in \{64, 128, 256, 384, 512\}$ при $|h| \leq l$, а при перевірці цілісності додатково виконується порівняння обчисленої імітовставки із тією, що була отримана разом із повідомленням.

Синхропосилка в цьому режимі не використовується.

Параметрами режиму є ключ автентифікації K , $|K|=k$ та q – довжина імітовставки, $64 \leq q \leq l$. Рекомендоване значення є $q = l$.

Режим вироблення імітовставки позначається як Калина- l/k -СМАС- q .

9.2 Обчислення

Повідомлення O ($|O|=l \cdot n_o$, де n_o – додатне ціле) подається у вигляді послідовності блоків: $O = o_1 \parallel o_2 \parallel \dots \parallel o_{n_o}$, $|o_i|=l$ для $i = 1, 2, \dots, n_o$.

Встановлюється значення $c_0 = 0^l$.

Якщо повідомлення було доповнене (був застосований алгоритм, наведений у додатку Б), то встановлюється $K_\delta = T_{l,k}^{(K)}(0x00..01)$, де $0x00..01$ – l -бітове подання 1 у форматі little endian; у іншому випадку $K_\delta = T_{l,k}^{(K)}(0^l)$.

Для $i = 1, 2, \dots, n_o - 1$ обчислюються $c_i = T_{l,k}^{(K)}(c_{i-1} \oplus o_i)$. Для $i = n_o$ задається $c_i = T_{l,k}^{(K)}(c_{i-1} \oplus o_i \oplus K_\delta)$.

Результатом обчислення є імітовставка $h = L_{l,q}(c_{n_o})$.

9.3 Перевірка

Для повідомлення M застосовується алгоритм обчислення імітовставки, визначений п.9.2.

У разі, якщо обчислена імітовставка не співпадає із тою, що була отримана разом із повідомленням, цілісність повідомлення є порушеною. У іншому випадку цілісність повідомлення підтверджена.

10 ЗЧЕПЛЕННЯ ШИФРБЛОКІВ

10.1 Загальні параметри

Режим забезпечує конфіденційність повідомлення шляхом шифрування.

Якщо довжина повідомлення не є кратною розміру блоку базового перетворення, то

застосовується алгоритм, наведений у додатку Б.

Шифрування виконує пряме відображення повідомлення M ($|M| = l \cdot n$, де n – додатне ціле) у шифртекст C , $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M .

Параметрами режиму є ключ шифрування K , $|K| = k$, синхропосилка S , $|S| = l$.

Додатковою вимогою до синхропосилки в цьому режимі є випадковість (непередбачуваність значення, яке буде застосовано для будь-якого повідомлення).

Режим зчеплення шифр блоків позначається як Калина- l/k -СВС.

10.2 Зашифрування

Повідомлення M подається у вигляді послідовності блоків: $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$, $|m_i| = l$ для $i = 1, 2, \dots, n$.

Встановлюється значення $c_0 = S$.

Для $i = 1, 2, \dots, n$ обчислюються $c_i = T_{l,k}^{(K)}(c_{i-1} \oplus m_i)$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$.

10.3 Розшифрування

Шифртекст C ($|C| = l \cdot n$, де n – додатне ціле) подається у вигляді послідовності блоків: $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$, $|c_i| = l$ для $i = 1, 2, \dots, n$.

Встановлюється значення $c_0 = S$.

Для $i = 1, 2, \dots, n$ обчислюються $m_i = c_{i-1} \oplus U_{l,k}^{(K)}(c_i)$.

Результатом розшифрування шифртексту є повідомлення $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$.

11 ГАМУВАННЯ ЗІ ЗВОРОТНІМ ЗВ'ЯЗКОМ ЗА ШИФРГАМОЮ

11.1 Загальні параметри

Режим забезпечує конфіденційність повідомлення шляхом шифрування.

Шифрування виконує пряме відображення повідомлення M ($|M| \geq 1$) у шифртекст C , $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M .

Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються.

Параметрами режиму є ключ шифрування K , $|K| = k$ та синхропосилка S , $|S| = l$.

Додаткові вимоги щодо синхропосилки не накладаються.

Режим гамування позначається як Калина- l/k -OFB.

11.2 Зашифрування

Повідомлення M ($|M| \geq 1$) подається у вигляді послідовності блоків: $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$, $|m_i| = l$ для $i = 1, 2, \dots, n-1$, $1 \leq |m_n| \leq l$.

Початкове значення блока гами γ_0 ($|\gamma_0| = l$) обчислюється як $\gamma_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків шифртекста обчислюється відповідно до співвідношення $c_i = m_i \oplus L_{l,|m_i|}(\gamma_{i-1})$ для $i = 1, 2, \dots, n$, та $\gamma_i = T_{l,k}^{(K)}(\gamma_{i-1})$ для $i = 1, 2, \dots, n-1$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$.

11.3 Розшифрування

Шифртекст C ($|C| \geq 1$) подається у вигляді послідовності блоків: $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$, $|c_i| = l$ для $i = 1, 2, \dots, n-1$, $1 \leq |c_n| \leq l$.

Початкове значення блока гами γ_0 ($|\gamma_0| = l$) обчислюється як $\gamma_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків повідомлення обчислюється відповідно до співвідношення $m_i = c_i \oplus L_{l,|m_i|}(\gamma_{i-1})$ для $i = 1, 2, \dots, n$, та $\gamma_i = T_{l,k}^{(K)}(\gamma_{i-1})$ для $i = 1, 2, \dots, n-1$.

Результатом розшифрування шифртекста є повідомлення $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$.

12 ВИБІРКОВЕ ГАМУВАННЯ ІЗ ПРИСКОРЕНИМ ВИРОБЛЕННЯМ ІМІТОВСТАВКИ

12.1 Загальні параметри

Режим забезпечує конфіденційність і цілісність повідомлення шляхом шифрування і обчислення та перевірки імітовставки.

Шифрування (гамування) є вибіркоким, тобто конфіденційність забезпечується для обраної частини повідомлення (довжина цієї частини обирається в залежності від вимог до засобу криптографічного захисту: від шифрування всього повідомлення до відсутності шифрування взагалі).

Повідомлення складається з двох частин: відкритої O (для якої буде забезпечена лише цілісність) та конфіденційної M (для якої буде забезпечена конфіденційність та цілісність), $|O| + |M| \geq 1$.

Режим забезпечує цілісність відкритої частини повідомлення O та шифртекста C (зашифрованої частини повідомлення M) шляхом обчислення та перевірки імітовставки.

Шифрування виконує пряме відображення повідомлення M ($|M| \geq 1$) у шифртекст C , $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M .

Крім того, виконується відображення криптограми (відкритої частини повідомлення O і шифртексту) в імітовставку h , $64 \leq |h| \leq l$, а при перевірці цілісності додатково виконується порівняння обчисленої імітовставки із тією, що була отримана разом із повідомленням.

Вимоги на кратність довжини повідомлення (відкритої або конфіденційної частини) розміру блоку базового перетворення не накладаються.

Параметрами режиму є ключ шифрування K , $|K|=k$, синхропосилка S , $|S|=l$ та q – довжина імітовставки, $64 \leq q \leq l$. Рекомендоване значення $q=l$.

Додаткові вимоги щодо синхропосилки не накладаються.

Режим вибіркового гамування із прискореним виробленням імітовставки для $|M| \geq 1$ позначається як Калина- l/k -GCM- q (забезпечується конфіденційність та цілісність), для $|M|=0$ режим позначається як Калина- l/k -GMAC- q (забезпечується тільки цілісність).

12.2 Вироблення імітовставки для відкритої частини повідомлення та шифртексту

Вироблення імітовставки є допоміжним алгоритмом, який використовується при прямому та оберненому криптографічному перетворенні для обробки відкритої частини повідомлення O та шифртексту C .

Якщо довжина шифртексту C не кратна розміру блоку базового перетворення ($|C| \neq n \cdot l$, $n \in \{0,1,2,\dots\}$), до нього застосовується алгоритм доповнення, визначений у п.Б.2 стандарту для отримання доповненого шифртексту: $C^* = c_1^* \parallel c_2^* \parallel \dots \parallel c_n^*$, де $|c_i^*|=l$ для $i=1,2,\dots,n$.

У іншому випадку (доповнення не потрібне) $C^* = C$.

Коли довжина відкритої частини повідомлення O не кратна розміру блоку базового перетворення ($|O| \neq n_o \cdot l$, $n_o \in \{0,1,2,\dots\}$), до неї застосовується алгоритм доповнення, визначений у п.Б.2 стандарту для отримання $O^* = o_1^* \parallel o_2^* \parallel \dots \parallel o_{n_o}^*$, де $|o_i^*|=l$ для $i=1,2,\dots,n_o$.

У іншому випадку (доповнення не потрібне) $O^* = O$.

Значення параметризованої змінної автентифікації H ($|H|=l$) обчислюється як $H = T_{l,k}^{(K)}(0^l)$.

Встановлюється значення $b_0 = 0^l$.

Обчислюються значення $b_i = (o_i^* \oplus b_{i-1}) \bullet_l H$ для $i=1,2,\dots,n_o$, $|b_i|=l$.

Встановлюється значення $b'_0 = b_{n_o}$, $|b'_i|=l$ для $i=1,2,\dots,n$.

Обчислюються значення $b'_i = (c_i^* \oplus b'_{i-1}) \bullet_l H$ для $i=1,2,\dots,n$.

Встановлюється $B = b'_n$.

Довжина відкритої та конфіденційної частини повідомлення (задана у бітах) подається у вигляді бітових послідовностей довжиною $l/2$ бітів кожна (формат little endian): $\lambda_o = |O|$,

$$\lambda_c = |C|, |\lambda_o| = |\lambda_c| = l/2.$$

Імітовставка h обчислюється як $h = L_{l,q}(T_{l,k}^{(K)}(B \oplus (\lambda_o \parallel \lambda_c)))$.

12.3 Зашифрування та забезпечення цілісності

Цей пункт визначає пряме перетворення Калина- l/k -GCM- q , коли присутня конфіденційна частина повідомлення M ($|M| \geq 1$).

M подається у вигляді послідовності блоків: $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$, $|m_i| = l$ для $i = 1, 2, \dots, n-1$, $1 \leq |m_n| \leq l$.

Початкове значення лічильника s_0 ($|s_0| = l$) обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків шифртекста обчислюється відповідно до співвідношення $c_i = m_i \oplus L_{l,|m_i|}(T_{l,k}^{(K)}(L_{l,l/2}(s_0 + i) \parallel R_{l,l/2}(s_0)))$ для $i = 1, 2, \dots, n$, $|c_i| = |m_i|$.

Результатом зашифрування конфіденційної частини повідомлення є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$.

Імітовставка h для відкритої частини повідомлення O і шифртексту C обчислюється відповідно до п.12.2.

Результатом роботи прямого перетворення режиму Калина- l/k -GCM- q є шифртекст C та імітовставка h .

12.4 Перевірка цілісності та розшифрування

Цей пункт визначає обернене перетворення Калина- l/k -GCM- q , коли у складі вхідних даних присутній шифртекст C ($|C| \geq 1$).

Імітовставка h для відкритої частини повідомлення O і шифртексту C обчислюється відповідно до п.12.2.

У разі, якщо обчислена імітовставка не співпадає із тою, що була отримана разом із вхідними даними, цілісність є порушеною. Обробка переривається та повертається повідомлення про порушення цілісності.

Якщо цілісність підтверджена, то виконується розшифрування конфіденційної частини повідомлення.

Шифртекст C ($|C| \geq 1$) подається у вигляді послідовності блоків: $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$, $|c_i| = l$ для $i = 1, 2, \dots, n-1$, $1 \leq |c_n| \leq l$.

Початкове значення лічильника s_0 обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків повідомлення обчислюється відповідно до співвідношення

$$m_i = c_i \oplus L_{l,|m_i|} \left(T_{l,k}^{(K)} \left(L_{l,l/2}(s_0 + i) \parallel R_{l,l/2}(s_0) \right) \right) \text{ для } i = 1, 2, \dots, n.$$

Результатом розшифрування шифртекста є повідомлення $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$.

Результатом роботи оберненого перетворення режиму Калина- l/k -GCM- q є $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$ або повідомлення про порушення цілісності.

12.5 Вироблення імітовставки для відкритого повідомлення

Цей пункт визначає перетворення Калина- l/k -GMAC- q , коли відсутня конфіденційна частина повідомлення M ($|M|=0$).

Якщо довжина відкритої частини повідомлення O не кратна розміру блоку базового перетворення ($|O| \neq n_o \cdot l$, $n_o \in \{1, 2, \dots\}$), до неї застосовується алгоритм доповнення, визначений у п.Б.2 стандарту для отримання $O^* = o_1^* \parallel o_2^* \parallel \dots \parallel o_n^*$, де $|o_i^*| = l$ для $i = 1, 2, \dots, n$.

У іншому випадку (доповнення не потрібне) $O^* = O$.

Значення параметризованої змінної автентифікації H ($|H|=l$) обчислюється як $H = T_{l,k}^{(K)}(0^l)$.

Встановлюється значення $b_0 = 0^l$.

Обчислюються значення $b_i = (o_i^* \oplus b_{i-1}) \bullet_l H$ для $i = 1, 2, \dots, n_o$, $|b_i| = l$.

Встановлюється $B = b_{n_o}$, $|B| = l$.

Довжина відкритої та конфіденційної частини повідомлення подається у вигляді бітових послідовностей довжиною $l/2$ бітів кожна (формат little endian): $\lambda_o = |O|$, $\lambda_M = 0^{l/2}$, $|\lambda_o| = |\lambda_M| = l/2$.

Імітовставка h обчислюється як $h = L_{l,q} \left(T_{l,k}^{(K)} (B \oplus (\lambda_o \parallel \lambda_M)) \right)$.

Результатом роботи режиму Калина- l/k -GMAC- q є імітовставка h .

12.6 Перевірка цілісності для відкритого повідомлення

Цей пункт визначає перетворення Калина- l/k -GMAC- q , коли відсутня конфіденційна частина повідомлення M ($|M|=0$), а для відкритої частини повідомлення вже обчислена імітовставка.

Для відкритої частини повідомлення O застосовується алгоритм обчислення імітовставки, визначений п.12.5.

У разі, якщо обчислена імітовставка не співпадає із тою, що була отримана разом із

повідомленням, цілісність повідомлення є порушеною. У іншому випадку цілісність повідомлення підтверджена.

13 ВИРОБЛЕННЯ ІМІТОВСТАВКИ І ГАМУВАННЯ

13.1 Загальні параметри

Режим забезпечує цілісність і конфіденційність повідомлення шляхом вироблення імітовставки та шифрування.

Шифрування (гамування) є вибіркоким, тобто конфіденційність може забезпечуватися лише для обраної частини повідомлення.

На вхід режиму для прямого перетворення подається повідомлення, що складається з двох частин: відкритої O (для якої буде забезпечена лише цілісність), та конфіденційної M (для якої буде забезпечена конфіденційність та цілісність), бітова довжина обох частин є кратною 8: $|O| = 8 \cdot r'$, $r' \in \{0, 1, 2, \dots\}$ і $|M| = 8 \cdot r$, $r \in \{1, 2, \dots\}$.

Режим забезпечує цілісність обох частин повідомлення (O та M) і конфіденційність M .

Для оберненого перетворення на вхід подається відкрита частина O повідомлення та шифртекст, що був сформований при виконанні прямого перетворення.

Параметрами режиму є ключ шифрування K , $|K| = k$, синхропосилка S , $|S| = l$, N_{\max} – найбільша можлива довжина відкритої або конфіденційної частини повідомлення (в бітах), яке повинно бути оброблене засобом криптографічного захисту, та q – довжина імітовставки, яке обирається як $q \in \{64, 128, 256, 384, 512 | q \leq l\}$. Рекомендоване значення $q = l$.

N_{\max} не може перевищувати значень, наведених у табл.Г.1. У якості N_{\max} рекомендується обирати найменше значення, яке задовольняє практичним потребам (наприклад, коли довжина повідомлення завжди менша 4 ГБ, тобто не перевищує $2^{32} - 1$ байтів, $N_{\max} = 2^{35} - 8$).

Мінімальна необхідна кількість байтів N_B для збереження довжини повідомлення у байтах (тобто $8 \cdot N_B$ бітів) обчислюється за формулою $N_B = \left\lceil \frac{1}{8} (-3 + \log_2 N_{\max}) + 1 \right\rceil$.

Для прикладу $N_{\max} = 2^{35} - 8$ обчислене $N_B = 4$.

Додатковою вимогою до синхропосилки в цьому режимі є унікальність значень $L_{l, l-8(N_B+1)}(S)$ для всіх повідомлень, що захищаються на одному ключі (унікальність всіх значень $\frac{l}{8} - (N_B + 1)$ молодших байтів синхропосилки S , які залишаються після її усічення для формування заголовку автентифікації, див. табл. 13.1).

Режим вироблення імітовставки і гамування позначається як Калина- l/k -ССМ- $(8 \cdot N_B)$, q (наприклад, Калина-256/512-ССМ-32,128 визначає режим ССМ з використанням базового

перетворення з розміром блоку 256 бітів, довжиною ключа 512 бітів, довжина конфіденційної частини повідомлення завжди менша 2^{32} байтів і довжина імітовставки дорівнює 128 бітам).

13.2 Вироблення імітовставки

Вироблення імітовставки є допоміжним алгоритмом, який використовується при прямому та оберненому криптографічному перетворенні для обробки відкритої частини повідомлення O та конфіденційної частини M .

Формується заголовок автентифікації G_1 , $|G_1| = l$, який складається із молодших байтів синхропосилки, до яких додане поле довжиною N_B байтів, що містить запис довжини конфіденційної частини повідомлення у форматі little endian, та байт прапорців таким чином, щоб загальний розмір заголовку дорівнював розміру блоку базового перетворення. Формат заголовку наведений у табл.13.1.

Таблиця 13.1

Довжина поля, байтів	$l/8 - (N_B + 1)$	N_B	l
Індекс байтів заголовку	$0 \dots l/8 - (N_B + 2)$	$l/8 - (N_B + 1) \dots l/8 - 2$	$l/8 - 1$
Зміст	$L_{l, l-8(N_B+1)}(S)$	$ M /8$	Байт прапорців

Зміст і формат байту прапорців наведений у табл.13.2.

Таблиця 13.2

Ваговий коефіцієнт біта	7	6	5	4	3	2	1	0
Зміст	$ O > 0$	код довжини імітовставки			$N_B - 1$			

Найстарший біт вказує наявність (1) чи відсутність (0) відкритої частини повідомлення O . Наступні три біта визначають довжину імітовставки відповідно до таблиці 13.3. Молодші чотири біти містять значення $N_B - 1$.

Таблиця 13.3

Код довжини імітовставки	Довжина імітовставки в байтах ($q/8$)
2	8
3	16
4	32
5	48
6	64

Якщо наявна відкрита частина повідомлення ($|O| > 0$), то довжина цієї частини подається у вигляді бітової послідовності довжиною $8 \cdot N_B$ бітів (формат little endian): $\lambda_o = |O|/8$, $|\lambda_o| = 8 \cdot N_B$.

Формується блок довжини відкритої частини повідомлення G_2 шляхом додавання $(l - (|O| \bmod l) - 8 \cdot N_B) \bmod l$ нульових бітів до довжини відкритої частини: $G_2 = (\lambda_o \parallel 0^{(l - (|O| \bmod l) - 8 \cdot N_B) \bmod l})$ таким чином, щоб довжина послідовності $(G_1 \parallel G_2 \parallel O)$ була кратною довжині блоку базового перетворення.

Послідовність $(G_1 \parallel G_2 \parallel O)$ подається у вигляді блоків $(G_1 \parallel G_2 \parallel O) = (g_1 \parallel g_2 \parallel g_3 \parallel \dots \parallel g_{n_g})$, де $n_g = \lceil (G_1 \parallel G_2 \parallel O) / l \rceil$.

Встановлюється значення $b_0 = 0^l$.

Для $i = 1, 2, \dots, n_g$ обчислюються $b_i = T_{l,k}^{(K)}(b_{i-1} \oplus g_i)$, $|b_i| = l$.

Встановлюється $B = b_{n_g}$, $|B| = l$.

Якщо відкрита частина повідомлення відсутня ($|O| = 0$), то встановлюється $B = G_1$, $|B| = l$.

У разі, коли довжина конфіденційної частини повідомлення M не є кратною розміру блоку базового перетворення, то застосовується алгоритм, наведений у додатку Б, для формування доповненої конфіденційної частини $M^* = m_1^* \parallel m_2^* \parallel \dots \parallel m_n^*$, де $|m_i^*| = l$ для $i = 1, 2, \dots, n$.

Встановлюється значення $b'_0 = B$, $|b'_0| = l$.

Для $i = 1, 2, \dots, n$ обчислюються $b'_i = T_{l,k}^{(K)}(b'_{i-1} \oplus m_i^*)$, $|b'_i| = l$.

Імітовставка h обчислюється як $h = L_{l,q}(b'_n)$.

13.3 Пряме перетворення

Для відкритої частини повідомлення O та конфіденційної частини повідомлення M обчислюється імітовставка h відповідно до п.13.2.

Повідомлення для зашифрування M'' складається з конфіденційної частини повідомлення (M) та імітовставки h : $M'' = M \parallel h$, $M'' = m_1'' \parallel m_2'' \parallel \dots \parallel m_{n_m}''$, $|m_i''| = l$ для $i = 1, 2, \dots, n_m - 1$, $1 \leq |m_{n_m}''| \leq l$.

Початкове значення лічильника s_0 ($|s_0| = l$) обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків шифртекста обчислюється відповідно до співвідношення

$$c_i = m_i'' \oplus L_{l, |m_i|} \left(T_{l, k}^{(K)} \left(L_{l, l/2} (s_0 + i) \parallel R_{l, l/2} (s_0) \right) \right) \text{ для } i = 1, 2, \dots, n_m, |c_i| = |m_i''|.$$

Результатом роботи режиму є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$.

13.4 Обернене перетворення

При розшифруванні шифртекст C ($|C| \geq 1$) подається у вигляді послідовності блоків: $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$, $|c_i| = l$ для $i = 1, 2, \dots, n-1$, $1 \leq |c_n| \leq l$.

Початкове значення лічильника s_0 обчислюється як $s_0 = T_{l, k}^{(K)}(S)$.

Кожен з блоків отриманої бітової послідовності обчислюється відповідно до співвідношення $m_i'' = c_i \oplus L_{l, |m_i|} \left(T_{l, k}^{(K)} \left(L_{l, l/2} (s_0 + i) \parallel R_{l, l/2} (s_0) \right) \right)$ для $i = 1, 2, \dots, n$.

Результатом розшифрування шифртекста є $M'' = m_1'' \parallel m_2'' \parallel \dots \parallel m_{n_m}''$, $|m_i''| = l$ для $i = 1, 2, \dots, n_m - 1$, $1 \leq |m_{n_m}''| \leq l$.

З M'' отримується імітовставка $h' = R_{|M'', q|} (M'')$ та конфіденційна частина повідомлення $M = L_{|M'', q|, |M''| - q} (M'')$.

Для відкритої частини повідомлення O та розшифрованої конфіденційної частини повідомлення M обчислюється імітовставка h відповідно до п.13.2.

У разі, якщо обчислена імітовставка не співпадає із тою, що була отримана разом із повідомленням ($h \neq h'$), обробка переривається та повертається повідомлення про порушення цілісності.

У іншому випадку цілісність повідомлення підтверджена, і результатом роботи режиму є конфіденційна частина повідомлення M .

14 ІНДЕКСОВАНА ЗАМІНА

14.1 Загальні параметри

Режим забезпечує конфіденційність повідомлення шляхом шифрування.

Це перетворення не забезпечує криптографічну послугу збереження цілісності повідомлення, але у випадку модифікації будь-якого блоку шифртексту відповідний блок відкритого тексту після розшифрування відповідно до п.14.3 буде мати псевдовипадкове значення (його зміст буде цілком зіпсований), а інші блоки залишаться непошкодженими. У разі застосування п.14.5 для розшифрування модифікація останніх l бітів шифртексту призводить до псевдовипадкових значень останніх двох блоків відкритого тексту.

Шифрування виконує пряме відображення повідомлення M ($|M| \geq l$) у шифртекст C , $|C| = |M|$, та обернене відображення шифртексту C в повідомлення M .

Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються.

Параметрами режиму є ключ шифрування K , $|K| = k$ та синхропосилка S , $|S| = l$.

Додаткові вимоги щодо синхропосилки не накладаються.

У разі, коли розмір повідомлення є кратним розміру блоку базового перетворення, виконується шифрування без доповнення (п.14.2 і 14.3). У іншому випадку застосовується модифікований алгоритм із доповненням (визначений у п.14.4 і 14.5).

Режим індексованої заміни позначається як Калина- l/k -XTS (без доповнення) або Калина- l/k -XTS-р (із доповненням).

14.2 Зашифрування без доповнення

Повідомлення M ($|M| = l \cdot r$, де r – додатне ціле) подається у вигляді послідовності блоків: $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$, $|m_i| = l$ для $i = 1, 2, \dots, n$.

Початкове значення лічильника s_0 ($|s_0| = l$) обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків шифртекста обчислюється відповідно до співвідношення $c_i = (T_{l,k}^{(K)}(m_i \oplus (\alpha_l^i \bullet_l s_0))) \oplus (\alpha_l^i \bullet_l s_0)$ для $i = 1, 2, \dots, n$, $|c_i| = |m_i|$, де α_l^i визначається відповідно до розділу 4 стандарту.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$.

14.3 Розшифрування без доповнення

Шифртекст C ($|C| = l \cdot r$, де r – додатне ціле) подається у вигляді послідовності блоків: $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$, $|c_i| = l$ для $i = 1, 2, \dots, n$.

Початкове значення лічильника s_0 обчислюється як $s_0 = T_{l,k}^{(K)}(S)$.

Кожен з блоків повідомлення обчислюється відповідно до співвідношення $m_i = (U_{l,k}^{(K)}(c_i \oplus (\alpha_l^i \bullet_l s_0))) \oplus (\alpha_l^i \bullet_l s_0)$ для $i = 1, 2, \dots, n$.

Результатом розшифрування є повідомлення $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$.

14.4 Зашифрування із доповненням

Повідомлення M ($|M| > l$) подається у вигляді послідовності блоків: $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$, $|m_i| = l$ для $i = 1, 2, \dots, n-1$, $1 \leq |m_n| < l$.

Блоки m_1, m_2, \dots, m_{n-1} обробляються відповідно до п.14.2 для отримання фрагменту шифртексту $C^* = c_1 \parallel c_2 \parallel \dots \parallel c_{n-2} \parallel c_{n-1}$.

Обчислюється $c_n = (T_{l,k}^{(K)}((m_n \parallel R_{l,l-|m_n|}(c_{n-1}))) \oplus (\alpha_l^n \bullet_l s_0)) \oplus (\alpha_l^n \bullet_l s_0)$, де $s_0 = T_{l,k}^{(K)}(S)$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_{n-2} \parallel c_n \parallel L_{l,|m_n|}(c_{n-1})$.

14.5 Розшифрування із доповненням

Шифртекст C ($|C| > l$) подається у вигляді послідовності блоків: $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$, $|c_i| = l$ для $i = 1, 2, \dots, n-1$, $1 \leq |c_n| < l$.

Блоки c_1, c_2, \dots, c_{n-2} обробляються відповідно до п.14.3 для отримання фрагменту відкритого тексту $M^* = m_1 \parallel m_2 \parallel \dots \parallel m_{n-2}$.

Обчислюються $m_n^* = (U_{l,k}^{(K)}(c_{n-1} \oplus (\alpha_l^n \bullet_l s_0))) \oplus (\alpha_l^n \bullet_l s_0)$ і $m_{n-1} = (U_{l,k}^{(K)}((c_n \parallel R_{l,l-|c_n|}(m_n^*)) \oplus (\alpha_l^{n-1} \bullet_l s_0))) \oplus (\alpha_l^{n-1} \bullet_l s_0)$, де $s_0 = T_{l,k}^{(K)}(S)$.

Результатом розшифрування є повідомлення $M = m_1 \parallel m_2 \parallel \dots \parallel m_{n-1} \parallel L_{l,|c_n|}(m_n^*)$.

15 ЗАХИСТ КЛЮЧОВИХ ДАНИХ

15.1 Загальні параметри

Режим забезпечує конфіденційність та цілісність повідомлення.

Шифрування виконує пряме відображення повідомлення M ($|M| \geq l$) у шифртекст C , $|M| < |C| < |M| + 2 \cdot l$, та обернене відображення шифртексту C в повідомлення M .

Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються.

Параметром режиму є ключ шифрування K , $|K| = k$

У разі, коли розмір повідомлення є кратним розміру блоку базового перетворення, виконується шифрування без доповнення (п.15.2 і 15.3). У іншому випадку застосовується алгоритм із доповненням (визначений у п.15.4 і 15.5).

Режим захисту ключових даних позначається як Калина- l/k -KW (без доповнення) або Калина- l/k -KW-p (із доповненням).

15.2 Зашифрування без доповнення

До повідомлення M ($|M| = l \cdot r$, де r – додатне ціле) додається 0^l для отримання M^* : $M^* = M \parallel 0^l$.

M^* подається у вигляді послідовності напівблоків: $M^* = m_1^* \parallel m_2^* \parallel \dots \parallel m_n^*$, $|m_i^*| = l/2$ для

$i = 1, 2, \dots, n$ та $n = 2 \cdot (r + 1)$.

Встановлюється $V = (n - 1) \cdot 6$ і $B^0 = m_1^*$, де $|B^j| = l/2$ для $j = 0, 1, \dots, V$.

Задається $b_i^0 = m_i^*$ для $i = 2, \dots, n$, де $|b_i^j| = l/2$ для $j = 0, 1, \dots, V$.

Для $j = 1, \dots, V$ обчислюється

$$B^j = R_{l,l/2}(T_{l,k}^{(K)}(B^{j-1} \parallel b_2^{j-1})) \oplus \mu_{l/2}^{(j)},$$

$$b_n^j = L_{l,l/2}(T_{l,k}^{(K)}(B^{j-1} \parallel b_2^{j-1})) \text{ та}$$

$$b_i^j = b_{i+1}^{j-1} \text{ для } i = 2, \dots, n-1.$$

Задається $c_1 = B^V$ і $c_i = b_i^V$ для $i = 2, \dots, n$.

Результатом є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$.

15.3 Розшифрування без доповнення

Шифртекст C ($|C| = l \cdot r$, де r – додатне ціле) подається у вигляді послідовності напівблоків: $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$, $|c_i| = l/2$ для $i = 1, 2, \dots, n$ та $n = 2 \cdot r$.

Встановлюється $V = (n - 1) \cdot 6$ і $B^V = c_1$, де $|B^j| = l/2$ для $j = 0, 1, \dots, V$.

Задається $b_i^V = c_i$ для $i = 2, \dots, n$, де $|b_i^j| = l/2$ для $j = 0, 1, \dots, V$.

Для $j = V, V - 1, \dots, 1$ обчислюється

$$B^{j-1} = L_{l,l/2}(U_{l,k}^{(K)}(b_n^j \parallel (B^j \oplus \mu_{l/2}^{(j)}))),$$

$$b_2^{j-1} = R_{l,l/2}(U_{l,k}^{(K)}(b_n^j \parallel (B^j \oplus \mu_{l/2}^{(j)}))) \text{ і}$$

$$b_{i+1}^{j-1} = b_i^j \text{ для } i = 2, \dots, n-1.$$

Задається $m_1^* = B^0$ і $m_i^* = b_i^0$ для $i = 2, \dots, n$.

Формується $M^* = m_1^* \parallel m_2^* \parallel \dots \parallel m_n^*$.

У разі, коли $R_{n,l/2,l}(M^*)$ не дорівнює 0^l , повертається повідомлення про порушення цілісності.

У іншому випадку повертається розшифроване повідомлення $M = L_{n,l/2,n,l/2-l}(M^*)$.

15.4 Зашифрування із доповненням

До повідомлення M ($|M| > l$) додається бітове подання довжини $\mu_{l/2}^{(|M|)}$, після чого до результату $(M \parallel \mu_{l/2}^{(|M|)})$ застосовується алгоритм доповнення, визначений у п.Б.2 стандарту для отримання доповненого повідомлення $M'' = m_1'' \parallel m_2'' \parallel \dots \parallel m_{n_m}''$, $|m_i''| = l$ для $i = 1, 2, \dots, n_m$.

Доповнене повідомлення M'' обробляється відповідно до п.15.2 для отримання

шифртексту $C = c_1 \parallel c_2 \parallel \dots \parallel c_{n_m}$, який є результатом роботи режиму.

15.5 Розшифрування із доповненням

Шифртекст C ($|C| = l \cdot r$, де r – додатне ціле) обробляються відповідно до п.15.3 для отримання доповненого повідомлення M'' .

Якщо результатом роботи є повідомлення про порушення цілісності, подальша обробка припиняється із повертанням повідомлення про порушення цілісності.

У іншому випадку до доповненого повідомлення M'' застосовується алгоритм зняття доповнення повідомлення, заданий п.Б.3. Якщо результатом є помилка оберненого перетворення, подальша обробка припиняється із повідомленням про порушення цілісності.

У разі, коли $\mu_{l/2}^{(|M''|-l/2)} \neq R_{|M''|,l/2}(M'')$, повертається повідомлення про порушення цілісності.

При $\mu_{l/2}^{(|M''|-l/2)} = R_{|M''|,l/2}(M'')$ результатом роботи режиму є відкритий текст $M = L_{|M''|,|M''|-l/2}(M'')$.

Додаток А
(обов'язковий)
Нелінійні таблиці заміни

А.1 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

```

A.2 Таблиці заміни для шару оберненого нелінійного бієктивного відображення

(шістнадцяткове подання)

Підстановка $_{-1}\pi_0$:

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

Підстановка $_{-1}\pi_1$:

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

Підстановка $_{-1}\pi_2$:

```

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

```

Підстановка $_{-1}\pi_3$:

```

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

```

Додаток Б
(обов'язковий)
Доповнення повідомлення

Б.1 Загальні положення

Режими роботи СМАС, СВС криптографічного алгоритму симетричного блокового перетворення передбачають обробку повідомлень, довжина яких є кратною розміру блоку базового перетворення.

Якщо у засобі криптографічного захисту інформації допускається застосування алгоритму симетричного перетворення у зазначених режимах для обробки повідомлень, чия довжина не є кратною розміру блоку базового перетворення, то перед початком застосування прямого перетворення режимів СМАС, СВС обов'язково застосовується доповнення повідомлення, визначене у п.Б.2, а після застосування оберненого перетворення обов'язково застосовується зняття доповнення повідомлення, визначене у п.Б.3.

Режими GCM, CCM використовують доповнення повідомлення відповідно до алгоритму п.Б.2 без застосування оберненого перетворення.

Режим KW застосовує алгоритми, визначені у пп.Б.2, Б.3, при формуванні проміжних даних обробки.

Б.2 Доповнення повідомлення

Для доповнення повідомлення (або його частини) довжиною N бітів ($N \geq 1$) у його кінець додається одиничний біт, а після нього ще $l-1-(N \bmod l)$ нульових бітів, де l – довжина блоку базового перетворення.

У результаті роботи повертається доповнене повідомлення, чия довжина кратна розміру блоку базового перетворення.

Б.3 Зняття доповнення повідомлення

Для зняття доповнення повідомлення з його кінця видаляються усі нульові біти (якщо такі присутні) і одиничний біт.

У разі, коли одиничний біт не виявлений (після застосування оберненого перетворення повідомлення складається лише з нулів) або після зняття доповнення повідомлення його довжина у бітах N дорівнює нулю, повертається повідомлення про помилку зняття доповнення (помилку оберненого перетворення).

У іншому випадку повертається повідомлення, з якого знято доповнення.

Додаток В
(довідковий).
Приклади для перевірки

В.1 Позначення

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

Таблиця В.1 – Скорочення, які застосовані у прикладах для перевірки

PLAINTEXT	M (відкритий текст або конфіденційна частина повідомлення)
PLAINTEXT[i]	m_i
N	N (довжина відкритого тексту або конфіденційної частини повідомлення в бітах)
AUHTTEXT	O (відкрита частина повідомлення)
AUHTTEXT[i]	o_i
No	N_o (довжина відкритої частини повідомлення в бітах)
KEY	K (ключ шифрування або ключ автентифікації, залежно від режиму)
KT	K_σ (допоміжний ключ)
k0	K_α
k1	K_ω
KD	K_δ
id	в залежності індексу циклового ключа та співвідношення розміру блоку та довжини ключа: $(K \ggg 32 \cdot i)$, або $L_{l,l/2}(K \ggg 16 \cdot i)$ чи $R_{l,l/2}\left(K \ggg 64 \cdot \left\lfloor \frac{i}{4} \right\rfloor\right)$
tmv	$\vartheta \ll (i/2)$
round[i]	i -й цикл перетворення зашифрування (розшифрування)
round[i].rkey	цикловий ключ, отриманий для використання на i -ої ітерації перетворення
add_rkey	результат виконання перетворення $\eta_l^{(K_v)}$
xor_rkey	результат виконання перетворення $\kappa_l^{(K_v)}$
s_box	результат виконання перетворення π'_l або ${}_{-1}\pi'_l$
s_row	результат виконання перетворення τ_l або ${}_{-1}\tau_l$
m_col	результат виконання перетворення ψ_l або ${}_{-1}\psi_l$
ShiftLeft	результат виконання перетворення \ll
Rotate	результат виконання перетворення \ggg
RotateLeft	результат виконання перетворення \lll

state[i]	значення внутрішнього стану процедури розгортання ключів на i -му циклі перетворення
CIPHERTEXT	шифртекст
CIPHERTEXT[i]	c_i
IV	S (синхропосилка)
ctr	s_0 (початкове значення лічильника);
ctr + i	$L_{l,l/2}(s_0 + i)$ при шифруванні в режимах CTR, GCM, CCM; $L_{l,l-q}(c_{i-1}^\#) \parallel c_i$ при шифруванні у режимі CFB;
gamma[i]	$L_{l, m_i }(T_{l,k}^{(K)}(L_{l,l/2}(s_0 + i) \parallel R_{l,l/2}(s_0)))$ при зашифруванні або $L_{l, c_i }(T_{l,k}^{(K)}(L_{l,l/2}(s_0 + i) \parallel R_{l,l/2}(s_0)))$ при розшифруванні в режимах CTR, GCM, CCM; $c_i^\#$ при шифруванні у режимі CFB
padded	результат виконання операції доповнення відкритого тексту до довжини, кратної розміру блоку базового перетворення
unpadded	результат виконання операції зняття доповнення
H	H (параметризована змінна автентифікації режиму GCM)
h	обчислене значення імітовставки відповідно до режимів CMAC, GCM, CCM
KD	K_δ
b[i]	b_i у режимі GCM
b[j,i]	b_i^j у режимі KW
bs[i]	b_i'
B	B у режимі GCM
B[j]	B^j у режимі KW
lambda_o	λ_o (довжина відкритої частини повідомлення)
lambda_c	λ_c (довжина конфіденційної частини повідомлення)
G1	G_1 (заголовок автентифікації режиму CCM)
alpha^i	α_l^i
alpha^i_mult_s	$\alpha_l^i \bullet s_0$
V	V

Вхідні значення і результати виконання операцій алгоритму шифрування подаються як бітові послідовності у шістнадцятковій нотації (запис до внутрішнього стану виконується у відповідності до п.6.2).

У разі, коли розмір відкритого або шифртексту не кратний розміру блоку, його довжина у бітах вказана після позначення (наприклад, PLAINTEXT (N = 259)). При цьому, якщо значення N не кратне 8, з останнього байту вибираються (N mod 8) старших бітів, наприклад, для N = 21 бітова послідовність, яка відповідає числу 871D18 у шістнадцятковій нотації, дорівнює 101101110001110100011; для N = 11 бітова послідовність, яка відповідає числу C2A0 у шістнадцятковій нотації, дорівнює 11000010101.

В.2 Базове перетворення

В.2.1 Розгортання 128-бітного ключа для шифрування 128-бітного блоку

```
KEY:
    000102030405060708090A0B0C0D0E0F

ТЕСТ ФОРМУВАННЯ ПРОМІЖНОГО КЛЮЧА КТ

state [0]:
    05000000000000000000000000000000

state [0].k0:
    000102030405060708090A0B0C0D0E0F

state [0].k1:
    000102030405060708090A0B0C0D0E0F

state [0].add_rkey:
    050102030405060708090A0B0C0D0E0F

state [0].s_box:
    75BB9A4D6BCB452A713ADFB31790511F

state [0].s_row:
    75BB9A4D1790511F713ADFB36BCB452A

state [0].m_col:
    62C97C6E6ABF4133ED5131D624C7C182

state [0].xor_rkey:
    62C87E6D6EBA4734E5583BDD28CACF8D

state [0].s_box:
    FC4F5E9CC3232E40D98141FC1FD382BF

state [0].s_row:
    FC4F5E9C1FD382BFD98141FCC3232E40

state [0].m_col:
    53E85C8F02C0CA94B7578DD19C8B8A35

state [0].add_rkey:
    53E95E9206C5D09BBF6097DCA8989844

state [0].s_box:
    5A04E6B66C846B1D26E724A5C50B28E5

state [0].s_row:
    5A04E6B6C50B28E526E724A56C846B1D

state [0].m_col:
    862F1F653B775BA1D05CBC2F38E2D87D

КТ:
    862F1F653B775BA1D05CBC2F38E2D87D

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-128/128 З ПАРНИМИ ІНДЕКСАМИ

state [0]:
    862F1F653B775BA1D05CBC2F38E2D87D

state [0].КТ:
    862F1F653B775BA1D05CBC2F38E2D87D
```

```

state [0].id:
000102030405060708090A0B0C0D0E0F

state [0].tmv:
01000100010001000100010001000100

state[0].add_rkey (tmv):
872F20653C775CA1D15CBD2F39E2D97D

state[0].add_rkey (kt_round):
87302268407C62A8D965C73A45EFE78C

state [0].s_box:
467CC09BDCA48F49074589CEE4597F21

state [0].s_row:
467CC09BE4597F21074589CEDCA48F49

state [0].m_col:
1A9A6AF231E9AD8BF973D32B8458BE1A

state[0].xor_rkey (kt_round):
9DB54A970D9EF12A282F6E04BDBA6767

state [0].s_box:
30E14EC0F0B004551F4DDA73AA23E2AA

state [0].s_row:
30E14EC0AA23E2AA1F4DDA73F0B00455

state [0].m_col:
8F203E065FC35445B5FEB9ACA7A0C676

state[0].add_rkey (kt_round):
16505E6B9B3AB1E6865B77DCE082A0F4

state[2].ShiftLeft (tmv):
02000200020002000200020002000200

state[2].Rotate (id):
08090A0B0C0D0E0F0001020304050607

state[2].add_rkey (tmv):
882F21653D775DA1D25CBE2F3AE2DA7D

state[2].add_rkey (kt_round):
90382B7049846BB0D25DC0323EE7E084

state [2].s_box:
EB9FC8EACC7E156C0A3752F3BBA6F67B

state [2].s_row:
EB9FC8EABBA6F67B0A3752F3CC7E156C

state [2].m_col:
1A29E0E1CC4D9E953829331A35006DB5

state[2].xor_rkey (kt_round):
9206C184F13AC334EA758D350FE2B7C8

state [2].s_box:
6913B67B54C8F34051B5EDCC09DDC196

state [2].s_row:

```

```

6913B67B09DDC19651B5EDCC54C8F340

state [2].m_col:
    F640660971D226D5B84DE2DA41B111C5

state[2].add_rkey (kt_round):
    7E70876EAE4984768AAAA00A7C93EC42

state[4].ShiftLeft (tmv):
    04000400040004000400040004000400

state[4].Rotate (id):
    000102030405060708090A0B0C0D0E0F

state[4].add_rkey (tmv):
    8A2F23653F775FA1D45CC02F3CE2DC7D

state[4].add_rkey (kt_round):
    8A302568437C65A8DC65CA3A48EFEA8C

state [4].s_box:
    217C9B9B37A49C493C45B0CE9C59E721

state [4].s_row:
    217C9B9B9C59E7213C45B0CE37A49C49

state [4].m_col:
    5F4F282C082C44E06D27B3AD5A6D0414

state[4].xor_rkey (kt_round):
    D5600B49375B1B41B97B7382668FD869

state [4].s_box:
    F8E7024FEED9D438EC06D610A5511B88

state [4].s_row:
    F8E7024FA5511B88EC06D610EED9D438

state [4].m_col:
    BB9EB160DF19E1536A15B652D328FC80

state[4].add_rkey (kt_round):
    45CED4C51E9140F53E7276820F0BD9FE

state[6].ShiftLeft (tmv):
    08000800080008000800080008000800

state[6].Rotate (id):
    08090A0B0C0D0E0F0001020304050607

state[6].add_rkey (tmv):
    8E2F2765437763A1D85CC42F40E2E07D

state[6].add_rkey (kt_round):
    963831704F8471B0D85DC63244E7E684

state [6].s_box:
    D39F2CEA277E0B6CC43719F342A60A7B

state [6].s_row:
    D39F2CEA42A60A7BC43719F3277E0B6C

state [6].m_col:
    24E625C345281CB2DDD2B8406AFC6B08

```

```

state[6].xor_rkey (kt_round):
AAC902A6065F7F13058E7C6F2A1E8B75

state [6].s_box:
A6779A076CCA333D753D60601567E9A6

state [6].s_row:
A6779A071567E9A6753D6060CCA333D

state [6].m_col:
FE47C7BD358960C17902A202C57DE333

state[6].add_rkey (kt_round):
8C77EE227900C462515F66320560C4B1

state[8].ShiftLeft (tmv):
10001000100010001000100010001000

state[8].Rotate (id):
000102030405060708090A0B0C0D0E0F

state[8].add_rkey (tmv):
962F2F654B776BA1E05CCC2F48E2E87D

state[8].add_rkey (kt_round):
963031684F7C71A8E865D63A54EFF68C

state [8].s_box:
D37C2C9B27A40B49124575CE96595421

state [8].s_row:
D37C2C9B96595421124575CE27A40B49

state [8].m_col:
9290A865A6D00D6FF71F20FDB73013F9

state[8].xor_rkey (kt_round):
04BF8700EDA766CE1743ECD2FFD2FB84

state [8].s_box:
6B058D68D6A0B984AFF35A82802F8B7B

state [8].s_row:
6B058D68802F8B7BAFF35A82D6A0B984

state [8].m_col:
7468437D115B4517CA2ACEF03DC4845A

state[8].add_rkey (kt_round):
0A9872E25CD2B0B8AA879A2086A66DD8

state[10].ShiftLeft (tmv):
20002000200020002000200020002000

state[10].Rotate (id):
08090A0B0C0D0E0F0001020304050607

state[10].add_rkey (tmv):
A62F3F655B777BA1F05CDC2F58E2F87D

state[10].add_rkey (kt_round):
AE384970678489B0F05DDE325CE7FE84

state [10].s_box:
A29FEFEA537EF76C8137E8F3BCA6747B

```

```
state [10].s_row:  
A29FEFEABCA6747B8137E8F3537EF76C
```

```
state [10].m_col:  
791B5A53FC485CDBC36C85A8CA94514E
```

```
state[10].xor_rkey (kt_round):  
DF346536A73F277A333059879276A933
```

```
state [10].s_box:  
C8089CE8A0BC85DB617C7BA0693FEB45
```

```
state [10].s_row:  
C8089CE8693FEB45617C7BA0A0BC85DB
```

```
state [10].m_col:  
B1F671433964497706AF16A690F54FE3
```

```
state[10].add_rkey (kt_round):  
5726B1A894DBC418F60BF3D5E8D74861
```

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-128/128 З НЕПАРНИМИ ІНДЕКСАМИ

```
roundKey [0]:  
16505E6B9B3AB1E6865B77DCE082A0F4
```

```
roundKey[1].RotateLeft:  
E6865B77DCE082A0F416505E6B9B3AB1
```

```
roundKey[3].RotateLeft:  
768AAA00A7C93EC427E70876EAE4984
```

```
roundKey[5].RotateLeft:  
F53E7276820F0BD9FE45CED4C51E9140
```

```
roundKey[7].RotateLeft:  
62515F66320560C4B18C77EE227900C4
```

```
roundKey[9].RotateLeft:  
B8AA879A2086A66DD80A9872E25CD2B0
```

СФОРМОВАНИ ЦИКЛОВІ КЛЮЧІ КАЛИНА-128/128

```
round[0].rkey:  
16505E6B9B3AB1E6865B77DCE082A0F4
```

```
round[1].rkey:  
E6865B77DCE082A0F416505E6B9B3AB1
```

```
round[2].rkey:  
7E70876EAE4984768AAA00A7C93EC42
```

```
round[3].rkey:  
768AAA00A7C93EC427E70876EAE4984
```

```
round[4].rkey:  
45CED4C51E9140F53E7276820F0BD9FE
```

```
round[5].rkey:  
F53E7276820F0BD9FE45CED4C51E9140
```

```
round[6].rkey:  
8C77EE227900C462515F66320560C4B1
```

```

round[7].rkey:
62515F66320560C4B18C77EE227900C4

round[8].rkey:
0A9872E25CD2B0B8AA879A2086A66DD8

round[9].rkey:
B8AA879A2086A66DD80A9872E25CD2B0

round[10].rkey:
5726B1A894DBC418F60BF3D5E8D74861

```

В.2.2 Розгортання 256-бітного ключа для шифрування 128-бітного блоку

```

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

ТЕСТ ФОРМУВАННЯ ПРОМІЖНОГО КЛЮЧА КТ

state [0]:
07000000000000000000000000000000

state [0].k0:
000102030405060708090A0B0C0D0E0F

state [0].k1:
101112131415161718191A1B1C1D1E1F

state [0].add_rkey:
070102030405060708090A0B0C0D0E0F

state [0].s_box:
59BB9A4D6BCB452A713ADFB31790511F

state [0].s_row:
59BB9A4D1790511F713ADFB36BCB452A

state [0].m_col:
4E79B8861793DD1FED5131D624C7C182

state [0].xor_rkey:
5E68AA950386CB08F5482BCD38DADF9D

state [0].s_box:
4712CEC20655EAD444D1C812F4DE91FF

state [0].s_row:
4712CEC2F4DE91FF44D1C8120655EAD4

state [0].m_col:
40FC95632BA11B2E408AF2832E729F57

state [0].add_rkey:
40FD97662FA621354893FC8E3A7FAD66

state [0].s_box:
DCC0245FC6703CCC9CFEF827D55FEE5F

state [0].s_row:
DCC0245FD55FEE5F9CFEF827C6703CCC

state [0].m_col:
1F4477802D3668599A40153652482CBF

```



```
КТ:
1F4477802D3668599A40153652482CBF

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-128/256 З ПАРНИМИ ІНДЕКСАМИ

state [0]:
1F4477802D3668599A40153652482CBF

state [0].КТ:
1F4477802D3668599A40153652482CBF

state [0].id:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

state [0].tmv:
0100010001000100010001000100

state[0].add_rkey (tmv):
204478802E3669599B40163653482DBF

state[0].add_rkey (kt_round):
20457A83323B6F60A34920415F553BCE

state [0].s_box:
3E33B1F19EAE3872E59B4938413C4184

state [0].s_row:
3E33B1F1413C4184E59B49389EAE3872

state [0].m_col:
F9F45F8A351DE7190CED38BE9E391A20

state[0].xor_rkey (kt_round):
D9B0270A1B2B8E4097AD2E88CD71379F

state [0].s_box:
078B8526FDB180B570E6D10520DCB4B2

state [0].s_row:
078B852620DCB4B270E6D105FDB180B5

state [0].m_col:
37849E6A1148A98452EC5420936D915B

state[0].add_rkey (kt_round):
57C816EB3F7E12DEED2C6B56E6B5BE1A

state[2].ShiftLeft (tmv):
0200020002000200020002000200

state[2].add_rkey (tmv):
214479802F366A599C40173654482EBF

state[2].add_rkey (kt_round):
31558B93434B8070B459315170654CDE

state [2].s_box:
723CE9D7374E87EAAE492C1422459D80

state [2].s_row:
723CE9D722459D80AE492C14374E87EA

state [2].m_col:
```

```

B352D956D536B2654E47C35D1428ADDB

state[2].xor_rkey (kt_round):
9216A0D6FA00D83CD207D46B40608364

state [2].s_box:
6988B387E6CE1B3A0AC101ABDCE75D37

state [2].s_row:
6988B387DCE75D370AC101ABE6CE1B3A

state [2].m_col:
B7C220FD5864632731F16C0F188480B0

state[2].add_rkey (kt_round):
D8069A7D889ACD80CD3184456CCCAE6F

state[4].ShiftLeft (tmv):
0400040004000400040004000400

state[4].Rotate (id):
08090A0B0C0D0E0F1011121314151617
18191A1B1C1D1E1F0001020304050607

state[4].add_rkey (tmv):
23447B8031366C599E401936564830BF

state[4].add_rkey (kt_round):
2B4D858B3D437A68AE512B496A5D46D6

state [4].s_box:
E1953F77A4F3B19BA263C84F5B37C387

state [4].s_row:
E1953F775B37C387A263C84FA4F3B19B

state [4].m_col:
C543C5047DC319547E7F3E36CEC258A3

state[4].xor_rkey (kt_round):
E607BE844CF5750DE03F2700988A681C

state [4].s_box:
13C1DD7B8FED6E1EACBC8568679CAC25

state [4].s_row:
13C1DD7B679CAC25ACBC85688FED6E1E

state [4].m_col:
A01D511704DDD4C0E4F133F510FAC23F

state[4].add_rkey (kt_round):
C361CC973513411A82324D2B6742F3FE

state[6].ShiftLeft (tmv):
0800080008000800080008000800

state[6].add_rkey (tmv):
27447F8035367059A2401D365A4834BF

state[6].add_rkey (kt_round):
3F5D999B51538E78A2411F395E4D3AC6

state [6].s_box:
A137301DE75B8067016BE10847950EE6

```

```

state [6].s_row:
  A137301D47950EE6016BE108E75B8067

state [6].m_col:
  B5E77C683534B50FAAAC63F3B3BC1CD3

state[6].xor_rkey (kt_round):
  92A303E80002C55608EC7EC5E9F4286C

state [6].s_box:
  694BB50BA8EBBED371345E06295A5389

state [6].s_row:
  694BB50B295A538971345E06A8EBBED3

state [6].m_col:
  5CCCE90B3099104B67AE52746470DB96

state[6].add_rkey (kt_round):
  8310698C65CF80A409EF6FAABEB80F56

state[8].ShiftLeft (tmv):
  10001000100010001000100010001000

state[8].Rotate (id):
  101112131415161718191A1B1C1D1E1F
  000102030405060708090A0B0C0D0E0F

state[8].add_rkey (tmv):
  2F4487803D367859AA40253662483CBF

state[8].add_rkey (kt_round):
  3F559993514B8E70C2593F517E655ADE

state [8].s_box:
  A13C30D7E74E80EAE849901408451880

state [8].s_row:
  A13C30D708451880E8499014E74E80EA

state [8].m_col:
  0BF3DD6AB724DFBDA53C3FC9C6A16AE7

state[8].xor_rkey (kt_round):
  24B75AEA8A12A7E40F7C1AFFA4E95658

state [8].s_box:
  B4A818E32156BCBA09A47161000455A1

state [8].s_row:
  B4A818E3000455A109A471612156BCBA

state [8].m_col:
  97913D434410A221590C44E2DF47D950

state[8].add_rkey (kt_round):
  C6D5C4C381461A7B034D691842901510

state[10].ShiftLeft (tmv):
  20002000200020002000200020002000

state[10].add_rkey (tmv):
  3F4497804D368859BA40353672484CBF

```

```

state[10].add_rkey (kt_round):
    3F459983513B8E60C2493F417E555ACE

state [10].s_box:
    A13330F1E7AE8072E89B9038083C1884

state [10].s_row:
    A13330F1083C1884E89B9038E7AE8072

state [10].m_col:
    39B1A6C170C3F9D57BCEEB12D8996F25

state[10].xor_rkey (kt_round):
    06F531413DF5718CC18EDE24AAD1239A

state [10].s_box:
    6CED2C38A4ED0B21EF3DE8EDA67AD88C

state [10].s_row:
    6CED2C38A67AD88CEF3DE8EDA4ED0B21

state [10].m_col:
    458C61A1F89135A0F8723B45DB00ECBE

state[10].add_rkey (kt_round):
    84D0F82146C8BDF9B2B3707B4D49387E

state[12].ShiftLeft (tmv):
    40004000400040004000400040004000

state[12].Rotate (id):
    18191A1B1C1D1E1F0001020304050607
    08090A0B0C0D0E0F1011121314151617

state[12].add_rkey (tmv):
    5F44B7806D36A859DA40553692486CBF

state[12].add_rkey (kt_round):
    775DD19B8953C678DA415739964D72C6

state [12].s_box:
    3B37F51D7D5B1967576BC608D39505E6

state [12].s_row:
    3B37F51DD39505E6576BC6087D5B1967

state [12].m_col:
    3CDEFEBF436BDB230B258F8591F35287

state[12].xor_rkey (kt_round):
    639A493F2E5D737AD165DAB303BB3E38

state [12].s_box:
    B79DEFDF9337D6DBEA453D8E0676B256

state [12].s_row:
    B79DEFDF0676B256EA453D8E9337D6DB

state [12].m_col:
    E4B524A8329B2CD2E5B8DAC2E7FCD9F3

state[12].add_rkey (kt_round):
    43FADB28A0D1D42BBFF92FF9794546B3

state[14].ShiftLeft (tmv):

```

80008000800080008000800080008000

state[14].add_rkey (tmv):
9F44F780AD36E8591A419536D248ACBF

state[14].add_rkey (kt_round):
A74D018CB943F6682A52A749E65DC2D6

state [14].s_box:
A095D921ECF3549B158EBC4F13370887

state [14].s_row:
A095D92113370887158EBC4FECF3549B

state [14].m_col:
BA67CCF50AA5E5DF662CF57A04B36300

state[14].xor_rkey (kt_round):
25233B75A7930D867C6D604CD6FBCFBF

state [14].s_box:
B65841A6A0FEDC63148C56235027827A

state [14].s_row:
B65841A65027827A148C5623A0FEDC63

state [14].m_col:
24DAF027D1F504CB40E00EFF2A6AAFD2

state[14].add_rkey (kt_round):
C31EE8A87E2CED245A21A435FDB25B92

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-128/256 З НЕПАРНИМИ ІНДЕКСАМИ

roundKey [0]:
57C816EB3F7E12DEED2C6B56E6B5BE1A

roundKey[1].RotateLeft:
DEED2C6B56E6B5BE1A57C816EB3F7E12

roundKey[3].RotateLeft:
80CD3184456CCCAE6FD8069A7D889ACD

roundKey[5].RotateLeft:
1A82324D2B6742F3FEC361CC97351341

roundKey[7].RotateLeft:
A409EF6FAABEB80F568310698C65CF80

roundKey[9].RotateLeft:
7B034D691842901510C6D5C4C381461A

roundKey[11].RotateLeft:
F9B2B3707B4D49387E84D0F82146C8BD

roundKey[13].RotateLeft:
2BBFF92FF9794546B343FADB28A0D1D4

СФОРМОВАНИ ЦИКЛОВІ КЛЮЧІ КАЛИНА-128/256

round[0].rkey:
57C816EB3F7E12DEED2C6B56E6B5BE1A

round[1].rkey:
DEED2C6B56E6B5BE1A57C816EB3F7E12

```

round[2].rkey:
D8069A7D889ACD80CD3184456CCCAE6F

round[3].rkey:
80CD3184456CCCAE6FD8069A7D889ACD

round[4].rkey:
C361CC973513411A82324D2B6742F3FE

round[5].rkey:
1A82324D2B6742F3FEC361CC97351341

round[6].rkey:
8310698C65CF80A409EF6FAABEB80F56

round[7].rkey:
A409EF6FAABEB80F568310698C65CF80

round[8].rkey:
C6D5C4C381461A7B034D691842901510

round[9].rkey:
7B034D691842901510C6D5C4C381461A

round[10].rkey:
84D0F82146C8BDF9B2B3707B4D49387E

round[11].rkey:
F9B2B3707B4D49387E84D0F82146C8BD

round[12].rkey:
43FADB28A0D1D42BBFF92FF9794546B3

round[13].rkey:
2BBFF92FF9794546B343FADB28A0D1D4

round[14].rkey:
C31EE8A87E2CED245A21A435FDB25B92

```

В.2.3 Розгортання 256-бітного ключа для шифрування 256-бітного блоку

```

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

ТЕСТ ФОРМУВАННЯ ПРОМІЖНОГО КЛЮЧА КТ

state [0]:
09000000000000000000000000000000
00000000000000000000000000000000

state [0].k0:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

state [0].k1:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

state [0].add_rkey:
090102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

```

```
state [0].s_box:
  DFBB9A4D6BCB452A713ADFB31790511F
  6D152B3DC91CBB83795C71D56F5716BD
```

```
state [0].s_row:
  DFBB71D5C91C511F713A9A4D6F57BB83
  6D15DFB36BCB16BD795C2B3D1790452A
```

```
state [0].m_col:
  81B873FEF0692FBB4EE3702C2DC1ECF9
  1C3B2ECCB31C46CB0EF13CE6FEE16710
```

```
state [0].xor_rkey:
  81B971FDF46C29BC46EA7A2721CCE2F6
  0C2A3CDA70950DC16E826FDE2FC790F
```

```
state [0].s_box:
  4C0C0B1B4E89A1697AC6B111DDE2134C
  17024CEFA03A10A52CECAD1B64C7FD1F
```

```
state [0].s_row:
  4C0CAD1BA03A134C7AC60B1B64C710A5
  1702B1114E89FD1F2CEC4CEFDDE2A169
```

```
state [0].m_col:
  D905723FF356C644F1610397522EE49F
  A5A1D64F36C3C5C9671996CA04DD3C87
```

```
state [0].add_rkey:
  D9067442F75BCC4BF96A0DA25E3BF2AE
  B5B2E8624AD8DBE07F32B0E520FA5AA6
```

```
state [0].s_box:
  0713146E2AD94B852579DCF847AEA042
  E980C515AB3968CB552E735A3E8A1807
```

```
state [0].s_row:
  0713735AAB39A0422579146E3E8A68CB
  E980DCF82AD91807552EC51547AE4B85
```

```
state [0].m_col:
  19198C1CA96B064B8E0ED34A5D7F1A85
  EF0932D459CFE4B29BA66D7355B8AEF8
```

```
KT:
  19198C1CA96B064B8E0ED34A5D7F1A85
  EF0932D459CFE4B29BA66D7355B8AEF8
```

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-256/256 З ПАРНИМИ ІНДЕКСАМИ

```
state [0]:
  19198C1CA96B064B8E0ED34A5D7F1A85
  EF0932D459CFE4B29BA66D7355B8AEF8
```

```
state [0].KT:
  19198C1CA96B064B8E0ED34A5D7F1A85
  EF0932D459CFE4B29BA66D7355B8AEF8
```

```
state [0].id:
  000102030405060708090A0B0C0D0E0F
  101112131415161718191A1B1C1D1E1F
```

```
state [0].tmv:
  01000100010001000100010001000100
  01000100010001000100010001000100
```

```

state[0].add_rkey (tmv):
  1A198D1CAA6B074B8F0ED44A5E7F1B85
  F00933D45ACFE5B29CA66E7356B8AFF8

state[0].add_rkey (kt_round):
  1A1A8F1FAE700D529717DE556A8C2994
  001B45E76EE4FBC9B4BF888E72D5CD17

state [0].s_box:
  973629BDA230DCAE7043E8485B0EA129
  A8BA0078C3878BA3AE05C72724B36483

state [0].s_row:
  9736C727C387A129704329BD24B38BA3
  A8BAE848A2306483AE0500785B0EDCAE

state [0].m_col:
  FD9D025DF9E7BE0E93420E6B880D30D9
  FB690743F5ED5827B9B648088A7CF24C

state[0].xor_rkey (kt_round):
  E7848F41538CB9451C4CDA21D6722B5C
  0B603497AF22BD952510267BDCC45DB4

state [0].s_box:
  0C7E29385A0EFAF46F163D2F50B7C818
  95E776C0766496C2B642AD7C3C9A366F

state [0].s_row:
  0C7EAD7C7664C8186F1629383C9A96C2
  95E73D2F5A0E366FB64276C050B7FAF4

state [0].m_col:
  DDC1992A356A54EAA0F97DBD8490AF1C
  79A996086E3EF1CD8360BD4D16DC7E3D

state[0].add_rkey (kt_round):
  F7DA2647DFD55B352F085208E30FCBA1
  69B3C9DCC80DD7801F072CC16C942E36

state[2].ShiftLeft (tmv):
  02000200020002000200020002000200
  02000200020002000200020002000200

state[2].Rotate (id):
  08090A0B0C0D0E0F1011121314151617
  18191A1B1C1D1E1F0001020304050607

state[2].add_rkey (tmv):
  1B198E1CAB6B084B900ED54A5F7F1C85
  F10934D45BCFE6B29DA66F7357B8B0F8

state[2].add_rkey (kt_round):
  23229827B778165AA01FE75D7394329C
  09234EEF77EC04D29DA771765BBDB6FF

state [2].s_box:
  4F64281131D4BB41788D7FC428C4C4FB
  DF58CB363B34988230A00BA80F250D61

state [2].s_row:
  4F640BA83B34C4FB788D28110F259882
  DF587FC431D40D6130A0CB3628C4BB41

```



```

state [2].m_col:
7483738AAB21CB5E17E9CB7A18D2905A
3044F3F891B92D0E8664B18829DCE74D

state[2].xor_rkey (kt_round):
6F9AFD96004AC31587E71E3047AD8CDF
C14DC72CCA76CBBC1BC2DEFB7E6457B5

state [2].s_box:
1E9D0CEBA868F34A46A6167032E6ECEF
EF9589D1C13FEA69FD94E8C90896C650

state [2].s_row:
1E9DE8C9C13FECEF46A60CEB0896EA69
EF951670A868C650FD9489D132E6F34A

state [2].m_col:
C406833B5209E65A31475C7EC4101C56
357966BDA43338181AD68DC29997C2C9

state[2].add_rkey (kt_round):
DF1F1158FD74EEA5C15531C9239038DB
26839A9100031FCBB77CFD35F14F73C2

state[4].ShiftLeft (tmv):
04000400040004000400040004000400
04000400040004000400040004000400

state[4].Rotate (id):
101112131415161718191A1B1C1D1E1F
000102030405060708090A0B0C0D0E0F

state[4].add_rkey (tmv):
1D19901CAD6B0A4B920ED74A617F1E85
F30936D45DCFE8B29FA6717359B8B2F8

state[4].add_rkey (kt_round):
2D2AA22FC1802062AA27F1657D9C3CA4
F30A38D761D4EEB9A7AF7B7E65C5C007

state [4].s_box:
D2025766EF2A4915A6AA04BE9F074CF6
EDD6095C48534647A0F9E5AC8884522A

state [4].s_row:
D202E5AC48534CF6A6AA576688844647
EDD604BEEF2A522AA0F9095C9F074915

state [4].m_col:
A109372255EE05E6B92165C7B7C1D130
4DB87490C3774C28001C032FEACDC415

state[4].xor_rkey (kt_round):
BC10A73EF8850FAD2B2FB28DD6BECFB5
BEB142449EB8A49A9FBA725CB37576ED

state [4].s_box:
9442BCE185A259D0E14DCABF50248250
F646D7E591E0078CB1230518BDB56C98

state [4].s_row:
9442051891E08250E14DBCE1BDB5078C
F646CABF85A26C98B123D7E5502459D0

state [4].m_col:

```

AD11556EAF961BF3CFD185CC77B8B77
3E6CB13C9E420EAB4CF08F85036A4A1A

state[4].add_rkey (kt_round):
CA2AE58A5C656C0ACE0BF0A628FBA9FC
3176E710FC11F75DEB9601F95C22FD12

state[6].ShiftLeft (tmv):
08000800080008000800080008000800
08000800080008000800080008000800

state[6].Rotate (id):
18191A1B1C1D1E1F0001020304050607
08090A0B0C0D0E0F1011121314151617

state[6].add_rkey (tmv):
2119941CB16B0E4B960EDB4A657F2285
F7093AD461CFECB2A3A675735DB8B6F8

state[6].add_rkey (kt_round):
3932AE37CD882C6A960FDD4D6984288C
FF1244DF6DDCFAC1B3B7878671CDCC0F

state [6].s_box:
192E319420112DD8D3F865CFF97E5321
805611EF7B1F21C6BDA88D6333524B1F

state [6].s_row:
192E8D637B1F5321D3F83194335221C6
805665CF20114B1FBDA811EFF97E2DD8

state [6].m_col:
4AA6E8AF7E516A17E66B7739036BA142
1E8FD918F4A78B59A9F1ABBC7C4ACE92

state[6].xor_rkey (kt_round):
6BBF7CB3CF3A645C7065AC73661483C7
E986E3CC956867EB0A57DECF21F2786A

state [6].s_box:
DB05608E82C8CC182245AB0CA5655D2B
2955586AD712E2AD87A1E839DD0166D8

state [6].s_row:
DB05E839D7125D2B2245608EDD01E2AD
2955AB0C82C866D887A1586AA565CC18

state [6].m_col:
303E68D014A53103AEE60C228D73A9FB
CB91B47F8141D1CA55702E278E5F9A67

state[6].add_rkey (kt_round):
5157FCECC510404E44F5E76CF2F2CB80
C29BEE53E310BE7DF816A49AEB175160

state[8].ShiftLeft (tmv):
10001000100010001000100010001000
10001000100010001000100010001000

state[8].Rotate (id):
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

state[8].add_rkey (tmv):
29199C1CB96B164B9E0EE34A6D7F2A85

```

FF0942D469CFF4B2ABA67D7365B8BEF8

state[8].add_rkey (kt_round):
291A9E1FBD701C52A617ED55798C3894
0F1B54E77DE40ACAC3BF978E81D5DC17

state [8].s_box:
BF3640BDAA30CDAE98430648770E0929
09BA4D789F87DF1C8C0524274CB32A83

state [8].s_row:
BF3624279F870929984340BD4CB3DF1C
09BA0648AA302A838C054D78770ECD4E

state [8].m_col:
385521F2597A5C8ABB3B2F35571EDEC7
9C88CB7B477C127DF539FFD0004CDF8F

state[8].xor_rkey (kt_round):
114CBDEEE0114AC12535CC7F3A61F442
638189AF2EB3E6CF5E9F82A365F46177

state [8].s_box:
F316963BAC154EC6B65D4B5BD52B396E
B7DAF7C7931E0A394798F065885A81EC

state [8].s_row:
F316F065931E396EB65D963B885A0A39
B7DA4B5BAC1581EC4798F7C7D52B4EC6

state [8].m_col:
3503796BE2E56FDF030FEF3CEA018E4C
0CC6609C407774FDC0D3CB3EE27BA8F2

state[8].add_rkey (kt_round):
5E1C15889B51862AA11DD2875781B8D1
0BD0A270AA4669B06B7A49B2473467EB

state[10].ShiftLeft (tmv):
20002000200020002000200020002000
20002000200020002000200020002000

state[10].Rotate (id):
08090A0B0C0D0E0F1011121314151617
18191A1B1C1D1E1F0001020304050607

state[10].add_rkey (tmv):
3919AC1CC96B264BAE0EF34A7D7F3A85
0F0A52D479CF04B3BBA68D7375B8CEF8

state[10].add_rkey (kt_round):
4122B627D578345ABE1F055E9194509C
27236CEF95EC22D2BBA78F7679BDD4FF

state [10].s_box:
F2640D11F8D47641F68D222C84C410FB
0E58A436D734C08299A029A877250161

state [10].s_row:
F26429A8D73410FBF68D0D117725C082
0E58222CF8D4016199A0A43684C47641

state [10].m_col:
4641D0938B13DFE45A7B1CCDBA270481
1FF4E160AB164E2DB1ADA6996A4D2157

```

```

state[10].xor_rkey (kt_round):
    7F587C8F4278F9AFF475EF87C7583E04
    10FEB3B4D2D94A9E0A0B2BEA1FF5EFAF

state [10].s_box:
    5581600983D434C74EB544A07F81B273
    6D293A6F0A354EC187B2C8E339ED44C7

state [10].s_row:
    5581C8E30A35B2734EB5600939ED4EC1
    6D2944A083D444C787B23A6F7F8134C7

state [10].m_col:
    FE387A41563DC05F5A1BB64EB4487CF6
    F9598D131BA04A3CC1B41F091D5A0C0A

state[10].add_rkey (kt_round):
    3752265E1FA9E6AA082AA99931C8B67B
    0864DFE7946F4FEF7C5BAD7C9212DB02

state[12].ShiftLeft (tmv):
    40004000400040004000400040004000
    40004000400040004000400040004000

state[12].Rotate (id):
    101112131415161718191A1B1C1D1E1F
    000102030405060708090A0B0C0D0E0F

state[12].add_rkey (tmv):
    5919CC1CE96B464BCE0E134B9D7F5A85
    2F0A72D499CF24B3DBA6AD7395B8EEF8

state[12].add_rkey (kt_round):
    692ADE2FFD805C62E6272D66B99C78A4
    2F0B74D79DD42ABAE3AFB77EA1C5FC07

state [12].s_box:
    F902E8668B2AD31513AAE05FEC0766F6
    C6B2145C30537A3F10F9C1AC1184F82A

state [12].s_row:
    F902C1AC305366F613AAE86611847A3F
    C6B2E05F8B2AF82A10F9145CEC07D315

state [12].m_col:
    0F050A1A16CAE04C8014C1DA4136B7C3
    C669FDD3BA832B8287F32F35EB78B8DD

state[12].xor_rkey (kt_round):
    561CC606FFA1A6074E1AD291DC49ED46
    E9638F07234C0F315C5582467EC05625

state [12].s_box:
    23F5194E80328A2A0436799F3C9B06F9
    29FD292A4F16595DBC3CF0F908F15551

state [12].s_row:
    23F5F0F94F1606F90436194E08F1595D
    29FD799F80325551BC3C292A3C9B8A2A

state [12].m_col:
    DF8D77B9961CF272A6C26B217AB48C40
    FCBD0BC4AA3691539E006FA36302A142

```

```
state[12].add_rkey (kt_round):
38A743D67F8838BE74D17E6C1734E7C5
2BC87D984406B60679A71C17F9BA8F3B
```

```
state[14].ShiftLeft (tmv):
80008000800080008000800080008000
80008000800080008000800080008000
```

```
state[14].Rotate (id):
18191A1B1C1D1E1F0001020304050607
08090A0B0C0D0E0F1011121314151617
```

```
state[14].add_rkey (tmv):
99190C1D296C864B0E0F534BDD7F9A85
6F0AB2D4D9CF64B31BA7ED73D5B82EF9
```

```
state[14].add_rkey (kt_round):
B13226384589A46A0E10554EE184A08C
7713BCDFE5DC72C22BB8FF86E9CD4410
```

```
state [14].s_box:
BE2EAD56E4D507D8D842A932527EB321
3BB4BDEFD91F0593E1E0676329521122
```

```
state [14].s_row:
BE2E6763D91FB321D842AD5629520593
3BB4A932E4D51122E1E0BDEF527E07D8
```

```
state [14].m_col:
6B32139766E2C11626F86626C792297A
C2811243AC6428547C2FC387411FE262
```

```
state[14].xor_rkey (kt_round):
F22B1F8A4F8E475D28F7356D1AEDB3FF
AD8BA09775AB4CE767882EF494A7CC9B
```

```
state [14].s_box:
C0B1E143273D2EC41F66789C97FB3A61
0BCFB3C0C7C39D785311D1599DA04B1D
```

```
state [14].s_row:
C0B1D159C7C33A611F66E1439DA09D78
0BCF789C273D4B1D5311B3C097FB2EC4
```

```
state [14].m_col:
6350A58A0C5544FE0A419870AB566227
EE6B64418240377ED68A5651E36CBB09
```

```
state[14].add_rkey (kt_round):
FC69B1A735C1CA491850EBBB88D6FCAC
5D7616165C109C31F13144C5B825EA02
```

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-256/256 З НЕПАРНИМИ ІНДЕКСАМИ

```
roundKey [0]:
F7DA2647DFD55B352F085208E30FCBA1
69B3C9DCC80DD7801F072CC16C942E36
```

```
roundKey[1].RotateLeft:
08E30FCBA169B3C9DCC80DD7801F072C
C16C942E36F7DA2647DFD55B352F0852
```

```
roundKey[3].RotateLeft:
C9239038DB26839A9100031FCBB77CFD
35F14F73C2DF1F1158FD74EEA5C15531
```

roundKey[5].RotateLeft:
 A628FBA9FC3176E710FC11F75DEB9601
 F95C22FD12CA2AE58A5C656C0ACE0BF0

roundKey[7].RotateLeft:
 6CF2F2CB80C29BEE53E310BE7DF816A4
 9AEB1751605157FCECC510404E44F5E7

roundKey[9].RotateLeft:
 875781B8D10BD0A270AA4669B06B7A49
 B2473467EB5E1C15889B51862AA11DD2

roundKey[11].RotateLeft:
 9931C8B67B0864DFE7946F4FEF7C5BAD
 7C9212DB023752265E1FA9E6AA082AA9

roundKey[13].RotateLeft:
 6C1734E7C52BC87D984406B60679A71C
 17F9BA8F3B38A743D67F8838BE74D17E

СФОРМОВАНИ ЦИКЛОВІ КЛЮЧІ КАЛИНА-256/256

round[0].rkey:
 F7DA2647DFD55B352F085208E30FCBA1
 69B3C9DCC80DD7801F072CC16C942E36

round[1].rkey:
 08E30FCBA169B3C9DCC80DD7801F072C
 C16C942E36F7DA2647DFD55B352F0852

round[2].rkey:
 DF1F1158FD74EEA5C15531C9239038DB
 26839A9100031FCBB77CFD35F14F73C2

round[3].rkey:
 C9239038DB26839A9100031FCBB77CFD
 35F14F73C2DF1F1158FD74EEA5C15531

round[4].rkey:
 CA2AE58A5C656C0ACE0BF0A628FBA9FC
 3176E710FC11F75DEB9601F95C22FD12

round[5].rkey:
 A628FBA9FC3176E710FC11F75DEB9601
 F95C22FD12CA2AE58A5C656C0ACE0BF0

round[6].rkey:
 5157FCECC510404E44F5E76CF2F2CB80
 C29BEE53E310BE7DF816A49AEB175160

round[7].rkey:
 6CF2F2CB80C29BEE53E310BE7DF816A4
 9AEB1751605157FCECC510404E44F5E7

round[8].rkey:
 5E1C15889B51862AA11DD2875781B8D1
 0BD0A270AA4669B06B7A49B2473467EB

round[9].rkey:
 875781B8D10BD0A270AA4669B06B7A49
 B2473467EB5E1C15889B51862AA11DD2

round[10].rkey:
 3752265E1FA9E6AA082AA99931C8B67B

0864DFE7946F4FEF7C5BAD7C9212DB02

round[11].rkey:
9931C8B67B0864DFE7946F4FEF7C5BAD
7C9212DB023752265E1FA9E6AA082AA9

round[12].rkey:
38A743D67F8838BE74D17E6C1734E7C5
2BC87D984406B60679A71C17F9BA8F3B

round[13].rkey:
6C1734E7C52BC87D984406B60679A71C
17F9BA8F3B38A743D67F8838BE74D17E

round[14].rkey:
FC69B1A735C1CA491850EBBB88D6FCAC
5D7616165C109C31F13144C5B825EA02

В.2.4 Розгортання 512-бітного ключа для шифрування 256-бітного блоку

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

ТЕСТ ФОРМУВАННЯ ПРОМІЖНОГО КЛЮЧА КТ

state [0]:
0D000000000000000000000000000000
00000000000000000000000000000000

state [0].k0:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

state [0].k1:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

state [0].add_rkey:
0D0102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

state [0].s_box:
F0BB9A4D6BCB452A713ADFB31790511F
6D152B3DC91CBB83795C71D56F5716BD

state [0].s_row:
F0BB71D5C91C511F713A9A4D6F57BB83
6D15DFB36BCB16BD795C2B3D1790452A

state [0].m_col:
AE04BE1C9546BC944EE3702C2DC1ECF9
1C3B2ECCB31C46CB0EF13CE6FEE16710

state [0].xor_rkey:
8E259C3FB1639AB366CA5A0701ECC2D6
2C0A1CFF872970FC36C806DDC2DC592F

state [0].s_box:
89F43EDFBEFD958EA5D3182A43340887
49D6CD61460F1E57FA4F45FCE81F7B66

```
state [0].s_row:
  89F445FC460F0887A5D33EDFE81F1E57
  49D6182ABEFD7B66FA4FCD614334958E
```

```
state [0].m_col:
  FB38EF23C9943F7F252BB9CAB6405AAD
  99589805F39649485E9FE892FE2A188D
```

```
state [0].add_rkey:
  FB39F126CD9945862D34C3D5C24D68BC
  A969AA1807AC5F5F76B802AE1A4836AC
```

```
state [0].s_box:
  CA14049E208F0063D208F39DE895AC69
  020DCE1359A94871B2E09A4297D1B7B9
```

```
state [0].s_row:
  CA149A4259A9AC69D208049E97D14871
  020DF39D208FB7B9B2E0CE13E8950063
```

```
state [0].m_col:
  AD632F572D6E2D6E7C09DFA2F2206E6E
  6E941BE6D4514D414B83EE3181E65B46
```

```
KT:
  AD632F572D6E2D6E7C09DFA2F2206E6E
  6E941BE6D4514D414B83EE3181E65B46
```

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-256/512 З ПАРНИМИ ІНДЕКСАМИ

```
state [0]:
  AD632F572D6E2D6E7C09DFA2F2206E6E
  6E941BE6D4514D414B83EE3181E65B46
```

```
state [0].KT:
  AD632F572D6E2D6E7C09DFA2F2206E6E
  6E941BE6D4514D414B83EE3181E65B46
```

```
state [0].id:
  000102030405060708090A0B0C0D0E0F
  101112131415161718191A1B1C1D1E1F
  202122232425262728292A2B2C2D2E2F
  303132333435363738393A3B3C3D3E3F
```

```
state [0].tmv:
  01000100010001000100010001000100
  01000100010001000100010001000100
```

```
state[0].add_rkey (tmv):
  AE6330572E6E2E6E7D09E0A2F3206F6E
  6F941CE6D5514E414C83EF3182E65C46
```

```
state[0].add_rkey (kt_round):
  AE64325A327334758512EAADFF2D7D7D
  7FA52EF9E9666458649C094D9E037B65
```

```
state [0].s_box:
  A296C4419E6C76A6DA56E7D0806DAFDD
  553BD19129FCCA16A076ACF9192E5BE
```

```
state [0].s_row:
  A2966ACF29FCAFDDDA56C4419192CCA1
  553BE7D09E6CE5BE6A07D191806D76A6
```

```
state [0].m_col:
```



```

7AEC1A5F1B29136969224EF37117F911
5082050AFA459DDCB43FE4EDEE7B8106

state[0].xor_rkey (kt_round):
D48F2A0835473D07142BAE518237967F
3F1619EC2F14D39DF8BC0BDC6C9DDD40

state [0].s_box:
7E517AD463FADE2AC9B13114FE3E375B
A188E474C665BFFF851D02A538B965B5

state [0].s_row:
7E5102A5C665375BC9B17AD438B9BFFF
A188311463FA65B5851DE474FE3EDE2A

state [0].m_col:
495A67E19FDBAE3A8E90DD68CFD78B3
19CCE15C710A51151055050232E32C7E

state[0].add_rkey (kt_round):
F7BD9738CE49DDA80B9ABD79801EE821
8860FE42475C9F565CD8F433B4C989C4

state[2].ShiftLeft (tmv):
02000200020002000200020002000200
02000200020002000200020002000200

state[2].add_rkey (tmv):
AF6331572F6E2F6E7E09E1A2F420706E
70941DE6D6514F414D83F03183E65D46

state[2].add_rkey (kt_round):
CF84537A53935595A6320BCE204E9E9D
A0C54F190B87857885BC2A6DBF239C85

state [2].s_box:
827E9EDB5AFE9C2982E02843E9140FF
7884358A95BF3F67DA1D7A9C26583E8F

state [2].s_row:
827E7A9C95BF40FF982E9EDB26583F67
788402845AFE3E8FDA1D358A3E91A9C2

state [2].m_col:
90BEEC22C412E3566D0C5E073CB45FDC
1A22E07311A7DBF6579837CD133089AA

state[2].xor_rkey (kt_round):
3FDDDD75EB7CCC381305BFA5C8942FB2
6AB6FD95C7F694B71A1BC7FC90D6D4EC

state [2].s_box:
A19965A6B9A44B56CBCB4375FBC47200
5BB80CC27FA750C597BA8957EB610174

state [2].s_row:
A19989577FA77200CBCB65A6EB6150C5
5BB84375B9A4017497BA0CC2FBC44B56

state [2].m_col:
91A74E4CB680E1F584F99CC1508750D5
50919E9D24F1446F53B0A16F6F256C8C

state[2].add_rkey (kt_round):
400B80A3E5EE106402037E6445A8C043

```

C025BC83FB4294B0A03392A1F20BCAD2

state[4].ShiftLeft (tmv):
 04000400040004000400040004000400
 04000400040004000400040004000400

state[4].Rotate (id):
 08090A0B0C0D0E0F1011121314151617
 18191A1B1C1D1E1F2021222324252627
 28292A2B2C2D2E2F3031323334353637
 38393A3B3C3D3E3F0001020304050607

state[4].add_rkey (tmv):
 B1633357316E316E8009E3A2F620726E
 72941FE6D85151414F83F23185E65F46

state[4].add_rkey (kt_round):
 B96C3D623D7B3F7D901AF5B50A368885
 8AAD3901F56E6F606FA41455A90B866D

state [4].s_box:
 EC89DE15A40690DDEB3686508744C78F
 21E63B8D44E338721EEF944802B2889C

state [4].s_row:
 EC89944844E3C78FEB36DE1502B23872
 21E68650A406889C1EEF3B8D874490DD

state [4].m_col:
 D0D2A52F00CAA937AF0AEC45D1F620D4
 BB99DD9A3F2EAD2FE6DC926AF357B71E

state[4].xor_rkey (kt_round):
 61B1967831A498592F030FE727D652BA
 C90DC27CE77FFC6EA95F605B76B1E858

state [4].s_box:
 4846376772EF2892C69259780E614F3F
 059008280C5FF8FA02CA56B1B246C5A1

state [4].s_row:
 484656B10C5F4F3FC6923767B246F8FA
 0590597872EFC5A102CA08280E612892

state [4].m_col:
 1FAEA40EB0780D0AB532F94600C1BF77
 FDE58F6ACAAFC245494A60727B6579BE

state[4].add_rkey (kt_round):
 D011D865E1E63E78353CDCE9F6E131E6
 6F7AAF50A301148798CD52A4004CD904

state[6].ShiftLeft (tmv):
 08000800080008000800080008000800
 08000800080008000800080008000800

state[6].add_rkey (tmv):
 B5633757356E356E8409E7A2FA20766E
 769423E6DC5155415383F63189E66346

state[6].add_rkey (kt_round):
 DD8C6182619B639DB43A19D62E56ACA5
 AECD5D21198F93805384F8348DEB694D

state [6].s_box:

```

620E8110486A77FFAEC8E4879319AB75
A252362FE051A8345A7E8C401B03B8CF

state [6].s_row:
620E8C40E051AB75AEC881101B03A834
A252E487486AB8CF5A7E362F931977FF

state [6].m_col:
BD93C3FD74216DD1B4C31EAE6DD2299D
2B7A5161A7E323BEDC1D3C630EC82CAE

state[6].xor_rkey (kt_round):
08F0F4AA414F58BF30CAF90C97F25FF3
5DEE72877BB276FF8F9ECA52872E4FE8

state [6].s_box:
71B639E4F2EED07A92D33454700148F0
A9DB05A0F5806C61FFB0B0AE4673350B

state [6].s_row:
71B6B0AEF58048F092D339E446736C61
A9DB3454F2EE350BFFB005A07001D07A

state [6].m_col:
FD35509E796E47E2C57D43EFB9B69761
F8362F80F625F1EEA0ADFB9E931CCB8FE

state[6].add_rkey (kt_round):
B29987F5AEDC7C5049872A92B4D70DD0
6ECB5266D3774630F330F21BBBB21C45

state[8].ShiftLeft (tmv):
10001000100010001000100010001000
10001000100010001000100010001000

state[8].Rotate (id):
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
000102030405060708090A0B0C0D0E0F

state[8].add_rkey (tmv):
BD633F573D6E3D6E8C09EFA202217E6E
7E942BE6E4515D415B83FE3191E66B46

state[8].add_rkey (kt_round):
CD74516A51835385A42209BE1E3E9C8D
9EB54D090977836883AC285DBD139A75

state [8].s_box:
204AD5D8E7009E8F00646AE245D83EBF
91E17D52DF975D9B60A953C4AAB495A6

state [8].s_row:
204A53C4DF973EBF0064D5D8AAB45D9B
91E16AE2E70095A660A97D5245D89E8F

state [8].m_col:
33E7193F1E502A1F6478A38FA24735B0
485388A09E15B35A0C6C99D60337FAFC

state[8].xor_rkey (kt_round):
8E842668233E1771E8714C2DA0664BDE
36C7A3467A44EE1B57EF67E792D191BA

```

```

state [8].s_box:
    897EAD9B4FD8A3BC12DC9D1678FC1280
    FAA31FF9BABD46D52B59E278697ACF3F

state [8].s_row:
    897EE278BABD128012DCAD9B697A46D5
    FAA39D164FD8CF3F2B591FF978FCA3BC

state [8].m_col:
    96F7850E919AFA70A4F27B11D5B09E58
    9F5BE3CABE75396BB9E5E9943D9AB746

state[8].add_rkey (kt_round):
    535BC565CE0838DF30FC6AB4D7D11CC7
    1DF00EB1A3C796AC1469E8C6CE80238D

state[10].ShiftLeft (tmv):
    20002000200020002000200020002000
    20002000200020002000200020002000

state[10].add_rkey (tmv):
    CD634F574D6E4D6E9C09FFA212218E6E
    8E943BE6F4516D416B830E32A1E67B46

state[10].add_rkey (kt_round):
    FD94818A81A383A5D44239DE4E5ECCAD
    8E953DE9F8567348738C183DADF38955

state [10].s_box:
    8BC4C9434C4B5D757E693B8004604BD0
    8947DE958519D6E9280E62D20BF0F748

state [10].s_row:
    8BC462D285194BD07E69C9430BF0D6E9
    89473B804C4BF748280EDE9504605D75

state [10].m_col:
    EBED1B41E47BF5347A4318A53298A03
    A61B4E0E6B52456A082D2E3B12FBC825

state[10].xor_rkey (kt_round):
    268E5416A915B63DDBADCE284108046D
    288F75E89F03282B63AE2009B31DB363

state [10].s_box:
    9A3D4D53021C0DD2B8E684F2F2E9989C
    1F516E0BB192535EB7784952BD573AFD

state [10].s_row:
    9A3D4952B192989CB8E64D53BD57535E
    1F5184F2021C3AFDB7786E0BF2E90DD2

state [10].m_col:
    8AF008FEE045302EC63CF177DE3D7910
    3F039DDF6676C91DCC14F00517AEFC51

state[10].add_rkey (kt_round):
    575458552EB47D9C6246F01AF15E077F
    CD97D8C55BC8365F3798FE37B8947898

state[12].ShiftLeft (tmv):
    40004000400040004000400040004000
    40004000400040004000400040004000

state[12].Rotate (id):

```

```
18191A1B1C1D1E1F2021222324252627
28292A2B2C2D2E2F3031323334353637
38393A3B3C3D3E3F0001020304050607
08090A0B0C0D0E0F1011121314151617
```

```
state[12].add_rkey (tmv):
ED636F576D6E6D6EBC091FA33221AE6E
AE945BE614528D418B832E32C1E69B46
```

```
state[12].add_rkey (kt_round):
057D8972898B8B8DDC2A41C65646D495
D6BD8511417FBB70BBB46065F51BD27D
```

```
state [12].s_box:
75A5F7627DCF9BF3C02A5E623AB01C2
50253F03F25F6FEA993856BE44BA79DD
```

```
state [12].s_row:
75A556BEF25F01C23C02F76244BA6FEA
5025A5E67DCF79DD99383F0323ABE9BF
```

```
state [12].m_col:
4904EC17619C76E16EDCC35F41AAE239
EEED3A3868C5D647DA128E40C07839E6
```

```
state[12].xor_rkey (kt_round):
A46783400CF21B8FD2D5DCFC738B4C57
407961DE7C975B065191A072019EA2A0
```

```
state [12].s_box:
00415DB51701D4090AB32A5728CF9D30
DC6281801486974EE793B36243B05797
```

```
state [12].s_row:
0041B36214869D300AB35DB543B0974E
DC622A5717015797E793818028CFD409
```

```
state [12].m_col:
C1AC36FE4137026F7A95BF0AF1592D5B
0B3B5BB7FF54EA20BCF06768F11B8A2E
```

```
state[12].add_rkey (kt_round):
AE10A655AFA56FDD369FDEAD237BDBC9
B9CFB69D14A777624774969AB2022675
```

```
state[14].ShiftLeft (tmv):
80008000800080008000800080008000
80008000800080008000800080008000
```

```
state[14].add_rkey (tmv):
2D64AF57AD6EAD6EFC095FA37221EE6E
EE949BE65452CD41CB836E3201E7DB46
```

```
state[14].add_rkey (kt_round):
659DE992E9ABEBADFC0A61A67626F475
F69DA5F1605FDB50DB94804515FCF15D
```

```
state [14].s_box:
88B9A7B629C361D07CD68107B22239A6
A7B91C6D34CA6831B8C487F44DC704C4
```

```
state [14].s_row:
88B987F434CA39A67CD6A7B64DC76831
A7B9810729C304C4B8C41C6DB22261D0
```

```

state [14].m_col:
52CE3A5C45CD792D26096551D72119FB
6884C66F66A2E2281528DE7B4E863534

state[14].xor_rkey (kt_round):
7FAA950BE8A3D443DA003AF2A500F795
86105D8932F02F69DEABB0494F61EE72

state [14].s_box:
55FF0FB3124B010E57CE0EDC68CEAAC2
1842369A9EB67288E3C3734F272B4662

state [14].s_row:
55FF734F9EB6AAC257CE0FB3272B7288
18420EDC124B4662E3C3369A68CE010E

state [14].m_col:
0E43B4841D8A94569F092BD6E4228E26
DD6DC57E548AD30892EC238986A448AE

state[14].add_rkey (kt_round):
3BA763DCCAF841C59B138A7957447C95
CB026165A9DCA04A5D7092BB878B24F5

state[16].ShiftLeft (tmv):
0001000100010001000100010001
0001000100010001000100010001

state[16].Rotate (id):
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

state[16].add_rkey (tmv):
AD642F582D6F2D6F7C0ADFA3F2216E6F
6E951BE7D4524D424B84EE3281E75B47

state[16].add_rkey (kt_round):
CD85517B51945396A43309CF1E4F9C9E
9EC64D1A0988837983BD286EBD249A86

state [16].s_box:
20A2D57CE7C49EEB00F76A3945EE3EC1
91E87DB7DF115D20602553FAAA9E9563

state [16].s_row:
20A253FADF113EC100F7D57CAA9E5D20
91E86A39E7C4956360257DB745EE9EEB

state [16].m_col:
33EA3FD054E41A5679AEE6C6D4B74A71
0BC517D1E254A8425C3A0559ED7DAEE7

state[16].xor_rkey (kt_round):
9E8E1088798B373905A439652696241E
65500C363606E50017BEEB6B6C9AF5A0

state [16].s_box:
913D4A0577CFB40875EF3BBE9A095CF5
884C9FE8FA134768AF2461AB389D8697

state [16].s_row:
913D61ABFA135CF575EF4A05389D4768
884C3BBE77CF8697AF249FE89A09B408

```

```
state [16].m_col:
6C5916C2F3CF19CF2153A86FA30BEE6E
79A15F55692CEA862327B5D47192B231
```

```
state[16].add_rkey (kt_round):
19BE451A213F473E9D5D8713962D5CDE
E7367B3C3E7F37C96EABA307F3790E79
```

```
state[18].ShiftLeft (tmv):
00020002000200020002000200020002
00020002000200020002000200020002
```

```
state[18].add_rkey (tmv):
AD652F592D702D707C0BDFA4F2226E70
6E961BE8D4534D434B85EE3381E85B48
```

```
state[18].add_rkey (kt_round):
AD66315C317533778414E9AFFE2F7C7F
7EA72DFBE868635A639E084F9D057A67
```

```
state [18].s_box:
0BFC2C1872B5E3EC5C65A7C7564D605B
08A0E0C912127741B7B0BA9930CBB1AA
```

```
state [18].s_row:
0BFCBA991212605B5C652C1830CB7741
08A0A7C772B5B1AAB7B0E0C9564DE3EC
```

```
state [18].m_col:
B6EE6D7593FB1EF2E18F0BEE31D7D437
E298CAB7EC12C78AB4B6B62E70F1A74B
```

```
state[18].xor_rkey (kt_round):
1B8B422CBE8B33829D84D44AC3F5BA47
8C0ED15F38418AC9FF33581DF119FC03
```

```
state [18].s_box:
FDCFD7D1F6CFE310307E01D68CEDF286
3F17F571F46B1DA380F7D079545CF84D
```

```
state [18].s_row:
FDCFD079F46BF286307ED7D1545C1DA3
3F1701D6F6CFF84D80F7F5718CEDE310
```

```
state [18].m_col:
AE64E3E5D4A91771995533643A3BC601
7B57D0BDA4354458932798CB6D716EDB
```

```
state[18].add_rkey (kt_round):
5BCA123F021A45E1156112092D5E3472
E9EDEBA57989919BDEAC86FFEE59CA23
```

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-256/512 З НЕПАРНИМИ ІНДЕКСАМИ

```
roundKey [0]:
F7BD9738CE49DDA80B9ABD79801EE821
8860FE42475C9F565CD8F433B4C989C4
```

```
roundKey[1].RotateLeft:
79801EE8218860FE42475C9F565CD8F4
33B4C989C4F7BD9738CE49DDA80B9ABD
```

```
roundKey[3].RotateLeft:
6445A8C043C025BC83FB4294B0A03392
```

A1F20BCAD2400B80A3E5EE106402037E

roundKey[5].RotateLeft:
E9F6E131E66F7AAF50A301148798CD52
A4004CD904D011D865E1E63E78353CDC

roundKey[7].RotateLeft:
92B4D70DD06ECB5266D3774630F330F2
1BBBB21C45B29987F5AEDC7C5049872A

roundKey[9].RotateLeft:
B4D7D11CC71DF00EB1A3C796AC1469E8
C6CE80238D535BC565CE0838DF30FC6A

roundKey[11].RotateLeft:
1AF15E077FCD97D8C55BC8365F3798FE
37B8947898575458552EB47D9C6246F0

roundKey[13].RotateLeft:
AD237BDBC9B9CFB69D14A77762477496
9AB2022675AE10A655AFA56FDD369FDE

roundKey[15].RotateLeft:
7957447C95CB026165A9DCA04A5D7092
BB878B24F53BA763DCCAF841C59B138A

roundKey[17].RotateLeft:
13962D5CDEE7367B3C3E7F37C96EABA3
07F3790E7919BE451A213F473E9D5D87

СФОРМОВАНИ ЦИКЛОВІ КЛЮЧІ КАЛИНА-256/512

round[0].rkey:
F7BD9738CE49DDA80B9ABD79801EE821
8860FE42475C9F565CD8F433B4C989C4

round[1].rkey:
79801EE8218860FE42475C9F565CD8F4
33B4C989C4F7BD9738CE49DDA80B9ABD

round[2].rkey:
400B80A3E5EE106402037E6445A8C043
C025BC83FB4294B0A03392A1F20BCAD2

round[3].rkey:
6445A8C043C025BC83FB4294B0A03392
A1F20BCAD2400B80A3E5EE106402037E

round[4].rkey:
D011D865E1E63E78353CDCE9F6E131E6
6F7AAF50A301148798CD52A4004CD904

round[5].rkey:
E9F6E131E66F7AAF50A301148798CD52
A4004CD904D011D865E1E63E78353CDC

round[6].rkey:
B29987F5AEDC7C5049872A92B4D70DD0
6ECB5266D3774630F330F21BBBB21C45

round[7].rkey:
92B4D70DD06ECB5266D3774630F330F2
1BBBB21C45B29987F5AEDC7C5049872A

round[8].rkey:

535BC565CE0838DF30FC6AB4D7D11CC7
1DF00EB1A3C796AC1469E8C6CE80238D

round[9].rkey:
B4D7D11CC71DF00EB1A3C796AC1469E8
C6CE80238D535BC565CE0838DF30FC6A

round[10].rkey:
575458552EB47D9C6246F01AF15E077F
CD97D8C55BC8365F3798FE37B8947898

round[11].rkey:
1AF15E077FCD97D8C55BC8365F3798FE
37B8947898575458552EB47D9C6246F0

round[12].rkey:
AE10A655AFA56FDD369FDEAD237BDBC9
B9CFB69D14A777624774969AB2022675

round[13].rkey:
AD237BDBC9B9CFB69D14A77762477496
9AB2022675AE10A655AFA56FDD369FDE

round[14].rkey:
3BA763DCCAF841C59B138A7957447C95
CB026165A9DCA04A5D7092BB878B24F5

round[15].rkey:
7957447C95CB026165A9DCA04A5D7092
BB878B24F53BA763DCCAF841C59B138A

round[16].rkey:
19BE451A213F473E9D5D8713962D5CDE
E7367B3C3E7F37C96EABA307F3790E79

round[17].rkey:
13962D5CDEE7367B3C3E7F37C96EABA3
07F3790E7919BE451A213F473E9D5D87

round[18].rkey:
5BCA123F021A45E1156112092D5E3472
E9EDEBA57989919BDEAC86FFEE59CA23

В.2.5 Розгортання 512-бітного ключа для шифрування 512-бітного блоку

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

ТЕСТ ФОРМУВАННЯ ПРОМІЖНОГО КЛЮЧА КТ

state [0]:
11000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000

state [0].k0:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F

303132333435363738393A3B3C3D3E3F

state [0].k1:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

state [0].add_rkey:

110102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

state [0].s_box:

F3BB9A4D6BCB452A713ADFB31790511F
6D152B3DC91CBB83795C71D56F5716BD
3EF6C002B4F4AD111F0F7A5E496DD166
9226C445D15DB794F4140E1A5810B2DF

state [0].s_row:

F314C45EB457BB1F71BB0E4549F41683
6D3A9A1AD16DADB7915DF4D585DD111
3E5C2BB36B10B7661FF6713D17CBB294
920FC0D5C99045DFF4267A026F1C512A

state [0].m_col:

16D6D3F4211375579D40CE70414C6086
9A3801A4784DB204C5766C433973AC84
EE9B1D8953D5CF421773C8EF40AFFCCD
738240440513C00A4A038A1805B8C578

state [0].xor_rkey:

16D7D1F7251673509549C47B4D416E89
8A2913B76C58A413DD6F7658256EB29B
CEBA3FAA77F0E9653F5AE2C46C82D2E2
43B372773126F63D723AB0233985FB47

state [0].s_box:

2CAFF517B688D631D79BAE7C6E6BDA9A
210FC2C53881073D62206CA1B6E3CA1D
3D2390E43BB6A7BEA17B130A38C9796B
371E05EC722254D224C8730219A28B86

state [0].s_row:

2CC8050A3BE3079AD7AF73EC38B6CA3D
219BF50272C9A71D620FAE17192279BE
3D20C27CB6A2546BA1236CC56E888BD2
377B90A1386BD686241E13E4B681DA31

state [0].m_col:

0DDCB649DCAD739C008F8CC961A5339
A3323726365533C6E27DA5BA21FF93B8
BEA186B0CA310A643F44DCC928AB8B26
87143B65B736CC2981759E6C2474A06F

state [0].add_rkey:

0DDDBD67A1CFDD40C81102D8A2276148
B34349394A6A49DDFA96BFD53D1CB2D7
DEC2A8D3EE56308B676D06F554D8B955
B7456D98EB6B0261B9AED8A760B1DEAE

state [0].s_box:

F09996AA118265B5FB159A8101AA81E9
BDF3EF08AB79EFFCE609439DA4F5CA5C

E39420F77319A677538C45A99639FA48
31337CA4B9E59A44EC781B043446E842

state [0].s_row:
F0787CA973F5EFE9FB991BA49619CAFC
BD159604B939A65CE6F39AAA34E5FA77
E309EF8111469A48539443080182E844
318C209DABAA6542EC3345F7A47981B5

state [0].m_col:
3FA1F2AA32DBC89CB851FB92A7DC1981
574F00BCF22AACAAB3DFFE72935E67DC
C277C3E723BEEBEE11409466A10F1DC2
59B929E49B1FCE6C68AB5251731CC4BB

KT:
3FA1F2AA32DBC89CB851FB92A7DC1981
574F00BCF22AACAAB3DFFE72935E67DC
C277C3E723BEEBEE11409466A10F1DC2
59B929E49B1FCE6C68AB5251731CC4BB

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-512/512 З ПАРНИМИ ІНДЕКСАМИ

state [0]:
3FA1F2AA32DBC89CB851FB92A7DC1981
574F00BCF22AACAAB3DFFE72935E67DC
C277C3E723BEEBEE11409466A10F1DC2
59B929E49B1FCE6C68AB5251731CC4BB

state [0].KT:
3FA1F2AA32DBC89CB851FB92A7DC1981
574F00BCF22AACAAB3DFFE72935E67DC
C277C3E723BEEBEE11409466A10F1DC2
59B929E49B1FCE6C68AB5251731CC4BB

state [0].id:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

state [0].tmv:
01000100010001000100010001000100
01000100010001000100010001000100
01000100010001000100010001000100
01000100010001000100010001000100

state[0].add_rkey (tmv):
40A1F3AA33DBC99CB951FC92A8DC1A81
584F01BCF32AADAAB4DFFF72945E68DC
C377C4E724BEECEE12409566A20F1EC2
5AB92AE49C1FCF6C69AB5351741CC5BB

state[0].add_rkey (kt_round):
40A2F5AD37E0CFA3C15A069EB4E92890
686013CF0740C3C1CCF8198EB07B86FB
E398E60A49E312163A69BF91CE3C4CF1
8AEA5C17D15405A4A1E48D8CB05903FB

state [0].s_box:
DC7186D0EE728265EF7B45C1AE0453C3
86E7C239591AF3C69021E427B30688C9
100B0A26CCD02B53D50D439F3D549D6D
21C6D383EACC22F61187ED21B349B5C9

```

state [0].s_row:
DC87D39FCC06F3C3EF71ED833DD088C6
867B8621EA542BC990E745D0B3CC9D53
1021C2C1EE49226DD50BE439AE72B5F6
210D0A27590482C911C64326B31A5365

state [0].m_col:
8E45E2C3CFB0C98AEC3E837E26EF899E
4CB51B9282975E0D2D3F1B46C2D72289
D20FB19A71FE55684F397124CF0CB35B
692F3223B5B5E31B23CD93A4A4590579

state[0].xor_rkey (kt_round):
CEE41169FC6B0016556F7FEC8E33931F
14FA1A2E71BDF3A799E0E43456894A55
1178757D5540B9865D79E4426D03AD99
339618C729AA2C774A66C0F5D045C0C2

state [0].s_box:
3D8717887CE593531620337489F7A8BD
C98A713C3325DB044072F14023D54E48
F3D46EDD161AFA63A962F16E7B92EE8B
6109622BBFF2DECABFC52A9F7335293

state [0].s_row:
3DFC626E16D5DBBD1687522B7B1A4E04
C92017A9BF92FA48408A3388F7FFEE63
F37271747C332D8BA9D4F13C89E552EC
61626E4033F79393AB09F1DD2325A853

state [0].m_col:
D9A5CC51BFED0CB0F904FFDF84CBC7C0
309BBE466D0559A44F00F34AB849ECEC
E5D0F97C2040E3113FCA48A6793D252F
AD8328CDC6BF327298852A44DED59D29

state[0].add_rkey (kt_round):
1947C0FCF2C8D64CB256FB722DA8E241
88EABF026130064F03E0F2BD4CA854C9
A848BE6445FECF00510ADE0C1C4D43F1
073D53B163DF01DF01317E9552F262E5

state[2].ShiftLeft (tmv):
02000200020002000200020002000200
02000200020002000200020002000200
02000200020002000200020002000200
02000200020002000200020002000200

state[2].Rotate (id):
08090A0B0C0D0E0F1011121314151617
18191A1B1C1D1E1F2021222324252627
28292A2B2C2D2E2F3031323334353637
38393A3B3C3D3E3F0001020304050607

state[2].add_rkey (tmv):
41A1F4AA34DBCA9CBA51FD92A9DC1B81
594F02BCF42AAEAAB5DF0073955E69DC
C477C5E725BEEDEE13409666A30F1FC2
5BB92BE49D1FD06C6AAB5451751CC6BB

state[2].add_rkey (kt_round):
49AAFE540E8D8ABCA620FA6BDF13198
71681CD71048CCC9D5002396B9838F03
ECA0EF1252EB1B1E4371C899D74455F9
93F2651FDA5C0EAC6AAC56547921CCC2

```

```

state [2].s_box:
  CCFF7450DCEC1BD9C1485907AAC22CA4
  3312CD5C6DD14BA3F8CED8EBEC00294D
  CF184446E203D4F537DC328B1ABDA991
  3A019CBD576F51B95BA955C877F64B93

state [2].s_row:
  CCA99C8BE2004BA4C1FF55BD1A0329A3
  334874C857BDD44DF8125950776FA9F5
  CFCECD07DCF651913718D85CAAEC4BB9
  3ADC44EB6DC21B935B013246ECD12CD9

state [2].m_col:
  3DA107CB26FE80A82C4087C231CAE663
  1ED5EEE87A6255FDF1896F96EA0F8715
  AC170CA45E6F3F29B51B66DA2FC6BCA0
  8AA7CD233E2FED068EF6D7BA07C00750

state[2].xor_rkey (kt_round):
  7C00F36112254A3496117A509816FDE2
  479AEC548E48FB5744566FE57F51EEC9
  6860C9437BD1D2C7A65BF0BC8CC9A362
  D11EE6C7A3303D6AE45D83EB72DCC1EB

state [2].s_box:
  14CEDB441DF44E40D315B13167880C6B
  329D5AC889D18B304219385A556346A3
  86E7260EF57A792B98D942693F771F15
  EA670A2BE57CDED8D0375DAD241FB6AD

state [2].s_row:
  14370A69F5638B6BD3CE5D2B3F7A4630
  3215DBADE57779A3429DB144247C1F2B
  86195A311D1FDE1598E738C867F4B6D8
  EAD9265A89884EADD067420E55D10C40

state [2].m_col:
  E366FD4FFD4EC8D7E9AE79A95CDF60D6
  8A1A9F7AF7B62ACF0D00A2306EEA8BDC
  5FE40C30DBEC156D107F858C6C7DC371
  853F0FE5AFD831BA9912F73892BD479A

state[2].add_rkey (kt_round):
  2408F2FA312A9374A300773C06BC7C57
  E369A136ECE1D879C2DFA2A30349F5B8
  235CD21701AB035C23BF1BF30F8DE233
  E0F83AC94DF8012703BE4B8A07DA0D56

state[4].ShiftLeft (tmv):
  04000400040004000400040004000400
  04000400040004000400040004000400
  04000400040004000400040004000400
  04000400040004000400040004000400

state[4].Rotate (id):
  101112131415161718191A1B1C1D1E1F
  202122232425262728292A2B2C2D2E2F
  303132333435363738393A3B3C3D3E3F
  000102030405060708090A0B0C0D0E0F

state[4].add_rkey (tmv):
  43A1F6AA36DBCC9CBC51FF92ABDC1D81
  5B4F04BCF62AB0AAB7DF0273975E6BDC
  C677C7E727BEEFEE15409866A50F21C2

```

5DB92DE49F1FD26C6CAB5651771CC8BB

```
state[4].add_rkey (kt_round):
53B208BE4AF0E2B3D46A19AEC7F93BA0
7B7026DF1A50D6D1DF082D9EC38B990B
F6A8F91A5CF325264D79D2A1E14C5F01
5DBA2FE7A324D87374B4605C8329D6CA
```

```
state [4].s_box:
5A80BAE2ABB6138E7E79E4427F7F4197
F530ADEF974C75B0C8E9E0C18CCF30B3
A7E434B7BCF09B9E6E62792E5216488D
A9237278E59E1B0C36385618600F751C
```

```
state [4].s_row:
5A38722EBCCF75977E80567852F030B0
F579BA18E5169BB3C830E4E2609E489E
A7E9AD42AB0F1B8D6EE4E0EF7FB6750C
A96234C1977F131C362379B78C4C418E
```

```
state [4].m_col:
CAC24443D9FDAE3B4FA09E1F5049581E
E35ECB7D1C9267ECA2AFE3F9234539C
73B8DD0332A7A45B087420894DCEDF09
345C4609743D78495B133BBBE591D650
```

```
state[4].xor_rkey (kt_round):
8963B2E9EF2662A7F3F1618DFB95459F
B811CFC1EAB8D7461DF5FC4C056A3840
B5CF1AE415194BB51D34B8EFE8C1FECB
69E56BEDEB22AA2537B86DEA928D1EEB
```

```
state [4].s_box:
7DFDCA958D228F04EDC281BFCA4700B2
1C1582C651E063F94BEDF823757909B5
E98271BA4D5C12504B08FE36126E74AF
F9BE1598B964CE51EEE07CE3690A16AD
```

```
state [4].s_row:
7DE015364D7963B2EDFD7C98125C09F9
1CC2CAE3B96E12B54B15819569647450
E9ED82BF8D0ACEAF4B82F8C6CA221651
F908712351478FADEEBEFEB75E00004
```

```
state [4].m_col:
753E43BC72A1BE60A0FBEC59A68BD033
B09E527189AECA2B52B8622936AAE180
FDBC7908D9008B0BD9AB4CCB535E461C
43272D775FD9DE3D2E8D723403752268
```

```
state[4].add_rkey (kt_round):
B8DF3967A97C8BFD5C4DECEC5168EEB4
0BEE562D80D97AD60998659CCD084D5D
C33441F000BF7AFAEEEBE431F96D67DE
A0E05A5BFFF8B0AA9A38C9857A91EA23
```

```
state[6].ShiftLeft (tmv):
08000800080008000800080008000800
08000800080008000800080008000800
08000800080008000800080008000800
08000800080008000800080008000800
```

```
state[6].Rotate (id):
18191A1B1C1D1E1F2021222324252627
28292A2B2C2D2E2F3031323334353637
```

```

38393A3B3C3D3E3F0001020304050607
08090A0B0C0D0E0F1011121314151617

state[6].add_rkey (tmv):
47A1FAAA3ADB09CC0510393AFDC2181
5F4F08BCFA2AB4AABBD0F06739B5E6FDC
CA77CBE72BBEF3EE19409C66A90F25C2
61B931E4A31FD66C70AB5A517B1CCCB

state[6].add_rkey (kt_round):
5FBA14C656F8EEB07225B6D30148A8
877832E72658E2D9EB1039A6CF93A513
02B1052368FB312E19419E69AD142BC9
69C23BEFAF2CE47B80BC6C648F31E2D2

state [6].s_box:
412394E6232146CDACB79B010DBB9249
46D4C4789A811335B9423B0782FE1C3D
5F46220286272C3CE06B40880B65C8A3
F994413676DFF17C9B1DA437FF261382

state [6].s_row:
411D418886FE1349AC23A4360B271C35
46B7943776652C3DB9D49BE6FFDFC83C
5F42C4012326F1A3E0463B780D21137C
F96B22079ABB46829B944002828192CD

state [6].m_col:
B67A0E9FD21250ABBD0E23A335227C80
DCEFAFB53A0855A4A7BF7F59E9A219C6
65BEEF27859E37BC3344495D89920186
DB9A137AEE40BDC3DF648F200823A701

state[6].xor_rkey (kt_round):
F1DBF435E8C980377D5F20309AFE5D01
83A0A709C022E10E1C60792A72FC761A
AFC924C0AE20C4522A04D53B209D2444
BA23229E4D5F6BAFAFCFD571733F6BBA

state [6].s_box:
54CD39CC127787949FCA4970B529368D
6018BC522F64FF196FE7FD5524C76CB7
76775CA7A231AEAE15EA5F1A3EB95CE5
F158C0C16ECA15C776825FBC28BC153F

state [6].s_row:
5482C01AA2C7FF8D9FCD5FC13E316C19
60CA39BC6EB9AEB76F1849CC28CA5CAE
76E7BC7012BC15E51577FD52B57715C7
F1EA5C552F29873F76585FA724643694

state [6].m_col:
33152CCC6FC589269BA791F36CC361FF
A636493F88189D511BA5AE6A8740130F
705702163B48A4FFA0E229C75F6D43A6
A2BB1F48C540107E279FF855463D0FE8

state[6].add_rkey (kt_round):
7AB62677AAA05AC35BF994861CA08380
058651FB824351FCD684B5DD229F82EB
3ACFCDFD660698EEB922C62D097D6868
0375512C6960E6EA974A53A7C159DBA3

state[8].ShiftLeft (tmv):
1000100010001000100010001000

```

```
10001000100010001000100010001000
10001000100010001000100010001000
10001000100010001000100010001000
```

```
state[8].Rotate (id):
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
```

```
state[8].add_rkey (tmv):
4FA102AB42DBD89CC8510B93B7DC2981
674F10BC022BBACAC3DF0E73A35E77DC
D277D3E733BEFBEE2140A466B10F2DC2
69B939E4AB1FDE6C78AB6251831CD4BB
```

```
state[8].add_rkey (kt_round):
6FC224CE6600FFC3F07A35BEE30958B0
978042EF3660F2E1FB1849AEDF9BB51B
D278D5EA37C301F62949AE71BD1C3BD1
79CA4BF7BF34F48390C47C6C9F39F2DA
```

```
state [8].s_box:
1E945C84A5CE670F812D78E2103AD06C
702AD736FAE7A0BBCAC5EF42C86AFBD5
0AD45FE3EE28D94CBF9B31BCAAF541B0
77D31217260839F1EB9A6089B114A0DE
```

```
state [8].s_row:
1E9A12BCEE6AA06C81946017AA28FBBB
702D5C8926F5D9D5CA2A7884B108414C
0AC5D7E2A51439B0BFD4EF3610CEA0F1
779B5F42FA3A67DEEBD331E3C8E7D00F
```

```
state [8].m_col:
CAE1A187CD510ACE3B509B084B41EFD4
8A1B2505425A463AC760D8AB10E72A88
EDD37DF598F9E2A993375FA409B70C25
F80AFD1B8FC4F3107E75D658700B7044
```

```
state[8].xor_rkey (kt_round):
8540A32C8F8AD252F301909BFC9DC655
ED5435B94071FA9004BFD6D8B3B95D54
3FA4AE12AB471947B277FBC2B8B821E7
91B3C4FF24DB2D7C06DEB409F317A4FF
```

```
state [8].s_box:
DA1A1FD1FF9C79AEEDBB271D7CB91948
D6CC7847DCDC21C36B057581BD0C36C8
A1EF314674FAE486CE978B931CE03C78
841EAE61B4CDE0286CAC1A52ED430761
```

```
state [8].s_row:
DAACAE93740C2148ED1A1A611CFA36C3
D6BB1F52B4E0E4C86BCC27D1EDCD3C86
A105781DFF43E078CEEF75477C9C0728
84973181DCB979616C1E8B46BDDC19AE
```

```
state [8].m_col:
BC9F8687DF5B65738B332152730F8125
6E1BC4FF84A7BB74F41E903F115CFF2A
677808B0FD2AFD13C7E13C57E2F0321F
937FEB552C21655A1753084922698EC6
```

```
state[8].add_rkey (kt_round):
```



```
0B41893222373E1053852CE52AECAAA6
D56AD4BB87D2771FB7FE9EB2B4BA7607
39F0DB9731E9F802E821E1BD930060E1
FC38253AD84043C78FFE6A9AA5856282
```

```
state[10].ShiftLeft (tmv):
20002000200020002000200020002000
20002000200020002000200020002000
20002000200020002000200020002000
20002000200020002000200020002000
```

```
state[10].Rotate (id):
28292A2B2C2D2E2F3031323334353637
38393A3B3C3D3E3F0001020304050607
08090A0B0C0D0E0F1011121314151617
18191A1B1C1D1E1F2021222324252627
```

```
state[10].add_rkey (tmv):
5FA112AB52DBE89CD8511B93C7DC3981
774F20BC122BCCAAD3DF1E73B35E87DC
E277E3E743BE0BEF3140B466C10F3DC2
79B949E4BB1FEE6C88AB7251931CE4BB
```

```
state[10].add_rkey (kt_round):
87CA3CD67E0817CC08834DC6FB1170B8
AF885AF74E680AEAD3E02076B7638DE3
EA80EDF24FCB19FE4151C679D52453D9
91D263FFD73C0C8CA8CC9474B7410AE3
```

```
state [10].s_box:
46D34C8708E9A36A71007DE6CA151EDA
761118170412DFE30D7249A831FDED76
512A06DC2785E4E0F2631920F89E9E35
842F77611A549F21C5E25024316BDF76
```

```
state [10].s_row:
46E2772027FDDFDA71D35061F885EDE3
76004C241A9EE4760D117D8731549EE0
517218E6086B9F35F22A4917CAE9DF21
846306A80415A376C52F19DC31121E6A
```

```
state [10].m_col:
4B6821B420E1DDFB76C1E1F1AB876850
C39E81955F9EA76725ABC2D21F6D76DC
B4F3F0C6FB0BF7C24E094E8407ED06D8
8463DDCAF9C5B7EA5D606ED3B3CF482B
```

```
state[10].xor_rkey (kt_round):
14C9331F723A3567AE90FA626C5B51D1
B4D1A1294DB56BCDF674DCA1AC33F100
56841321B8B5FC2D7F49FAE2C6E23B1A
FDDA942E42DA5986D5CB1C8220D3AC90
```

```
state [10].s_box:
C977E3BD24C878AAA27D211538D9D5B0
AE7A693E6EE11512A74A2A2E2DF70468
237EC22F1CE1F816559B216BD4DD41B7
8BDE503C83DE7B63F885CD103E74ABC3
```

```
state [10].s_row:
C985506B1CF715B0A277CD3CD4E10412
AE7DE31083DDF868A77A21BD3EDE4116
234A691524747BB7557E2A3E38C8AB63
8B9BC22E6ED978C3F8DE212F2DE1D5AA
```

```

state [10].m_col:
53B2E4EA39BC981EF12D779ECCD56A79
7C46E184D0A717F254F765F9D7AB7523
2E680ABA9F870952270431710BB5CC2E
364F69206CB7539B2668C622F6F50997

state[10].add_rkey (kt_round):
B253F7958C9781BBC97F923194B2A4FA
F3950141E3D2E39C27D7846C8B0AFDFF
10E0EDA1E34515415844E5D7CCC409F1
AF08B30428D74108AE1339748912EE52

state[12].ShiftLeft (tmv):
40004000400040004000400040004000
40004000400040004000400040004000
40004000400040004000400040004000
40004000400040004000400040004000

state[12].Rotate (id):
303132333435363738393A3B3C3D3E3F
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F

state[12].add_rkey (tmv):
7FA132AB72DB089DF8513B93E7DC5981
974F40BC322BECAAF3DF3E73D35EA7DC
027803E863BE2BEF5140D466E10F5DC2
99B969E4DB1F0E6DA8AB9251B31C04BC

state[12].add_rkey (kt_round):
AFD264DEA6103FD4308B75CE231A98C0
975042BF3630F2B1FBE8487EDF6BB5EB
128915FB77D341066959EE81FD2C7BE1
B9DA8B0700453494D0D4BC7CDF4932EB

state [12].s_box:
762FCC80984290FE92CF6E844F3628A7
704CD77AFA7CA090CAEC92ACC8E5FBAD
1DD5F4C93B74A54EF949467E8BDFE5BB
ECDEE92AA8337629F753BD28C89BC4AD

state [12].s_row:
7653E97E3BE5A0A7922FBD2A8B74FB90
70CFCC28A8DFA5ADCA4C6E80C833E54E
1DECD784989B76BBF9D5927A4F42C429
EC49F4ACFA3690ADF7DE46C9C87C28FE

state [12].m_col:
711137EC4357F74C4C99D75FE5FB82E6
4FD5D7DD10CF90C6CD49B1C265F4DC5F
99FAE49D8487380AA713FABCA4050248
6478E16E6FB53712BF96FF361BF72D8B

state[12].xor_rkey (kt_round):
0EB00547318CFFD1B4C8ECCC0227DB67
D89A976122E47C6C3E968FB1B6AA7B83
9B82E775E73913E5F6532EDA450A5F8A
FDC1888AB4AA397F173D6D67A8EB2937

state [12].s_box:
D88B2286720E67B0AE4F5A6A5FAA68AA
C49D2444A3876089BB0929908AFFE5F1
DEC97FA60C14C25AA75BD1DEE4D64843
8B6EC743AEFF3B5BAF107CAAC503A194

```

```

state [12].s_row:
D810C7DE0CFF60AAAE8B7C43E414E589
C44F22AAAE6C2F1BB9D5A86C5FF485A
DE09246A72033B43A7C929445F0EA15B
8B5B7F90A3AA6794AF6ED1A68A8768B0

state [12].m_col:
1D9A540E7A473229639F698253924D59
CB69776EC9BF4BB441ED26F974F88172
0489BC5F24FAE337705DAA7A1A725A4E
36C6F7D88A2471A33BA147BDAFC61D48

state[12].add_rkey (kt_round):
9C3B87B9EC223BC65BF1A4153B6FA7DA
62B9B72AFCEA375F34CD656C4857294F
0601C04788B80F27C19D7EE1FB81B710
CF7F61BD66447F10E34CDA0E63E32104

state[14].ShiftLeft (tmv):
80008000800080008000800080008000
80008000800080008000800080008000
80008000800080008000800080008000
80008000800080008000800080008000

state[14].Rotate (id):
38393A3B3C3D3E3F0001020304050607
08090A0B0C0D0E0F1011121314151617
18191A1B1C1D1E1F2021222324252627
28292A2B2C2D2E2F3031323334353637

state[14].add_rkey (tmv):
BFA172ABB2DB489D38527B9327DD9981
D74F80BC722B2CAB33E07E73135FE7DC
427843E8A3BE6BEF9140146721109DC2
D9B9A9E41B204E6DE8ABD251F31C44BC

state[14].add_rkey (kt_round):
F7DAAE6EE1887DC38537D962BE29F88
DF588AC77E383ABA43F190862774FDF3
5A915D03C0DB890EB161368A4535C3E9
01E3D30F484D7C9C18DD048527527AF3

state [14].s_box:
2ADEAB7D73C58DA5F45BAFEBE1DD8305
C8811D2B089F0E3F37C227630E4A0CF0
6693364D2FCDF719BE2BB743E45DF395
43D0BF1F9C9560FB7999988F0E8EB1F0

state [14].s_row:
2A99BF432F4A0E05F4DE981FE4CD0C3F
C85BAB8F9C5DF7F03781AF7D0E95F319
66C21DEB738E6095BE93272BE1C5B1FB
432B366308DD8DF079D0B74D0E9F83A5

state [14].m_col:
73A6C3E7610EEE44C88552B4B4D58D21
7ED26D83848A3DAF4CEB57279DC3C6F2
C9DCA4E1EC193A2FB92C21E71DB6D421
32B3DE256DE1952AA009D3BFBFF37866

state[14].xor_rkey (kt_round):
CC07B14CD3D5A6D9F0D72927930814A0
A99DED3FF6A111047F0B29548E9C212E
8BA4E7094FA751C0286C35803CA649E3

```

EB0A77C176C1DB4748A201EE4CEF3CDA

state [14].s_box:

90C1F9230DB38A3581AFA1113AE99497
02B906DFA732177355B2A1C889073C3C
B0EF7F5227A0D5A71F8978345870EF76
B9D67EC6B26E68869C71D93B8F594CDE

state [14].s_row:

90717E342707179781C1D9C658A03C73
02AFF93BB270D53C55B9A1238F6EEFA7
B0B206110D5968761FEFA1DF3AB34C86
B9897FC8A7E98ADE9CD6785289329435

state [14].m_col:

7A3E153B84D79DF76422D3188D0036CD
89EC14A9B405A99EB42CD38CDD7A69B8
6ED6FC65C39CEA09AB7DB0E3D5418F75
B56093F9DF9C3EC31233698A0A95E737

state[14].add_rkey (kt_round):

39E087E636B3E6949C744EACB4DDCF4E
603C95652731D549E70C5200F1D95095
B04E404E675B56F93CBEC44AF7512C38
8E1A3DDEFB8C8C30FADE3BDCFDB12BF4

state[16].ShiftLeft (tmv):

00010001000100010001000100010001
00010001000100010001000100010001
00010001000100010001000100010001
00010001000100010001000100010001

state[16].Rotate (id):

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

state[16].add_rkey (tmv):

3FA2F2AB32DCC89DB852FB93A7DD1982
575000BDF22BACABB3E0FE73935F67DD
C278C3E823BFEBEF11419467A1101DC3
59BA29E59B20CE6D68AC5252731DC4BC

state[16].add_rkey (kt_round):

3FA3F4AE36E1CEA4C05B059FB3EA2791
676112D00641C2C2CBF9188FAF7C85FC
E299E50B48E41117396ABE92CD3D4BF2
89EB5B18D05504A5A0E58C8DAF5A02FC

state [16].s_box:

A14B3942FA2C84F62FD922B2BDC6859F
532B2BE76C6B08935E7F620976A43F57
648F47B39C8717831979DDB6201012DC
7D039713F73C987578BEECBF767B9A57

state [16].s_row:

A1BE97B69CA4089F2F4BEC1320873F93
53D939BFF71017575E2B2242763C1283
647F2BB2FA7B98DC198F62E7BD2C9A75
7D7947096CC684577803DDB3766B85F6

state [16].m_col:

4DDCF43A6D773018EF748CD8C7BBEB3C
47752AABDCB35412CA727906585AB287

```

12C5517DA4DF31F4C738149A690FE6D3
586F65FA7BDB2C92F5AE9D2E728830A6

state[16].xor_rkey (kt_round):
727E06915FABF8855726774B6066F2BE
10252A162E98F8B979928775CB05D55A
D0BD92958760DA1BD67980FDC81FFB10
01D54C1FE0FBE2FF9D02CF7C0195F41A

state [16].s_box:
2483459F41C38C8F2B227E8534FCA0E2
6DF47A53930B8C47771B8DA65ECB5F41
F72599C246E73DD55062871BF8B8D8B22
43B39DBDAC27136130EB8228434739B7

state [16].s_row:
24EB9D1B46CB8CE22B8382BDFBE75F47
6D224528AC8D3D4177F47E9F43278BD5
F71B7A854147132250258D5334C33961
436299A693FC8CB730B387C25E0BA08F

state [16].m_col:
A15A1B6F0C08332BC75942216A4DB114
81A23E9C4C59152192F8D336907CE627
AAF627209F75339B9E394E91FA1A3C80
FBE3E6B967074D4A51727FAF4DC73D71

state[16].add_rkey (kt_round):
E0FC0D1B3FE4FBC87FAC3DB5112BCB96
D8F23E593F85C1CC45D9D2AA23DC4D05
6C6FEB08C3341F8BAF7AE2F89B2B5943
549E109F03281BB8B91ED201C1E4012E

state[18].ShiftLeft (tmv):
00020002000200020002000200020002
00020002000200020002000200020002
00020002000200020002000200020002
00020002000200020002000200020002

state[18].Rotate (id):
08090A0B0C0D0E0F1011121314151617
18191A1B1C1D1E1F2021222324252627
28292A2B2C2D2E2F3031323334353637
38393A3B3C3D3E3F0001020304050607

state[18].add_rkey (tmv):
3FA3F2AC32DDC89EB853FB94A7DE1983
575100BEF22CACACB3E1FE74936067DE
C279C3E923C0EBF011429468A1111DC4
59BB29E69B21CE6E68AD5253731EC4BD

state[18].add_rkey (kt_round):
47ACFCB73EEAD6ADC8640DA8BBF32F9A
6F6A1AD90E4ACACBD3022198B7858D05
EAA2ED1450ED19204173C69BD54653FB
91F46321D85E0CAE68AE54567723CAC4

state [18].s_box:
32A9F8C5BBC675D0FB96DC4999F0728C
1E797135D868B0AF0DEB3CA431A2ED4B
5171062D2EFBE458F26C191DF8AB9EC9
845A772FC4609F4286784DD33B58B00A

state [18].s_row:
3278771D2EA2B08CFBA94D2FF8FBEDAF

```

```

1E96F8D3C4ABE44B0D79DCC53B609E58
51EB7149BB589FC9F2713C3599C6B042
846C06A4D8F0750A865A192D316872D0

```

```

state [18].m_col:
5AFDD8B9FE68517F395F11D6ACA5C7229
60D59FEA6DF1ECEC228D3D6CA146B08A
DED22CC77258CA954AF04D63CF210A72
B8506870076CA7C9509504B950905063

```

```

state[18].xor_rkey (kt_round):
655E2933D458DF6D2DA2E6FE6D826BAA
37849F549FDD4040916CC3183226D754
1CABEF2E519821655BB2D90B6E3017B6
E1EB41969C4D69A7383856EA238E94DE

```

```

state [18].s_box:
8860A1457E81919CD2710AE07BC915E4
EE7E83C8B19925B58489F3139E2263C8
6FC3443CE70B3CBE0F8023B3C37CA301
5203A5EB5D95B804F49F55E34F3D5080

```

```

state [18].s_row:
889FA5B3E72225E4D26055EBC30B63B5
EE71A1E35D7C3CC8847E0A454F95A3BE
6F8983E07E3DB8010FC3F3C87B815004
52804413B1C99180F403233C9E99159C

```

```

state [18].m_col:
44D7E6EB6B2C07F3F3DA620F31A586D4
175714B7D6D5862E0A7138BB03C2807C
E1D7643667817B597F2594C6DF3FA7E4
0F9F93D617C6D50EB0B467633A8AA766

```

```

state[18].add_rkey (kt_round):
837AD9989E09D091AB2E5EA4D883A057
6EA81475C90233DBBD5237309722E85A
A35128208B41674A9067282F8151C4A8
685ABDBC3E7A37D1862BAB6ADA86B24

```

ТЕСТ ФОРМУВАННЯ ЦИКЛОВИХ КЛЮЧІВ КАЛИНА-512/512 З НЕПАРНИМИ ІНДЕКСАМИ

```

roundKey [0]:
1947C0FCF2C8D64CB256FB722DA8E241
88EABF026130064F03E0F2BD4CA854C9
A848BE6445FECF00510ADE0C1C4D43F1
073D53B163DF01DF01317E9552F262E5

```

```

roundKey[1].RotateLeft:
026130064F03E0F2BD4CA854C9A848BE
6445FECF00510ADE0C1C4D43F1073D53
B163DF01DF01317E9552F262E51947C0
FCF2C8D64CB256FB722DA8E24188EABF

```

```

roundKey[3].RotateLeft:
36ECE1D879C2DFA2A30349F5B8235CD2
1701AB035C23BF1BF30F8DE233E0F83A
C94DF8012703BE4B8A07DA0D562408F2
FA312A9374A300773C06BC7C57E369A1

```

```

roundKey[5].RotateLeft:
2D80D97AD60998659CCD084D5DC33441
F000BF7AFAEEEBE431F96D67DEA0E05A
5BFFF8B0AA9A38C9857A91EA23B8DF39
67A97C8BFD5C4DECEC5168EEB40BEE56

```

roundKey[7].RotateLeft:
 FB824351FCD684B5DD229F82EB3ACFCD
 FD660698EEB922C62D097D6868037551
 2C6960E6EA974A53A7C159DBA37AB626
 77AAA05AC35BF994861CA08380058651

roundKey[9].RotateLeft:
 BB87D2771FB7FE9EB2B4BA760739F0DB
 9731E9F802E821E1BD930060E1FC3825
 3AD84043C78FFE6A9AA58562820B4189
 3222373E1053852CE52AECAAA6D56AD4

roundKey[11].RotateLeft:
 41E3D2E39C27D7846C8B0AFDFF10E0ED
 A1E34515415844E5D7CCC409F1AF08B3
 0428D74108AE1339748912EE52B253F7
 958C9781BBC97F923194B2A4FAF39501

roundKey[13].RotateLeft:
 2AFCEA375F34CD656C4857294F0601C0
 4788B80F27C19D7EE1FB81B710CF7F61
 BD66447F10E34CDA0E63E321049C3B87
 B9EC223BC65BF1A4153B6FA7DA62B9B7

roundKey[15].RotateLeft:
 652731D549E70C5200F1D95095B04E40
 4E675B56F93CBEC44AF7512C388E1A3D
 DEFBB8C30FADE3BDCFDB12BF439E087
 E636B3E6949C744EACB4DDCF4E603C95

roundKey[17].RotateLeft:
 593F85C1CC45D9D2AA23DC4D056C6FEB
 08C3341F8BAF7AE2F89B2B5943549E10
 9F03281BB8B91ED201C1E4012EE0FC0D
 1B3FE4FBC87FAC3DB5112BCB96D8F23E

СФОРМОВАНІ ЦИКЛОВІ КЛЮЧІ КАЛИНА-512/512

round[0].rkey:
 1947C0FCF2C8D64CB256FB722DA8E241
 88EABF026130064F03E0F2BD4CA854C9
 A848BE6445FECF00510ADE0C1C4D43F1
 073D53B163DF01DF01317E9552F262E5

round[1].rkey:
 026130064F03E0F2BD4CA854C9A848BE
 6445FECF00510ADE0C1C4D43F1073D53
 B163DF01DF01317E9552F262E51947C0
 FCF2C8D64CB256FB722DA8E24188EABF

round[2].rkey:
 2408F2FA312A9374A300773C06BC7C57
 E369A136ECE1D879C2DFA2A30349F5B8
 235CD21701AB035C23BF1BF30F8DE233
 E0F83AC94DF8012703BE4B8A07DA0D56

round[3].rkey:
 36ECE1D879C2DFA2A30349F5B8235CD2
 1701AB035C23BF1BF30F8DE233E0F83A
 C94DF8012703BE4B8A07DA0D562408F2
 FA312A9374A300773C06BC7C57E369A1

round[4].rkey:
 B8DF3967A97C8BFD5C4DECEC5168EEB4

0BEE562D80D97AD60998659CCD084D5D
C33441F000BF7AFAEEEBE431F96D67DE
A0E05A5BFFF8B0AA9A38C9857A91EA23

round[5].rkey:

2D80D97AD60998659CCD084D5DC33441
F000BF7AFAEEEBE431F96D67DEA0E05A
5BFFF8B0AA9A38C9857A91EA23B8DF39
67A97C8BFD5C4DECEC5168EEB40BEE56

round[6].rkey:

7AB62677AAA05AC35BF994861CA08380
058651FB824351FCD684B5DD229F82EB
3ACFCDFD660698EEB922C62D097D6868
0375512C6960E6EA974A53A7C159DBA3

round[7].rkey:

FB824351FCD684B5DD229F82EB3ACFCD
FD660698EEB922C62D097D6868037551
2C6960E6EA974A53A7C159DBA37AB626
77AAA05AC35BF994861CA08380058651

round[8].rkey:

0B41893222373E1053852CE52AECAAA6
D56AD4BB87D2771FB7FE9EB2B4BA7607
39F0DB9731E9F802E821E1BD930060E1
FC38253AD84043C78FFE6A9AA5856282

round[9].rkey:

BB87D2771FB7FE9EB2B4BA760739F0DB
9731E9F802E821E1BD930060E1FC3825
3AD84043C78FFE6A9AA58562820B4189
3222373E1053852CE52AECAAA6D56AD4

round[10].rkey:

B253F7958C9781BBC97F923194B2A4FA
F3950141E3D2E39C27D7846C8B0AFDFF
10E0EDA1E34515415844E5D7CCC409F1
AF08B30428D74108AE1339748912EE52

round[11].rkey:

41E3D2E39C27D7846C8B0AFDFF10E0ED
A1E34515415844E5D7CCC409F1AF08B3
0428D74108AE1339748912EE52B253F7
958C9781BBC97F923194B2A4FAF39501

round[12].rkey:

9C3B87B9EC223BC65BF1A4153B6FA7DA
62B9B72AFCEA375F34CD656C4857294F
0601C04788B80F27C19D7EE1FB81B710
CF7F61BD66447F10E34CDA0E63E32104

round[13].rkey:

2AFCEA375F34CD656C4857294F0601C0
4788B80F27C19D7EE1FB81B710CF7F61
BD66447F10E34CDA0E63E321049C3B87
B9EC223BC65BF1A4153B6FA7DA62B9B7

round[14].rkey:

39E087E636B3E6949C744EACB4DDCF4E
603C95652731D549E70C5200F1D95095
B04E404E675B56F93CBEC44AF7512C38
8E1A3DDEFB8C8C30FADE3BDCFD12BF4

round[15].rkey:


```
652731D549E70C5200F1D95095B04E40
4E675B56F93CBEC44AF7512C388E1A3D
DEFB8C8C30FADE3BDCFDB12BF439E087
E636B3E6949C744EACB4DDCF4E603C95
```

```
round[16].rkey:
E0FC0D1B3FE4FBC87FAC3DB5112BCB96
D8F23E593F85C1CC45D9D2AA23DC4D05
6C6FEB08C3341F8BAF7AE2F89B2B5943
549E109F03281BB8B91ED201C1E4012E
```

```
round[17].rkey:
593F85C1CC45D9D2AA23DC4D056CFEB
08C3341F8BAF7AE2F89B2B5943549E10
9F03281BB8B91ED201C1E4012EE0FC0D
1B3FE4FBC87FAC3DB5112BCB96D8F23E
```

```
round[18].rkey:
837AD9989E09D091AB2E5EA4D883A057
6EA81475C90233DBBD5237309722E85A
A35128208B41674A9067282F8151C4A8
685ABDBC3E7A37D1862BAB6ADA86B24
```

В.2.6 Шифрування 128-бітного блоку з використанням 128-бітового ключа

ТЕСТ ЗАШИФРУВАННЯ КАЛИНА-128/128

```
KEY:
000102030405060708090A0B0C0D0E0F
PLAINTEXT:
101112131415161718191A1B1C1D1E1F
```

```
round [0].rkey:
16505E6B9B3AB1E6865B77DCE082A0F4
```

```
round [0].add_rkey:
2661707EAF4FC7FD9E7491F7FC9FBE13
```

```
round [1].s_box:
9A2B1EAC76EE891B914ACF177C98DD3D
```

```
round [1].s_row:
9A2B1EAC7C98DD3D914ACF1776EE891B
```

```
round [1].m_col:
16CEDEE8D9990F9E25B506F042D3B305
```

```
round [1].r_key:
E6865B77DCE082A0F416505E6B9B3AB1
```

```
round [1].xor_rkey:
F048859F05798D3ED1A356AE294889B4
```

```
round [2].s_box:
81D13FB27562EDE1EA4B5542BFD1F76F
```

```
round [2].s_row:
81D13FB2BFD1F76FEA4B55427562EDE1
```

```
round [2].m_col:
32F172C7E2D2E1C93B4D13958FBCE28D
```

```
round [2].r_key:
7E70876EAE4984768AAAA00A7C93EC42
```

```
round [2].xor_rkey:
  4C81F5A94C9B65BFB1E7B39FF32F0ECF

round [3].s_box:
  8FDA86338F6A9C7ABEA63AB2ED4D5139

round [3].s_row:
  8FDA8633ED4D5139BEA63AB28F6A9C7A

round [3].m_col:
  044E672502E945D313F24197773D4547

round [3].r_key:
  768AAAA00A7C93EC427E70876EAE4984

round [3].xor_rkey:
  72C4CD850895D63F518C311019930CC3

round [4].s_box:
  249A648F714775DFE70E2C22E0FE9F0F

round [4].s_row:
  249A648FE0FE9F0FE70E2C22714775DF

round [4].m_col:
  73EC521DA9BAF9777A44212456FE0215

round [4].r_key:
  45CED4C51E9140F53E7276820F0BD9FE

round [4].xor_rkey:
  362286D8B72BB982443657A659F5DBEB

round [5].s_box:
  FA64888131B1FA104244C60765ED68AD

round [5].s_row:
  FA64888165ED68AD4244C60731B1FA10

round [5].m_col:
  5DCBF7EE9765340D700AB86C7E3CFCBC

round [5].r_key:
  F53E7276820F0BD9FE45CED4C51E9140

round [5].xor_rkey:
  A8F58598156A3FD48E4F76B8BB226DFC

round [6].s_box:
  C5ED3FA44D7990FE89EE6CDA99647C57

round [6].s_row:
  C5ED3FA499647C5789EE6CDA4D7990FE

round [6].m_col:
  9EDCE2CB1E774F272D2C66281402B14F

round [6].r_key:
  8C77EE227900C462515F66320560C4B1

round [6].xor_rkey:
  12AB0CE967778B457C73001A116275FE

round [7].s_box:
```

1DC39F955397E9F4146C93B7F3486EE0

round [7].s_row:
1DC39F95F3486EE0146C93B75397E9F4

round [7].m_col:
44B90F555C682F068FDB6918B7108ED5

round [7].r_key:
62515F66320560C4B18C77EE227900C4

round [7].xor_rkey:
26E850336E6D4FC23E571EF695698E11

round [8].s_box:
9AEC1045C38C3593BBA1164CD70D8003

round [8].s_row:
9AEC1045D70D8003BBA1164CC38C3593

round [8].m_col:
1073FCB6ECF68F31BCB77E752220169C

round [8].r_key:
0A9872E25CD2B0B8AA879A2086A66DD8

round [8].xor_rkey:
1AEB8E54B0243F891630E455A4867B44

round [9].s_box:
970380C8B39E909A2C7CF1480055E5E5

round [9].s_row:
970380C80055E5E52C7CF148B39E909A

round [9].m_col:
375DCC2C800C45F61DD9C471E522E0A6

round [9].r_key:
B8AA879A2086A66DD80A9872E25CD2B0

round [9].xor_rkey:
8FF74BB6A08AE39BC5D35C03077E3216

round [10].s_box:
FF661201789C581D0374D34D5983C453

round [10].s_row:
FF6612015983C4530374D34D789C581D

round [10].m_col:
2A996BD4E2BFE707EBBDF763CBFA64A5

round [10].add_rkey:
81BF1C7D779BAC20E1C9EA39B4D2AD06

CIPHERTEXT:
81BF1C7D779BAC20E1C9EA39B4D2AD06

ТЕСТ РОЗШИФРУВАННЯ КАЛИНА-128/128

KEY:
0F0E0D0C0B0A09080706050403020100

CIPHERTEXT:
1F1E1D1C1B1A19181716151413121110

round [10].rkey:
45D32764EB4B669ED8A3B2E73888CC77

round [10].sub_rkey:
DA4AF5B72FCEB2793F72622CDA894498

round [10].m_col:
AFF9B83FCDB4966CB66A08CEB5CB2EAD

round [10].s_row:
AFF9B83FB5CB2EADB66A08CECDB4966C

round [10].s_box:
17AF69BA9A0547EB259BC23A8813BDB0

round [9].r_key:
2479F950B52187E2AE8BD65CCC7452D0

round [9].xor_rkey:
33D690EA2F24C0098B1014664467EF60

round [9].m_col:
57462621E191A0381BF38C63CF30B906

round [9].s_row:
57462621CF30B9061BF38C63E191A038

round [9].s_box:
DAB1C98CEC7066C58D43F8862B4EF241

round [8].r_key:
8BD65CCC7452D02479F950B52187E2AE

round [8].xor_rkey:
516795409822B6E1F4BAA8330AC910EF

round [8].m_col:
9642B19B65CF2889BDE6680A472ACF71

round [8].s_row:
9642B19B472ACF71BDE6680A65CF2889

round [8].s_box:
54107A685E80915FB3ADDBC4598B986C

round [7].r_key:
028F414771A7C56F54CA78E33B34F568

round [7].xor_rkey:
569F3B2F2F275430E767A32762BF6D04

round [7].m_col:
A6CDDEE3A0583E57AC8E7CD65D9B2B3F

round [7].s_row:
A6CDDEE35D9B2B3FAC8E7CD6A0583E57

round [7].s_box:
AADB3DEA9C4912BAE0526D4AA7239CFC

round [6].r_key:
CA78E33B34F568028F414771A7C56F54

round [6].xor_rkey:

60A3DED1A8BC7AB86F132A3B00E6F3A8

round [6].m_col:
8D530B8B7402299F3A503F7DF2AB32C7

round [6].s_row:
8D530B8BF2AB32C73A503F7D7402299F

round [6].s_box:
EFD471994146C8AF93D085E6AB2A8F91

round [5].r_key:
7F6553DB7E6FD3F87EF21749B0A405C2

round [5].xor_rkey:
90B122423F291B57ED2292AF1B8E8A53

round [5].m_col:
401954D8D158D58A39F7F8FC5629A7BD

round [5].s_row:
401954D85629A7BD39F7F8FCD158D58A

round [5].s_box:
9956F66AFEFEE91F1F33FCDD34235119

round [4].r_key:
F21749B0A405C27F6553DB7E6FD3F87E

round [4].xor_rkey:
6B41BFDA5AFB2B607A6027A35BF0A967

round [4].m_col:
4A97D857436E3AE986CA521D43136ED5

round [4].s_row:
4A97D85743136ED586CA521D436E3AE9

round [4].s_box:
4B7723FC0106751B685FC09B01C1B348

round [3].r_key:
D802781E471AB0CAFA9845CC2A6036C0

round [3].xor_rkey:
93755BE2461CC5D192C785572BA18588

round [3].m_col:
9622BE6806AF0D7EDED06D2B82536AF3

round [3].s_row:
9622BE6882536AF3DED06D2B06AF0D7E

round [3].s_box:
5426C500CFD409329BE384C703D7B681

round [2].r_key:
9845CC2A6036C0D802781E471AB0CAFA

round [2].xor_rkey:
CC63092AAFE2C9EA999B9A8019677C7B

round [2].m_col:
AA4DF979D644A69FCA4C64030DEF4808

```

round [2].s_row:
AA4DF9790DEF4808CA4C6403D644A69F

round [2].s_box:
BD2FB11DD3A45F39FB50CD11ED363091

round [1].r_key:
AD2D1BB5A3ADDF1F3B9CED1432A9A3D7

round [1].xor_rkey:
1002AAA870098026C0CC2005DF9F9346

round [1].m_col:
D85F982C138E21465D9E7EFE81F940F3

round [1].s_row:
D85F982C81F940F35D9E7EFE138E2146

round [1].s_box:
0E7F045EF0AF9E329C2477D4E652FA12

round [0].sub_rkey:
7291EF2B470CC7846F09C2303973DAD7

PLAINTEXT:
7291EF2B470CC7846F09C2303973DAD7

```

В.2.7 Шифрування 128-бітного блоку з використанням 256-бітового ключа

```

ТЕСТ ЗАШИФРУВАННЯ КАЛИНА-128/256

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

PLAINTEXT:
202122232425262728292A2B2C2D2E2F

round [0].rkey:
57C816EB3F7E12DEED2C6B56E6B5BE1A

round [0].add_rkey:
77E9380E64A338051556958112E3EC49

round [1].s_box:
3B0409196A4B094B4D190F7E1DD05A4F

round [1].s_row:
3B0409191DD05A4F4D190F7E6A4B094B

round [1].m_col:
837E4D092BF2EC90C77690C58B4D640A

round [1].r_key:
DEED2C6B56E6B5BE1A57C816EB3F7E12

round [1].xor_rkey:
5D9361627D14592EDD2158D360721A18

round [2].s_box:
A9FE81159F657B3C62F6D0F734B77113

round [2].s_row:

```

A9FE811534B7711362F6D0F79F657B3C

round [2].m_col:
D307A5B6D309C3F1979C20CC8430F3DE

round [2].r_key:
D8069A7D889ACD80CD3184456CCCAE6F

round [2].xor_rkey:
0B013FCB5B930E715AADA489E8FC5DB1

round [3].s_box:
95BB90AF0FFE51BC66E6079A12C73690

round [3].s_row:
95BB90AF12C7369066E6079A0FFE51BC

round [3].m_col:
AB6B52A69B5A923227E8DDB17B13599B

round [3].r_key:
80CD3184456CCCAE6FD8069A7D889ACD

round [3].xor_rkey:
2BA66322DE365E9C4830DB2B069BC356

round [4].s_box:
E170770DE344E6FB9C7C685E6C6AF3D3

round [4].s_row:
E170770D6C6AF3D39C7C685EE344E6FB

round [4].m_col:
84958A6BC7C60F15E6296722E488975A

round [4].r_key:
C361CC973513411A82324D2B6742F3FE

round [4].xor_rkey:
47F446FCF2D54E0F641B2A0983CA64A4

round [5].s_box:
325AC357C0B3CB1F6ABA7A5260D3CCF6

round [5].s_row:
325AC35760D3CCF66ABA7A52C0B3CB1F

round [5].m_col:
819B71BCE05B75E3F99EF1714E4D3B42

round [5].r_key:
1A82324D2B6742F3FEC361CC97351341

round [5].xor_rkey:
9B1943F1CB3C3710075D90BDD9782803

round [6].s_box:
DE5C036D5E54B422593727A207D4534D

round [6].s_row:
DE5C036D07D4534D593727A25E54B422

round [6].m_col:
9724FDB357EFCABBFBCCA18E7148854C

round [6].r_key:
8310698C65CF80A409EF6FAABEB80F56

round [6].xor_rkey:
1434943F32204A1FF223CE24CFF08A1A

round [7].s_box:
C90850DF9E314EBDC05884ED82B61DB7

round [7].s_row:
C90850DF82B61DB7C05884ED9E314EBD

round [7].m_col:
51E8912C2A9B61CAC023604CD2F27536

round [7].r_key:
A409EF6FAABEB80F568310698C65CF80

round [7].xor_rkey:
F5E17E438025D9C596A070255E97BAB6

round [8].s_box:
442C5E0E9BF42306D3181E514786F201

round [8].s_row:
442C5E0E4786F201D3181E519BF42306

round [8].m_col:
8C5B243390BA9222A3D5043A43629F06

round [8].r_key:
C6D5C4C381461A7B034D691842901510

round [8].xor_rkey:
4A8EE0F011FC8859A0986D2201F28A16

round [9].s_box:
AB3DF664F3C7C792780B7C0D43011D53

round [9].s_row:
AB3DF66443011D53780B7C0DF3C7C792

round [9].m_col:
DD155C0CB27E38249147CAF0DA1DEA9D

round [9].r_key:
7B034D691842901510C6D5C4C381461A

round [9].xor_rkey:
A6161165AA3CA83181811F34199CAC87

round [10].s_box:
988817BEA654205D4CDAE140E007ABA0

round [10].s_row:
988817BEE007ABA04CDAE140A654205D

round [10].m_col:
68FBCA337ED2DCDDA13989273391189D

round [10].r_key:
84D0F82146C8BDF9B2B3707B4D49387E

round [10].xor_rkey:
EC2B3212381A6124138AF95C7ED820E3


```
round [11].s_box:
    CFB1C446F43681EDCB9C341808394976

round [11].s_row:
    CFB1C44608394976CB9C3418F43681ED

round [11].m_col:
    3A0461D2E3A0619EDF1A301B0591F3BA

round [11].r_key:
    F9B2B3707B4D49387E84D0F82146C8BD

round [11].xor_rkey:
    C3B6D2A298ED28A6A19EE0E324D73B07

round [12].s_box:
    8CB879F867FB530711B0F676B4AF412A

round [12].s_row:
    8CB879F8B4AF412A11B0F67667FB5307

round [12].m_col:
    321CE7907F7A3DC259BFA0E4AB9B98F8

round [12].r_key:
    43FADB28A0D1D42BBFF92FF9794546B3

round [12].xor_rkey:
    71E63CB8DFABE9E9E6468F1DD2DEDE4B

round [13].s_box:
    335E4CDAC8C3A79513AB29790AAACE885

round [13].s_row:
    335E4CDA0AAACE88513AB2979C8C3A795

round [13].m_col:
    C5BECE42A6B7CC87CEE9BB9AFC3EF122

round [13].r_key:
    2BBFF92FF9794546B343FADB28A0D1D4

round [13].xor_rkey:
    EE01376D5FCE89C17DAA4141D49E20F6

round [14].s_box:
    73BBB49C41F2F7C69FFFA5387EB0494C

round [14].s_row:
    73BBB49C7EB0494C9FFFA53841F2F7C6

round [14].m_col:
    95CD566091D32765B72653E17180F381

round [14].add_rkey:
    58EC3E091000158A1148F7166F334F14

CIPHERTEXT:
    58EC3E091000158A1148F7166F334F14

ТЕСТ РОЗШИФРУВАННЯ КАЛИНА-128/256

KEY:
    1F1E1D1C1B1A19181716151413121110
```

0F0E0D0C0B0A09080706050403020100

CIPHERTEXT:

2F2E2D2C2B2A29282726252423222120

round [14].rkey:

44FEDFC4E5CDB7AA3F52FCDD9538EF2

round [14].sub_rkey:

EB2F4D67455C717DE8D3284649CE922D

round [14].m_col:

07364CA471C4E367E417C0B352317200

round [14].s_row:

07364CA452317200E417C0B371C4E367

round [14].s_box:

D91A3C98E1202FB2450E220B08943378

round [13].r_key:

56DD948709B40D1FA85F1E30B4FE3E4E

round [13].xor_rkey:

8FC7A81FE89422ADED513C3BBC6A0D36

round [13].m_col:

67C17AA724BCC6F70387E50460F56840

round [13].s_row:

67C17AA760F568400387E50424BCC6F7

round [13].s_box:

98072AC0831CDB34C5E47BA7723F57D3

round [12].r_key:

5F1E30B4FE3E4E56DD948709B40D1FA8

round [12].xor_rkey:

C7191A747D2295621870FCAEC632487B

round [12].m_col:

9BDA5A3EF9E732B04D512FD4AFBFE593

round [12].s_row:

9BDA5A3EAFBFE5934D512FD4F9E732B0

round [12].s_box:

8081EC2917877BC2158F6A086960C8D1

round [11].r_key:

8736F598CD4C31FA14C99BDF628C7DFF

round [11].xor_rkey:

07B719B1DACB4A380146F1D70BECB52E

round [11].m_col:

4C1727896BE04BE835D8B3FC77715A94

round [11].s_row:

4C17278977715A9435D8B3FC6BE04BE8

round [11].s_box:

810E906C79A2EC37C43EA0DD04B8CC36

```
round [10].r_key:
    C99BDF628C7DFF8736F598CD4C31FA14

round [10].xor_rkey:
    48954F0EF5DF13B0F2CB381048893622

round [10].m_col:
    B17D54978D064D3F4DD0E175318092C5

round [10].s_row:
    B17D5497318092C54DD0E1758D064D3F

round [10].s_box:
    9F90F6A0B7B248B715E31FA5EF7B54BA

round [9].r_key:
    11802F59009668A7CEE93685BB646C8A

round [9].xor_rkey:
    8E10D9F9B7242010DB0A2920541F3830

round [9].m_col:
    D1ABE7BE77892A9D88E01A668C94F7CD

round [9].s_row:
    D1ABE7BE8C94F7CD88E01A6677892A9D

round [9].s_box:
    3446EA65C3C289BB65B8B42F796CDCD5

round [8].r_key:
    E93685BB646C8A11802F59009668A7CE

round [8].xor_rkey:
    DD706FDEA7AE03AAE597ED2FEF047B1B

round [8].m_col:
    0612FA09E4D01B40F90AF747D4C02F31

round [8].s_row:
    0612FA09D4C02F31F90AF747E4D01B40

round [8].s_box:
    0368B98FC6FD6A50698D89B945E3D834

round [7].r_key:
    87F46663EB5A51FD9AEBF6C636BD5842

round [7].xor_rkey:
    849CDFEC2DA73BADF3667F7F735E8076

round [7].m_col:
    6B4BC58A8B5F92B2AE80B2CC935E9A66

round [7].s_row:
    6B4BC58A935E9A66AE80B2CC8B5F92B2

round [7].s_box:
    04A3E8192EE6022FB4B23E35FD7F489F

round [6].r_key:
    EBF6C636BD584287F46663EB5A51FD9A

round [6].xor_rkey:
    EF552E2F93BE40A840D45DDEA72EB505
```

round [6].m_col:
E5D0F931DDC734DD4E6D623F046A248B

round [6].s_row:
E5D0F931046A248B4E6D623FDCC734DD

round [6].s_box:
A3E3B1504E9B9799F42D18BA21FCF97D

round [5].r_key:
94A7148430A76B18CCB45688BD991EEF

round [5].xor_rkey:
3744A5D47E3CFC8138994E329C65E792

round [5].m_col:
F8A92ECA7CA71B55EC429F80C043D1CF

round [5].s_row:
F8A92ECAC043D1CFEC429F807CA71B55

round [5].s_box:
D5AC4702F2172E4DB9100CDEFCF6D82A

round [4].r_key:
B45688BD991EEF94A7148430A76B18CC

round [4].xor_rkey:
61FACFBF6B09C1D91E0488EE5B9DC0E6

round [4].m_col:
7FEFC8D43BC036CC9C04561353A0C72B

round [4].s_row:
7FEFC8D453A0C72B9C0456133BC036CC

round [4].s_box:
C7A42B0867A788C748E9601877FD5D35

round [3].r_key:
6474A47C57ED785BB6A7B299EFEF2106

round [3].xor_rkey:
A3D08F74304AF09CFE4ED28198127C33

round [3].m_col:
3241DCDA5BB6FC81C97DA831AF7A0ED5

round [3].s_row:
3241DCDAF7A0ED5C97DA8315BB6FC81

round [3].s_box:
47670DB817D13A1B149093506AF007D8

round [2].r_key:
A7B299EFEF21066474A47C57ED785BB6

round [2].xor_rkey:
E0D59457F8F03C7F6034EF0787885C6E

round [2].m_col:
016A66A8E9E8259455631C7EA79DCA0C

round [2].s_row:

```
016A66A8A79DCA0C55631C7EE9E82594

round [2].s_box:
A29B7876F69AB2737F51A581B5C64037

round [1].r_key:
77C1FAA7C0E06FDF0C126E684EE61403

round [1].xor_rkey:
D55A82D1367ADDAC7343CBE9FB205434

round [1].m_col:
751FCD75F3C8FA65C719FC5DAE5658A1

round [1].s_row:
751FCD75AE5658A1C719FC5DF3C8FA65

round [1].s_box:
05DC1CA5B412E35875560731113AB9A3

round [0].sub_rkey:
F36DB456CEFDDFE1B45B5F7030CAD996

PLAINTEXT:
F36DB456CEFDDFE1B45B5F7030CAD996
```

В.2.8 Шифрування 256-бітного блоку з використанням 256-бітового ключа

```
ТЕСТ ЗАШИФРУВАННЯ КАЛИНА-256/256

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

PLAINTEXT:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

round [0].rkey:
F7DA2647DFD55B352F085208E30FCBA1
69B3C9DCC80DD7801F072CC16C942E36

round [0].add_rkey:
17FC486A03FB815C57317C330F3DF9D0
99E4FB0FFD420DB8574066FCA8D16C75

round [1].s_box:
AFC792D80627C9182B266045091034E7
40878B1F8B69DCDA2B1AB957C57AA4A6

round [1].s_row:
AFC7B9578B6934E72B2692D8C57ADCDA
408760450627A4A62B1A8B1F0910C918

round [1].m_col:
283D9E2711C75C40337BC7AAE17F3DDB
643F5DB7B208F27EBE1346E5383E5D77

round [1].r_key:
08E30FCBA169B3C9DCC80DD7801F072C
C16C942E36F7DA2647DFD55B352F0852

round [1].xor_rkey:
```

20DE91ECB0AEEF89EFB3CA7D61603AF7
A553C99984FF2858F9CC93BE0D115525

round [2].s_box:
3EACCF74B378449A8D1EB0DD48E70E17
685B268B5CD753A125E2A8E2F015A951

round [2].s_row:
3EACA8E25CD70E178D1ECF74F01553A1
685BB0DDB378A95125E2268B48E7449A

round [2].m_col:
265A9ED9588BDE16848906BF840AC222
79F7FEFB690BA863738A0AADDDB72E3D7

round [2].r_key:
DF1F1158FD74EEA5C15531C9239038DB
26839A9100031FCBB77CFD35F14F73C2

round [2].xor_rkey:
F9458F81A5FF30B345DC3776A79AFAF9
5F74646A6908B7A8C4F6F7982A3D9015

round [3].s_box:
2533297E68D7A68EE41FB4A8A09D2191
414ACCD8F9E9C14935A7AAA41510274A

round [3].s_row:
2533AAA4F9E92191E41F297E1510C149
414AB4A868D7274A35A7CCD8A09DA68E

round [3].m_col:
C4F7BE3F60C4A2A584D11113A578A31D
927275BB6CF91F07C662E4F2EEC9A349

round [3].r_key:
C9239038DB26839A9100031FCBB77CFD
35F14F73C2DF1F1158FD74EEA5C15531

round [3].xor_rkey:
0DD42E07BBE2213F15D1120C6ECFDFE0
A7833AC8AE2600169E9F901C4B08F678

round [4].s_box:
F053D12A99DD3CDF4D7A2B54C38291CB
A0000E96A2229353919827254AE95467

round [4].s_row:
F0532725A22291CB4D7AD12A4AE99353
A0002B5499DD546791980E96C3823CDF

round [4].m_col:
5387F788E1BA245006B87D90E3FD8C7F
0B7AF743CFDA32633B147DF991D5F6AF

round [4].r_key:
CA2AE58A5C656C0ACE0BF0A628FBA9FC
3176E710FC11F75DEB9601F95C22FD12

round [4].xor_rkey:
99AD1202BDDF485AC8B38D36CB062583
3A0C105333CBC53ED0827C00CDF70BBB

round [5].s_box:
40E62BCAAAAD9241FB1EEDE85E139BF1

D5D24AEE6185BEE1F7C96068206602A2

round [5].s_row:
40E6606861859BF1FB1E2BCA2066BEE1
D5D2EDE8AAAD02A2F7C94AEE5E139241

round [5].m_col:
20E3A76A0CEE8F5E4232613ACAA7D764
DDCD1549A1D05A83CF5E0F37FF5CE9C7

round [5].r_key:
A628FBA9FC3176E710FC11F75DEB9601
F95C22FD12CA2AE58A5C656C0ACE0BF0

round [5].xor_rkey:
86CB5CC3F0DFF9B952CE70CD974C4165
249137B4B31A706645026A5BF592E237

round [6].s_box:
1885D30F81AD3447E2F21E127016A5BE
B493B46FBD361E5FE4EB2FB1441B1394

round [6].s_row:
18852FB1BD36A5BEE2F2D30F441B1E5F
B4931E1281AD1394E4EBB46F70163447

round [6].m_col:
14715F8EF4B7CE46DCE5DA190CEAA7B7
F51C844E711CF84260965F447CD968A7

round [6].r_key:
5157FCECC510404E44F5E76CF2F2CB80
C29BEE53E310BE7DF816A49AEB175160

round [6].xor_rkey:
4526A36231A78E0898103D75FE186C37
37876A1D920C463F9880FBDE97CE39C7

round [7].s_box:
E4221F1572A080D46742DEA656C5A494
EEBF2F7969D2C3DF672A8B8070F23B2B

round [7].s_row:
E4228B8069D2A49467421F1570F2C3DF
EEBFDEA672A03B2B672A2F7956C580D4

round [7].m_col:
532711BE326227E0CAB9C6ED320C9CAA
2BAA36AB2A1D6AA15905B6922A197A43

round [7].r_key:
6CF2F2CB80C29BEE53E310BE7DF816A4
9AEB1751605157FCECC510404E44F5E7

round [7].xor_rkey:
3FD5E375B2A0BC0E995AD6534FF48A0E
B14121FA4A4C3D5DB5C0A6D2645D8FA4

round [8].s_box:
A1B358A6CE18BD19407B75EE275A1D19
BE6B3CB8AB16DEC4E9F18A826A3729F6

round [8].s_row:
A1B38A82AB161D19407B58A66A37DEC4
BE6B75EECE1829F6E9F13CB8275ABD19

round [8].m_col:
 7A2D2B7F820289D86A6D260B1288E2B4
 C9ADA5F49A7529B6F807F4947EB3F5F0

round [8].r_key:
 5E1C15889B51862AA11DD2875781B8D1
 0BD0A270AA4669B06B7A49B2473467EB

round [8].xor_rkey:
 24313EF719530FF2CB70F48C45095A65
 C27D078430334006937DBD263987921B

round [9].s_box:
 B426B217E05B59DC5E303921E43A18BE
 E8A5FC7B92F7254E3AA5969E19BF99D5

round [9].s_row:
 B426969E92F718BE5E30B21719BF254E
 E8A53921E05B99D53AA5FC7BE43A59DC

round [9].m_col:
 9EB2CF8E39D65B728A0DACA356B86232
 BEDC7066681B7EA2E5F7E6AD296A2853

round [9].r_key:
 875781B8D10BD0A270AA4669B06B7A49
 B2473467EB5E1C15889B51862AA11DD2

round [9].xor_rkey:
 19E54E36E8DD8BD0FAA7EACAE6D3187B
 0C9B4401834562B76D6CB72B03CB3581

round [10].s_box:
 E0BECBE81299E9E7E6A0E71C1374627C
 176A118D60338FC57B89C15E0685787E

round [10].s_row:
 E0BEC15E6033627CE6A0CBE806858FC5
 176AE71C1299787E7B89118D1374E9E7

round [10].m_col:
 B13E2B20301F89BADE85228E8749D34F
 4C7916A4566E24C889BDA67E7D2838BE

round [10].r_key:
 3752265E1FA9E6AA082AA99931C8B67B
 0864DFE7946F4FEF7C5BAD7C9212DB02

round [10].xor_rkey:
 866C0D7E2FB66F10D6AF8B17B6816534
 441DC943C2016B27F5E60B02EF3AE3BC

round [11].s_box:
 1889DCACC6B8382250F9E9838ADA9C40
 4257260EE8BB1511445E02CA8DC85869

round [11].s_row:
 188902CAE8BB9C4050F9DCAC8DC81511
 4257E983C6B85869445E260E8ADA3822

round [11].m_col:
 11C543291599CFD537D49B0C27DC12B1
 19BE28BA642DB5644829DFBEA32ADACC

round [11].r_key:
9931C8B67B0864DFE7946F4FEF7C5BAD
7C9212DB023752265E1FA9E6AA082AA9

round [11].xor_rkey:
88F48B9F6E91AB0AD040F443C8A0491C
652C3A61661AE742163676580922F065

round [12].s_box:
CD5AE9B2C3938E26F71A390EFB18EF25
88DF0E44A5367F6E2C446CA1DF6442BE

round [12].s_row:
CD5A6CA1A536EF25F71AE9B2DF647F6E
88DF390EC39342BE2C440E44FB188E26

round [12].m_col:
2191299282D46C2A03988A61ABD93DC3
8E690127E2044580D4797B7596303E3D

round [12].r_key:
38A743D67F8838BE74D17E6C1734E7C5
2BC87D984406B60679A71C17F9BA8F3B

round [12].xor_rkey:
19366A44FD5C54947749F40DBCEDDA06
A5A17CBFA602F386ADDE67626F8AB106

round [13].s_box:
E0442FE58B6F4D293B9B391E94FB3D4E
6832607A98EBDB630BACE2151E9CF94E

round [13].s_row:
E044E21598EB3D4E3B9B2FE51E9CDB63
6832391E8B6FF94E0BAC607A94FB4D29

round [13].m_col:
9EAA058EE2002985E3500609B739E53D
3ADF3AFF8CC2F6DB8E1C00027D75C93E

round [13].r_key:
6C1734E7C52BC87D984406B60679A71C
17F9BA8F3B38A743D67F8838BE74D17E

round [13].xor_rkey:
F2BD3169272BE1F87B1400BFB1404221
2D268070B7FA51985863883AC3011840

round [14].s_box:
C0252C880EB1FF7FF565937ABE1AD72F
D22287EA318AD5A4C2FDC7CE8CBB62B5

round [14].s_row:
C025C7CE318AD72FF5652C888CBB5A4
D222937A0EB162B5C2FD87EABE1AFF7F

round [14].m_col:
FA048CAFD80757EB968AF86753E72DDF
43C34CD6C45971289706185FA859EF29

round [14].add_rkey:
F66E3D570EC92135AEDAE323DCBD2A8C
A03963EC206A0D5A88385C24617FD92C

CIPHERTEXT:

F66E3D570EC92135AEDAE323DCBD2A8C
A03963EC206A0D5A88385C24617FD92C

ТЕСТ РОЗШИФРУВАННЯ КАЛИНА-256/256

KEY:

1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

CIPHERTEXT:

3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120

round [14].rkey:

3DD43BC93076156C81E6C77D7638C7E3
95C83DB4DD578B62A6D4A3498BB95E97

round [14].sub_rkey:

026A01730AC423CCB64F6DB6BCF9694C
9A65EF774DD29DC5815181DA9768C288

round [14].m_col:

2427960B8BDF7CF2B5413581651A7E
9EDD55F423B57F74785A6948F414CCB5

round [14].s_row:

2427413523B5CCB5F2B555F4F414FF7C
9EDD69488BDF1A7E785A960B81657F74

round [14].s_box:

72FB3BD956756440417556453839E17B
32E2A155FD2CB481A0F4BDE8F014E7EC

round [13].r_key:

BCD79B8EEC4A6BC5A536832502E46FBE
18D8C7EECA5860AAFCFAEDB68D5057D9

round [13].xor_rkey:

CE2CA057BA3F0F85E443D5603ADD8EC5
2A3A66BB3774D42B5C0E505E7D44B035

round [13].m_col:

B89C1C9A4E919F7CD1027AC67E261D85
EEDF4945D4F1176966B4EDD67BF04BC2

round [13].s_row:

B89C7AC6D4F14BC2D10249457BF09F7C
EEDFEDD64E911D8566B41C9A7E261769

round [13].s_box:

DB8A2AC1C6C0CC95342A20336DF30C7B
372C8D4AF44E8A4B5A13A589D43111BC

round [12].r_key:

5860AAFCFAEDB68D5057D9BCD79B8EEC
4A6BC5A536832502E46FBE18D8C7EECA

round [12].xor_rkey:

83EA803D3C2D7A18647DF98FBA688297
7D4748EFC2CDAF49BE7C1B910CF6FF76

round [12].m_col:

068FC199BAAB1C576BBAD9F9D91555E
78375847B504B7E334F88D5314FC42F1

```

round [12].s_row:
068FAD9FB50442F16BBD584714FC1C57
78378D53BAAB555E34F8C1999D91B7E3

round [12].s_box:
039926919AE9F0830444E3B97C66A5FC
A05D87167A46562B600FB74F944E36EA

round [11].r_key:
A05443492334573C631005D855A3091F
093A108046ABD13ED177C0440BF70EE0

round [11].xor_rkey:
A3CD65D8B9DDA7BF6754E66129C5ACE3
A96797963CED8715B178770B9FB9380A

round [11].m_col:
4E9B2069DEB617F4BA94B70BDF00AE32
FF690A0F8335AE6C5B5ED9220257460F

round [11].s_row:
4E9BB70B8335460FBA940A0F025717F4
FF69D922DEB6AE325B5E2069DF00AE6C

round [11].s_box:
F44936E842D9EEC37AC2E6C3A91D1145
8F4201109BF0C44E6AE6A8BC0983C4B0

round [10].r_key:
ABD13ED177C0440BF70EE0A054434923
34573C631005D855A3091F093A108046

round [10].xor_rkey:
5F9808393519AAC88DCC0663FD5E5866
BB153D738BF51C1BC9EFB7B5339344F6

round [10].m_col:
CA29B16E69B1A280967DA79598AE2591
067889629CC7C619D47A3B12119D2D20

round [10].s_row:
CA29A7959CC72D20967D8962119DA280
06783B1269B12591D47AB16E98AEC619

round [10].s_box:
FBFEE9E948FC2C795490C772A19AAFDE
03AE39CD922B40F9C6D17A42A63B570E

round [9].r_key:
AFFE0B7F2A36AB76E1439917F5696AC6
9CF3865E419AA4C1037233CDCEFD99B4

round [9].xor_rkey:
5400E29662CA870FB5D35E6554F3C518
9F5DBF93D3B1E438C5A3498F68C6CEBA

round [9].m_col:
023D11CC89E6911CBE160965EE795AB7
19DE92F570DCB904FA3A8687E6135E2A

round [9].s_row:
023D096570DC5E2ABE1692F5E613911C
19DE868789E65AB7FA3A11CCEE79B904

round [9].s_box:

```

A98E38A397717E07B14C481EFA06DFCA
39DAF5D68EADEC1A36094435376A66A7

round [8].r_key:
9AA4C1037233CDCEFD99B4AFFE0B7F2A
36AB76E1439917F5696AC69CF3865E41

round [8].xor_rkey:
332AF9A0E542B3C94CD5FCB1040DA0E0
0F718337CD34FBEF5F6382A9C4EC38E6

round [8].m_col:
E54A7658070DF92D63DC75A65F068DE7
567195DB6A560BE02E64C02E3FFB3F29

round [8].s_row:
E54A75A66A563F2963DC95DB3FFBF92D
5671C02E070D8DE72E6476585F060BE0

round [8].s_box:
A374D6756412859435719A7A8CEDB114
FEA222A1D96987D050223420027B71FE

round [7].r_key:
EC16284BAAD247CBAAB9F1C31904D06F
6058AF4643D5FC31E73DEF49CFA76050

round [7].xor_rkey:
4F62FE3ECEC0C25F9FC86BB995E9617B
9EFA8DE79ABC7BE1B71FDB69CDDC11AE

round [7].m_col:
4E272E6B48A5CA05717094765AA9E7A6
8F30AE36CC72719577BC0C7E94DB6381

round [7].s_row:
4E279476CC7263817170AE3694DBCA05
8F300C7E48A5E7A677BC2E6B5AA97195

round [7].s_box:
F4FB14E349E0D7D808A6C4EFBCCEB288
4C70FD81617DEA75793F47E253AC1AE9

round [6].r_key:
D5FC31E73DEF49CFA76050EC16284BAA
D247CBAAB9F1C31904D06F6058AF4643

round [6].xor_rkey:
21072504740F9E17AFC69403AAC6F922
9E37362BD88C296C7DEF28820B035CAA

round [6].m_col:
2E8E724BADCC3BDE740D9720B27C881D
31C7E4494E296CFCD0305167C8D11413

round [6].s_row:
2E8E97204E291413740DE449C8D13BDE
31C75167ADCC881DD030724BB27C6CFC

round [6].s_box:
50525B79F4FE7418AB6919A8DF4839DA
B7FC0E783B54869BE4702F05763076DD

round [5].r_key:
95974F65DB29D79DB30A0903AC810306

4616401AF54AE81E55628E034EFE3C37

round [5].xor_rkey:
C5C5141C2FD7A385186310AB73C93ADC
F1EA4E62CE1E6E85B112A10638CE4AEA

round [5].m_col:
A3B75E9A9738C1530007C8EB4DAC9D9A
9F3454782CD6F15E1400518494DCDAC5

round [5].s_row:
A3B7C8EB2CD6DAC50007547894DCC153
9F34518497389D9A14005E9A4DACF15E

round [5].s_box:
22722B96160A6EB7A49CF6E7BC71B716
7DEC0ECE1AB44C897C837E8915DEE42B

round [4].r_key:
4AE81E55628E034EFE3C3795974F65DB
29D79DB30A0903AC8103064616401AF5

round [4].xor_rkey:
689A35C374846DF95AA0C1722B3ED2CD
543B937D10BD4F25FD8078CF039EFEDE

round [4].m_col:
9FF4068CD12C70B2523C2CDC60DC8488
A1588510C452737444EED1FAE9ECCB40

round [4].s_row:
9FF42CDCC452CB40523C8510E9EC70B2
A158D1FAD12C848844EE068C60DC7374

round [4].s_box:
7D2531F2D8CD4E34E1552782B5E81D9F
3F232E6E34E1CE69F54FED9A8371B0EC

round [3].r_key:
3A4CD6E462CD392FBF122BE2E99D1A60
B4D0E79E1090587867C1259A6DA956A4

round [3].xor_rkey:
4769E716BA00771B5E470C605C7507FF
8BF3C9F024719611928EC800EED8E648

round [3].m_col:
DC4D43C0F1ACD896ED76727D30845746
0BA9D95352A0DBABE3174FC5D6D60B33

round [3].s_row:
DC4D727D52A00B33ED76D953D6D6D896
0BA94FC5F1AC5746E31743C03084DBAB

round [3].s_box:
402F2FE6E1A771A9F3BB0116ED0A23C8
ADAC52B7BADEA212DE0EBF979DC5F36B

round [2].r_key:
90587867C1259A6DA956A43A4CD6E462
CD392FBF122BE2E99D1A60B4D0E79E10

round [2].xor_rkey:
D07757812082EBC45AEDA52CA1DCC7AA
60957D08A8F540FB4314DF234D226D7B

```

round [2].m_col:
17707BEBB0F469C6725F3A6231C80C3F
07A0F4FC32DD9D6ACB1F60DA13CFA7B6

round [2].s_row:
17703A6232DDA7B6725FF4FC13CF69C6
07A060DAB0F40C3FCB1F7BEB31C89D6A

round [2].s_box:
0CA6B37247E2E992317F15DDE68BA1C1
D9A77CB88B25FDBA13DC5996B73A4CCC

round [1].r_key:
E02C1D2EEA7D57C95605BEC30ED52C2B
4AC1D238A7CABEC5AA16A6351B8B660E

round [1].xor_rkey:
EC8AAE5CAD9FBE5B677AAB1EE85E8DEA
9366AE802CEF437FB9CAFFA3ACB12AC2

round [1].m_col:
CC7E0C6072C0FDBF89AAA70D32A2886B
1F1E8CC30B909243FA36006C38E46D2E

round [1].s_row:
CC7EA70D0B906D2E89AA8CC338E4FDBF
1F1E006C72C0886BFA360C6032A29243

round [1].s_box:
4984E922AD0D84A18E27F8906CA8798D
28B345B031FD86E2361AFD6F4785488A

round [0].sub_rkey:
7FC5237896674E8603C1E9B03F8B4BA3
AB5B7C592C3FC3D361EDD12586B20FE3

PLAINTEXT:
7FC5237896674E8603C1E9B03F8B4BA3
AB5B7C592C3FC3D361EDD12586B20FE3

```

В.2.9 Шифрування 256-бітного блоку з використанням 512-бітового ключа

ТЕСТ ЗАШИФРУВАННЯ КАЛИНА-256/512

```

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

round [0].rkey:
F7BD9738CE49DDA80B9ABD79801EE821
8860FE42475C9F565CD8F433B4C989C4

round [0].add_rkey:
37FFD97B128F23F053E307C5CC6B3671
D8B150969BB1F5ADB4314F8F1027E823

round [1].s_box:

```

EED7237C1D51D8645AD0FC0690E5B7BC
C44610EBDE4686D0AE2635096DAAC502

round [1].s_row:
EED73509DE46B7BC5AD0237C6DAA86D0
C446FC061D51C502AE2610EB90E5D864

round [1].m_col:
0E024E3F31410B541F7A5326870535F9
D596CB7C8904DF9E1CF4CA83B8E612EE

round [1].r_key:
79801EE8218860FE42475C9F565CD8F4
33B4C989C4F7BD9738CE49DDA80B9ABD

round [1].xor_rkey:
778250D710C96BAA5D3D0FB9D159ED0D
E62202F54DF36209243A835E10ED8853

round [2].s_box:
3BC9105C6D7715E4A9105947EA49061E
13649AA96EF08F52B4C85D2C6DFBC7EE

round [2].s_row:
3BC95D2C6EF0061EA910105C6DFB8F52
136459476D77C7EEB4C89AA9EA4915E4

round [2].m_col:
CD179C15E91FCC4405EFB6C5111A7ACF
80DD714A467FB05F69EFF9DA3A3987D4

round [2].r_key:
400B80A3E5EE106402037E6445A8C043
C025BC83FB4294B0A03392A1F20BCAD2

round [2].xor_rkey:
8D1C1CB60CF1DC2007ECC8A154B2BA8C
40F8CDC9BD3D24EFC9DC6B7BC8324D06

round [3].s_box:
1BF5CD0117C22A585934322E9680F221
DC2164A3AA105C36051F157CFB2E7D4E

round [3].s_row:
1BF5157CAA10F2215934CD01FB2E5C36
DC21322E17C27D4E051F64A396802A58

round [3].m_col:
EAC6F69EDC22DDAA8C44FEC9C5203DC9
6C7F493E4127BA8718F15491311B6977

round [3].r_key:
6445A8C043C025BC83FB4294B0A03392
A1F20BCAD2400B80A3E5EE106402037E

round [3].xor_rkey:
8E835E5E9FE2F8160FBFBC5D75800E5B
CD8D42F49367B107BB14BA8155196A09

round [4].s_box:
8900E62CB1DD8C530905BDC4C72A51B1
200AD7593A41F92A9965F27E165C2F52

round [4].s_row:
8900F27E3A4151B10905E62C165CF92A

200ABDC4B1DD2F529965D759C72A8C53

round [4].m_col:
E8B4B452FF4F1202616D942D34F47F97
1092B746AFB4979751EDDA1EA1538777

round [4].r_key:
D011D865E1E63E78353CDCE9F6E131E6
6F7AAF50A301148798CD52A4004CD904

round [4].xor_rkey:
38A56C371EA92C7A545148C4C2154E71
7FE818160CB58310C92088BAA11F5E73

round [5].s_box:
F43BA49445402DDB9663920AE81CCBBC
55EC625317E15D220531C73F118DE60C

round [5].s_row:
F43BC73F17E1CBBC9663A494118D5D22
55EC920A4540E60C05316253E81C2DDB

round [5].m_col:
4917F1B070247D59E86BA29B28A387BD
6420FEBB61881901439808705A43C441

round [5].r_key:
E9F6E131E66F7AAF50A301148798CD52
A4004CD904D011D865E1E63E78353CDC

round [5].xor_rkey:
A0E11081964B07F6B8C8A38FAF3B4AEF
C020B262655808D92679EE4E2276F89D

round [6].s_box:
782C4A7ED34EFC4C1C4F1F0976AE4E36
2F31CA158881BA359A624632A33F8CFF

round [6].s_row:
782C463288814E361C4F4A7EA33FBA35
2F311F09D34E8CFF9A62CA1576AEFC4C

round [6].m_col:
1FA25C2A5C29D68B74986C9C904A6D58
43EEC59F5E4A395F9F1FB0AE52B6A7D0

round [6].r_key:
B29987F5AEDC7C5049872A92B4D70DD0
6ECB5266D3774630F330F21BBBB21C45

round [6].xor_rkey:
AD3BDBDFF2F5AADB3D1F460E249D6088
2D2597F98D3D7F6F6C2F42B5E904BB95

round [7].s_box:
0BAE68EFC0EDCEB4A48DC319B4B95605
D2F424911B103360384DD75029EA6FC2

round [7].s_row:
0BAED7501B105605A48D68EF29EA3360
D2F4C319C0ED6FC2384D2491B4B9CEB4

round [7].m_col:
4A31C749C44CD02004866D7182E2BF92
F2D5CA9DEA960DBA92C672BB84A166B8


```

round [7].r_key:
    92B4D70DD06ECB5266D3774630F330F2
    1BBBB21C45B29987F5AEDC7C5049872A

round [7].xor_rkey:
    D885104414221B7262551A37B2118F60
    E96E7881AF24943D6768AEC7D4E8E192

round [8].s_box:
    C4A24AE5C964D462FC3C7194CE152972
    29E3667E769E50D25312312B7EECFFB6

round [8].s_row:
    C4A2312B769E2972FC3C4AE57EEC50D2
    29E37194C964FFB65312667ECE15D462

round [8].m_col:
    46648730A91F78A21D438ADD2EC56B29
    901B072E3A5E1F041F298F1E1EC4AC58

round [8].r_key:
    535BC565CE0838DF30FC6AB4D7D11CC7
    1DF00EB1A3C796AC1469E8C6CE80238D

round [8].xor_rkey:
    153F42556717407D2DBFE069F91477EE
    8DEB099F999989A80B4067D8D0448FD5

round [9].s_box:
    4DBCD748534325DD205F68825657E3B
    1B036AB2408FF749951AE281F7BD299D

round [9].s_row:
    4DBCE281408F7E3BD205D748F7BDF749
    1B03F6885343299D951A6AB2256525DD

round [9].m_col:
    893CC8FC3829246CB7547EFFED166CC0
    3D784E90307A81CC3C836952554797C5

round [9].r_key:
    B4D7D11CC71DF00EB1A3C796AC1469E8
    C6CE80238D535BC565CE0838DF30FC6A

round [9].xor_rkey:
    3DEB19E0FF34D46206F7B96941020528
    FBB6CEB3BD29DA09594D616A8A776BAF

round [10].s_box:
    A403E4CB800801156C66FA88F2EB22F2
    CAB8848EAA0F3D52659581D8219715C7

round [10].s_row:
    A40381D8AA0F22F26C66E4CB21973D52
    CAB8FA88800815C76595848EF2EB0115

round [10].m_col:
    DA4D2268590D0628342F8561AE7BBADF
    DB0E56056101BCEA0080C210E64F55B2

round [10].r_key:
    575458552EB47D9C6246F01AF15E077F
    CD97D8C55BC8365F3798FE37B8947898
    
```

```

round [10].xor_rkey:
    8D197A3D77B97BB45669757B5F25BDA0
    16998EC03AC98AB537183C275EDB2D2A

round [11].s_box:
    1B5CB1D23B0CE56F230D6E7C41F49697
    2C8F80A7D5771D50EEC54C1147CDE055

round [11].s_row:
    1B5C4C11D5779697230DB1D247CD1D50
    2C8F6E7C3B0CE055EEC580A741F4E56F

round [11].m_col:
    5DF231D67160C6872B0F20FBC7120387
    2A57BBCEA72C7540261D0C5A0A3B9278

round [11].r_key:
    1AF15E077FCD97D8C55BC8365F3798FE
    37B8947898575458552EB47D9C6246F0

round [11].xor_rkey:
    47036FD10EAD515FEE54E8CD98259B79
    1DEF2FB63F7B21187333B8279659D488

round [12].s_box:
    329238B0D8E6D57173CCC51267F4D220
    4B597201A1063C1328F7FE11D3490105

round [12].s_row:
    3292FE11A106D22073CC38B0D3493C13
    4B59C512D8E6010528F7720167F4D571

round [12].m_col:
    615604CB78550718523FBD3E3ABB21A8
    05512DBCBE2A05DAC3A9FC556FDB5E5

round [12].r_key:
    AE10A655AFA56FDD369FDEAD237BDBC9
    B9CFB69D14A777624774969AB2022675

round [12].xor_rkey:
    CF46A29ED7F068C564A0639319C0FA61
    BC9E9B21AA75D73FEB4E095FE4FF9390

round [13].s_box:
    82AB57C11AB6AC066A1877D7E0F12144
    94B0D22FA6B563DFB9916A71D0D7A8C3

round [13].s_row:
    82AB6A71A6B521446A1857C1D0D763DF
    94B077D71AB6A8C3B991D22FE0F1AC06

round [13].m_col:
    AD3B055F99E78965CC4E5A00966F3488
    5266CCCE2DD3D67F8EE8204F69BA19FA

round [13].r_key:
    AD237BDBC9B9CFB69D14A77762477496
    9AB2022675AE10A655AFA56FDD369FDE

round [13].xor_rkey:
    00187E84505E46D3515AFD77F428401E
    C8D4CEE8587DC6D9DB478520B48C8624

round [14].s_box:

```

A8C55E7B2E60C3F7E77B0CEC4E7525F5
FB53840BC2A51935B8FA3F58AE0E88ED

round [14].s_row:
A8C53F58C2A525F5E77B5E7BAE0E1935
FB530CEC2E6088EDB8FA840B4E75C3F7

round [14].m_col:
59E952056E70D5107A170F3EF2C99374
4448FC38FEE163E8060D0F903CAAF62

round [14].r_key:
3BA763DCCAF841C59B138A7957447C95
CB026165A9DCA04A5D7092BB878B24F5

round [14].xor_rkey:
624E31D9A48894D5E1048547A58DEFE1
8F4A9D5D573DC3A25B7D9D2BBB21D897

round [15].s_box:
FC912C350011509D52EA3F86680A44BB
FF685BC42B10F3F80FA55B5E99F61BC0

round [15].s_row:
FC915B5E2B1044BB52EA2C3599F6F3F8
FF683F8600111BC00FA55BC4680A509D

round [15].m_col:
2B0E8543C2D5EFBE87CAE52873563234
D280B047FF42058AFC00104DD8DB36AA

round [15].r_key:
7957447C95CB026165A9DCA04A5D7092
BB878B24F53BA763DCCAF841C59B138A

round [15].xor_rkey:
5259C13F571EEDDFE2633988390B42A6
69073B630A79A2E920CAE80C1D402520

round [16].s_box:
E249B6DF2B6706EF64FD3B0519B2D707
F9C141FD876257953ED3C5544B1A9B58

round [16].s_row:
E249C5548762D70764FDB6DF4B1A5795
F9C13B052B679B583ED341FD19B206EF

round [16].m_col:
17571B6C8A0D70B7FAFA20039FEC737F
7BF449144B4BB3D48207CA176E1E47E4

round [16].r_key:
19BE451A213F473E9D5D8713962D5CDE
E7367B3C3E7F37C96EABA307F3790E79

round [16].xor_rkey:
0EE95E76AB32378967A7A71009C12FA1
9CC232287534841DECAC69109D67499D

round [17].s_box:
D804E6A8742EB49A53A0BC22DF6E722E
5D94C4F2C7086D79CFA9B8223041EFFF

round [17].s_row:
D804B822C708722E53A0E6A830416D79

5D94BC22742EEFFFCFA9C4F2DF6EB49A

round [17].m_col:
212D1FFE5776ED12E326A54D9B478B2C
926DFE56C7E01C99D19DA7211BE1A960

round [17].r_key:
13962D5CDEE7367B3C3E7F37C96EABA3
07F3790E7919BE451A213F473E9D5D87

round [17].xor_rkey:
32BB32A28991DB69DF18DA7A5229208F
959E8758BEF9A2DCCBBC9866257CF4E7

round [18].s_box:
9E76C4F87D936888C8C53DDBE20F4909
D7B08DA1F67F57A55E1D285FB6A43978

round [18].s_row:
9E76285FF67F4909C8C5C4F8B6A457A5
D7B03DDB7D9339785E1D8DA1E20F6888

round [18].m_col:
059F7DAAE49D71993675C68AAAC43345
A514DC96C24D50671F82EDA80EA593B5

round [18].add_rkey:
606990E9E6B7B67A4BD6D893D72268B7
8E02C83C3CD7E102FD2E74A8FDFE5DD9

CIPHERTEXT:
606990E9E6B7B67A4BD6D893D72268B7
8E02C83C3CD7E102FD2E74A8FDFE5DD9

ТЕСТ РОЗШИФРУВАННЯ КАЛИНА-256/512

KEY:
3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

CIPHERTEXT:
5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140

round [18].rkey:
4690D9074DD88B101B0E5402141EE27E
7DD221AAEC15B523291D748F6E01CF8

round [18].sub_rkey:
19CE83540E82CD473C4801523F346FD1
D27B2BA29C88EDF515B56DFB4C612448

round [18].m_col:
FE6531291810C4262A694AC955BC8F91
4AC2D17EFBA2CC2AB5B55BDF0D4816D8

round [18].s_row:
FE654AC9FBA216D82A69D17E0D48C426
4AC25BDF18108F91B5B5312955BCCC2A

round [18].s_box:
821410FBC8851E6AF7422E81D362320A
4BF19D3F863D62F99A75AE947F3F6407

```

round [17].r_key:
    EFAF2B3F72E868571424901B9FC9DA1E
    BBF6A2A5EC8637601221CD075B1FE272

round [17].xor_rkey:
    6DBB3BC4BA6D763DE366BE9A4CABE814
    F0073F9A6ABB55998854639324208675

round [17].m_col:
    629F12BFD60C65667F84009D02A25E79
    2EF6ADCCB34FC67FDB3E43A60B4CB653

round [17].s_row:
    629F009DB34FB6537F84ADCC0B4C6566
    2EF643A6D60C5E79DB3E12BF02A2C67F

round [17].s_box:
    DD3845D5B0C8C116C7C52635AD50DD2F
    5021BF75EDB97E1D6B374B8DA98557F8

round [16].r_key:
    8637601221CD075B1FE272EFAF2B3F72
    E868571424901B9FC9DA1EBBF6A2A5EC

round [16].xor_rkey:
    5B0F25C79105C64DD82754DA027BE25D
    B849E861C9296582A2ED55365F27F214

round [16].m_col:
    F45B62C13997F82461F53AABFC1EA2EB
    607C0F9A9382A9A24D46867F6AEADED1

round [16].s_row:
    F45B3AAB9382DED161F50F9A6AEAF824
    607C867F3997A2EB4D4662C1FC1EA9A2

round [16].s_box:
    3853B36B2ECF3D2C331C95896404FC74
    8330F5F81F77AF9615B1189E62B355BD

round [15].r_key:
    1C7218AE70870FC1774550657A0D2676
    D64DD6F41246C36B5016D8B3E86449F9

round [15].xor_rkey:
    2421ABC55E4832ED4459C5EC1E09DA02
    557D230C0D316CFD45A7C02D8AD71C44

round [15].m_col:
    FFE1EE279E908405A5A5CFB0E4FB27AF
    90B05FC2F70F2AAB63075F0A3D566687

round [15].s_row:
    FFE1CFB0F70F6687A5A55FC23D568405
    90B05F0A9E9027AF6307EE27E4FB2AAB

round [15].s_box:
    8FB591D1D02978D6667DD595CE12CE88
    CC9ED5C4320D90CB359CAD8E45EDDC6B

round [14].r_key:
    46C36B5016D8B3E86449F91C7218AE70
    870FC1774550657A0D2676D64DD6F412

```

```

round [14].xor_rkey:
  C976FA81C6F1CB3E02342C89BC0A60F8
  4B9114B3775DF5B138BADB58083B2879

round [14].m_col:
  ED138B92278B785AEBF69C8EF54A9A3F
  E4FBF72EA89E80EF92430CBB53D4EB6E

round [14].s_row:
  ED139C8EA89EEB6EEBF6F72E53D4785A
  E4FB0CBB278B9A3F92438B92F54A80EF

round [14].s_box:
  F30665B30024A942902189A1677835E5
  45EDFDE14FB002BA3017FB597B748EDF

round [13].r_key:
  70BEFAD04D2541841440842C116DD8CE
  0DD026B3E25DAC040AFDD5A49E546B15

round [13].xor_rkey:
  83B89F634D01E8C684610D8D7615ED2B
  483DDB52ADEDAEBE3AEA2EFDE520E5CA

round [13].m_col:
  F59FE680788A7725E58664300FFD5531
  A8024BA0117C8203F69F48E9B594C0C3

round [13].s_row:
  F59F6430117CC0C3E5864BA0B5947725
  A80248E9788A5531F69FE6800FFD8203

round [13].s_box:
  7B38CD57A1302290A397CC879AC2631C
  002A5F48A0FA5650BE385EDE5B63CF11

round [12].r_key:
  5DAC040AFDD5A49E546B1570BEFAD04D
  2541841440842C116DD8CE0DD026B3E2

round [12].xor_rkey:
  2694C95D5CE5860EF7FCD9F72438B351
  256BDB5CE07E7A41D3E090D38B457CF3

round [12].m_col:
  054680015FE854F0F9905C9B8D27C365
  360135BA8DACA732110F767E6A09D651

round [12].s_row:
  05465C9B8DACD651F99035BA6A0954F0
  3601767E5FE8C365110F80018D27A732

round [12].s_box:
  C9B12468EFDE7325690D4FE46496F6F3
  74F2348102C646A3A1298EB6EFFBE94E

round [11].r_key:
  81141555C47A68FEE3C9C9DD7EBF5032
  E817DD8DE95F205110910CB01C4929ED

round [11].xor_rkey:
  48A5313D2BA41BDB8AC486391A29A6C1
  9CE5E90CEB9966F2B1B88206F3B2C0A3

round [11].m_col:

```

279A83B93247027A38476B2F9CE7D23E
97094D220621BB2D6750500F7E28F6DF

round [11].s_row:
279A6B2F0621F6DF38474D227E28027A
9709500F3247D23E675083B99CE7BB2D

round [11].s_box:
4FC4D02103F8E03F6C955410D4C30BBF
1A9694C347959B2998D09FAC48601614

round [10].r_key:
5F205110910CB01C4929ED81141555C4
7A68FEE3C9C9DD7EBF5032E817DD8DE9

round [10].xor_rkey:
10E4813192F4502325BCB991C0D65E7B
60FE6A208E5C46572780AD445FBD9BFD

round [10].m_col:
16CA5331F8BA9B4B182D6E32C9529C7C
CB73039277EE0B6A2EB4AC4BE4F12654

round [10].s_row:
16CA6E3277EE2654182D0392E4F19B4B
CB73AC4BF8BA9C7C2EB45331C9520B6A

round [10].s_box:
555F754E794FC90C867A435945C02505
132E6805D51B657B5013285014CD71CC

round [9].r_key:
6AB451C78A00F46BF025AAD93CC624E2
66AF8EEC969A60E42888A96F11E7B265

round [9].xor_rkey:
3FEB2489F34F3D67765FE980790601E7
7581E6E94381059F789B813F052AC3A9

round [9].m_col:
B9C7FD224B7D9679FB7839A6DFA4D331
5ED1920860771FD86D805639CE5F44EE

round [9].s_row:
B9C739A6607744EEFB789208CE5F9679
5ED156394B7DD3316D80FD22DFA41FD8

round [9].s_box:
EBFCF47583C9EF53C8AE4839B27FBD1D
CB4860CF1D905C5010B27910097CA36A

round [8].r_key:
9A60E42888A96F11E7B2656AB451C78A
00F46BF025AAD93CC624E266AF8EEC96

round [8].xor_rkey:
719C105D0B6080422F1C2D53062E7A97
CBB0B3F383A856CD6969B76A6F24FFC

round [8].m_col:
0EF40353D69AAC4B1D38C525DA54F012
461FFFCCE2A14D87E10F2D05C6FD7FAD

round [8].s_row:
0EF4C525E2A17FAD1D38FFCCC6FDAC4B

461F2D05D69AF012E10F0353DA544D87

round [8].s_box:

2725E81C5257E7EB12B4E1352F636805
87DC2C88EDC482CD2B294316853C54D6

round [7].r_key:

772941896029BC7800AA363588BD9E02
7133C7DBB5ECC203881A861188235B2B

round [7].xor_rkey:

500CA995327E5B93121ED700A7DEF607
F6EFEB53582840CEA333C5070D1F0FFD

round [7].m_col:

30DDDD32F8974088519525C98A90ECD5
CE66705DA6AEDC88D2E4CF9599E6610F

round [7].s_row:

30DD25C9A6AE610F5195705D99E64088
CE66CF95F897ECD5D2E4DD328A90DC88

round [7].s_box:

9DE240FBAA3BEBC3EA4D1D31BBAD9E69
B2F791E9D5778C1B2DA8BE4EB60D0D69

round [6].r_key:

ECC203881A861188235B2B7729418960
29BC7800AA363588BD9E027133C7DBB5

round [6].xor_rkey:

71204373B0BDFA4BC916364692EC1709
9B4BE9E97F41B9939036BC3F85CAD6DC

round [6].m_col:

27E6BE56BADD57D25C8F150C16B442E3
51A2A3D0E57618E413EF6C6A7AEA74C0

round [6].s_row:

27E6150CE57674C05C8FA3D07AEA57D2
51A26C6ABADD42E313EFBE5616B418E4

round [6].s_box:

4FAD6B73A3BBFE97849917AD4604A23D
EA8576CC7AE2F0EAE6A4C53855135AAA

round [5].r_key:

FEFA326970EE4EA5DEB0E225ABF6508E
8FEF7FA4A22E72354E984EE66B87BE64

round [5].xor_rkey:

B157591AD355B0325A29F588EDF2F2B3
656A0968D8CC82DFA83C8BDE3E94E4CE

round [5].m_col:

C5F641BF3071224C089D81F7349F748D
3EFE778BF4D3F85DCDA70376C7F1C4E4

round [5].s_row:

C5F681F7F4D3C4E4089D778BC7F1224C
3EFE03763071748DCDA741BF349FF85D

round [5].s_box:

A82161D338CA32AA7E9A639975C005F6
209343E39DA2FE0188F63B8D6038FC31


```

round [4].r_key:
    2E72354E984EE66B87BE64FEFA326970
    EE4EA5DEB0E225ABF6508E8FEF7FA4A2

round [4].xor_rkey:
    8653549DA084D4C1F92407678FF26C86
    CEDDE63D2D40DBAA7EA6B5028F475893

round [4].m_col:
    0136E202D4D39A4F61E4BF71F54DE7E5
    D7657228B1C55107220459C154916116

round [4].s_row:
    0136BF71B1C5611661E4722854919A4F
    D76559C1D4D3E7E52204E202F54D5107

round [4].s_box:
    A21AD35F9F18EB2D33A82F7CF14E0249
    95140F9EC6CAEA4470E967237B2F0EA6

round [3].r_key:
    64C648AA0AFB2D9C10B14C7191344CC9
    E42F2B7C0DCCDFDF0374F895E46BD153

round [3].xor_rkey:
    C6DC9BF595E3C6B12319630D607A4E80
    713B24E2CB06359B739D9FB69F44DFF5

round [3].m_col:
    A7658C7A136C7C1FE9D92499E74C6477
    0A415BC3FBEFF0B48CFD49A66A9ED0BC

round [3].s_row:
    A7652499FBEFD0BCE9D95BC36A9E7C1F
    0A4149A6136C64778CFD8C7AE74CF0B4

round [3].s_box:
    F614974FC8A45871B55B9D9064246D0F
    D2672075E673CD8BC363F8BF515082DB

round [2].r_key:
    CCDFDF0374F895E46BD15364C648AA0A
    FB2D9C10B14C7191344CC9E42F2B7C0D

round [2].xor_rkey:
    3ACB484CBC5CCD95DE8ACEF4A26CC705
    294ABC65573FBC1AF72F315B7E7BFED6

round [2].m_col:
    967F381D66DC2B861EDADFA8B339D919
    F6D4A28BB902ECE98ED9CBEDAEADD8D2

round [2].s_row:
    967FDFA8B902D8D21EDAA28BAEAD2B86
    F6D4CBED66DCD9198ED9381DB339ECE9

round [2].s_box:
    54F90A76EB2A233D6F81AF99B4DF1247
    BE784E245A71010E785B6F9BB0D88C48

round [1].r_key:
    094F444BE269D9C01F77768A12ED6195
    DC5AB8834C0E080A0D8AFA771834B389
    
```

```
round [1].xor_rkey:
5DB64E3D0943FAFD70F6D913A63273D2
6222F6A7167F090475D195ECA8EC3FC1
```

```
round [1].m_col:
9A14ADD64D611B95812A6D407EB751E4
7F9BCF93545346D1978C7B56811D9D1D
```

```
round [1].s_row:
9A146D4054539D1D812ACF93811D1B95
7F9B7B564D6151E4978CADD67EB746D1
```

```
round [1].s_box:
26398434F1D44C9BF08091C2F0BCD8E9
C749593815D60EAA1A6D264AD472EE2C
```

```
round [0].sub_rkey:
18317A2767DAD482BCCD07B9A1788D07
5E7098189E5F84972D0B916D79BA6AE0
```

```
PLAINTEXT:
18317A2767DAD482BCCD07B9A1788D07
5E7098189E5F84972D0B916D79BA6AE0
```

В.2.10 Шифрування 512-бітного блоку з використанням 512-бітового ключа

ТЕСТ ЗАШИФРУВАННЯ КАЛИНА-512/512

```
KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
```

```
PLAINTEXT:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
```

```
round [0].rkey:
1947C0FCF2C8D64CB256FB722DA8E241
88EABF026130064F03E0F2BD4CA854C9
A848BE6445FECF00510ADE0C1C4D43F1
073D53B163DF01DF01317E9552F262E5
```

```
round [0].add_rkey:
59880240370E1D94FA9F45BE79F53091
D83B1256B5855CA65B394D19A905B328
08AA20C8A9633668B973487888BAB160
77AEC524D854785679AAF810CF6FE164
```

```
round [1].s_box:
65119AB5EE177029E69800E277EDA69F
C4AE2BD3E9A2D3070F147D8A02CB3AF2
71FF499602FDB79BEC6C9267CD23F972
3B78BEEDC4CC66D377FF8C228220FF37
```

```
round [1].s_row:
65FFBE6702CBD39FE6118CEDCDFD3A07
C4989A22C423B7F20FAE00B582CCF99B
71142BE2EE206672ECFF7DD37717FFD3
3B6C498AE9ED70377778929602A2A629
```

round [1].m_col:
541056BC458C8C5334A3511FF017BFB6
DF2F9322345BACCE61AF80F6BAF0D8CF
1952A486F6C1AB14155911BA99C6B321
733B5D72DEB3A3887388A65FA49F4A6A

round [1].r_key:
026130064F03E0F2BD4CA854C9A848BE
6445FECF00510ADE0C1C4D43F1073D53
B163DF01DF01317E9552F262E51947C0
FCF2C8D64CB256FB722DA8E24188EABF

round [1].xor_rkey:
567166BA0A8F6CA189EFF94B39BFF708
BB6A6DED340AA6106DB3CDB54BF7E59C
A8317B8729C09A6A800BE3D87CDDFF4E1
8FC995A49201F57301A50EBDE517A0D5

round [2].s_box:
23DCB93F8751A42E7D5934851905AAD4
99797C98D1D68A227B1E64504A6647FB
C526E5A0BFF195D89BB2588114AD39BB
FF770FF669BB860C433B51A2D943B39D

round [2].s_row:
233B0F81BF668AD47DDC51F614F14722
9959B9A269AD95FB7B79343FD9BB39D8
C51E7C85874386BB9B2664981951B30C
FFB2E550D105A49D437758A04AD6AA2E

round [2].m_col:
94A272EE19ED0CCBA3C3E5DEE99C1EF2
A4440BCB092236E30AB39099E3CFCEFC
776AFB74BE1288FBF1D4775802A632F3
8673171ABBDE3010DC819936A88928C1

round [2].r_key:
2408F2FA312A9374A300773C06BC7C57
E369A136ECE1D879C2DFA2A30349F5B8
235CD21701AB035C23BF1BF30F8DE233
E0F83AC94DF8012703BE4B8A07DA0D56

round [2].xor_rkey:
B0AA801428C79FBF00C392E2EF2062A5
472DAAFDE5C3EE9AC86C323AE0863B44
54362963BFB98BA7D26B6CAB0D2BD0C0
668B2DD3F6263137DF3FD2BCAF532597

round [3].s_box:
B3FF872D1FA3837AA828996B8D318F75
326DCE1BD928468CFB89C4CEAC5541E5
9644A1FD260CE9040AE5A4D9F0B16BA7
A5CFE0F7A7222C94C8BC7969765B9BC0

round [3].s_row:
B3BCE0D926554675A8FF79F7F00C418C
32288769A7B1E9E5FB6D992D76226B04
9689CE6B1F5B2CA70A44C41B8DA39B94
A5E5A1CED93183C0C8CFA4FDAC288F7A

round [3].m_col:
595B0F13C242CEB10B980C87B0DB3DB5
143C1F41EFF055F13BA630DA2E9EB7A1
F8B8CEF74B328379DB953706A83B6FDA
3820FDE9E779A3E172CD03D6696A4B68

round [3].r_key:

36ECE1D879C2DFA2A30349F5B8235CD2
1701AB035C23BF1BF30F8DE233E0F83A
C94DF8012703BE4B8A07DA0D562408F2
FA312A9374A300773C06BC7C57E369A1

round [3].xor_rkey:

6FB7EECB801113A89B457208F86167
033DB442B3D3EAEAC8A9BD381D7E4F9B
31F536F66C313D325192ED0BFE1F6728
C211D77A93DAA3964ECBBFAA3E8922C9

round [4].s_box:

1EA846AF992A173DC56A0062712181AA
06101A6EBD74E7E3FB4096564B83351D
72EDB74C3826DEF3E71B06B3568DE2F2
E81563DB3ADE1FEB048543E4BBD5C0A3

round [4].s_row:

1E8563B33883E7AAC5A843DB562635E3
066A46E43A8DDE1DFB1000AFBBDEE2F3
72401A6299D51FF2E7ED966E712AC0EB
E81BB756BD2117A30415064C4B74813D

round [4].m_col:

37964F89469782089A1E93875C5E6D0E
5BECAA7102AC77B67462D4ECB6E3AD7B
E8A1DA0524AE10EC322668E508CBC579
60AC28C55AF76813503CFEA1DC4C19EC

round [4].r_key:

B8DF3967A97C8BFD5C4DECEC5168EEB4
0BEE562D80D97AD60998659CCD084D5D
C33441F000BF7AFAE EEBE431F96D67DE
A0E05A5BFFF8B0AA9A38C9857A91EA23

round [4].xor_rkey:

8F4976EEEFEB09F5C6537F6B0D3683BA
5002FC5C82750D607DFAB1707BEBE026
2B959BF524116A16DCCD8CD4F1A6A2A7
C04C729EA50FD8B9CA043724A6DDF3CF

round [5].s_box:

FF9B6C3B8D036AA9D45B33ABF0445D3F
2EEBF818FEB5DC729F8AF9EAF503F69E
E147D2A9B4152F533C52ECFE54705704
2F1605C168F81B47C1EAB4ED9899DB39

round [5].s_row:

FFEA05FEB403DC3FD49BB4C15415F672
2E5B6CED68702F9E9FEB333B98F85753
E18AF8AB8D991B043C47F918F003DB47
2F52D2EAFE446A39C116ECA9F5B55DA9

round [5].m_col:

EBF6C2FC2AD41CC2190BEB5BA1932CE8
8C219956353EB751C709366B9C6801BE
C39B06F063014339BAF659BDE3233A5C
E37324CC43D3C78A7771D032CF77FDAA

round [5].r_key:

2D80D97AD60998659CCD084D5DC33441
F000BF7AFAE EEBE431F96D67DEA0E05A
5BFFF8B0AA9A38C9857A91EA23B8DF39

67A97C8BFD5C4DECEC5168EEB40BEE56

round [5].xor_rkey:

C6761B86FCDD84A785C6E316FC5018A9
7C21262CCFD05CB5F6F05B0C42C8E1E4
9864FE40C99B7BF03F8CC857C09BE565
84DA5847BE8F8A669B20B8DC7B7C13FC

round [6].s_box:

D43FD4637C996D04DAE858537C4C6233
14F6ADD18250D350A7B69754834FFFBA
679674B5056AE564A10E32302F6A47BE
5CDED086F6511D5FDE31FEA5F5A4C257

round [6].s_row:

D431D030054FD333DA3FFE862F6AFF50
14E8D4A5F66AE5BAA7F65863F5514764
67B6AD537CA41DBEA19697D17C99C25F
5C0E7454824C6D57DEDE32B583506204

round [6].m_col:

3A68103F437C26DADCE717B7CF90EDC1
2B83397D2281A9E2521386AEDDB1D102
08FE4A41B6FBC6B8B4FBED28C4B53389
311DCD6ABFBDE3A8FD9C326F10F0DEBD

round [6].r_key:

7AB62677AAA05AC35BF994861CA08380
058651FB824351FCD684B5DD229F82EB
3ACFCDFD660698EEB922C62D097D6868
0375512C6960E6EA974A53A7C159DBA3

round [6].xor_rkey:

40DE3648E9DC7C19871E8331D3306E41
2E056886A0C2F81E84973373FF2E53E9
323187BCD0FD5E560DD92B05CDC85BE1
32689C46D6DD05426AD661C8D1A9051E

round [7].s_box:

DCACB7E9291F608A46675D5D0D7CDA38
93CBAC6378948CF55C86E30C80739E95
9E268D69F7C0E6D3F035C84B204F97BB
9E123EF95099226E5B618196EA4022F5

round [7].s_row:

DC613E4BF7738C3846AC81F920C09EF5
9367B796504FE6955CCB5DE9EA9997D3
9E86AC5D294022BBF026E3630D1F226E
9E358D0C787C60F55B12C8698094DA8A

round [7].m_col:

8F9D397F44473A0605EEDD8F6F631377
D0E2061130D3FF219191D6720605D2C1
938553E6C530DB5C9CFEA03BD35B3E07
18D5729882E1D09EEA58DE577EAF08F

round [7].r_key:

FB824351FCD684B5DD229F82EB3ACFCD
FD660698EEB922C62D097D6868037551
2C6960E6EA974A53A7C159DBA37AB626
77AAA05AC35BF994861CA08380058651

round [7].xor_rkey:

741F7A2EB891BEB3D8CC420D8459DCBA
2D840089DE6ADDE7BC98AB1A6E06A790

BFEC33002FA7910F3B3FF9E070218821
6F7FD2C241BA290A6C447ED4FEAA46DE

round [8].s_box:

368DB13C1C93DD8EC4E2D71E5C492A3F
D27E939AE3796578940B8EB7C313BCC3
2634E368C6A0CF1FADBC34CB22F6C72F
1E5F7993F223A12638BD5EFE56FFC380

round [8].s_row:

36BD79CBC613653FC48D5E9322A0BC78
D2E2B1FEF2F6CFC3947ED73C5623C71F
260B931E1CFFA12FAD348E9A5C93C326
1EBCE3B7E349DD80385F3468C3792A8E

round [8].m_col:

0E7C998B7B7D424BE5902BB31ACE69CC
30E7892054EE97BB29A9C1B9B4FD1501
F2FD437162D41C7CF30E808A67717265
AEB444718E40F31B62034AC585B379B1

round [8].r_key:

0B41893222373E1053852CE52AECAA6
D56AD4BB87D2771FB7FE9EB2B4BA7607
39F0DB9731E9F802E821E1BD930060E1
FC38253AD84043C78FFE6A9AA5856282

round [8].xor_rkey:

053D10B9594A7C5BB61507563022C36A
E58D5D9BD33CE0A49E575F0B00476306
CB0D98E6533DE47E1B2F6137F4711284
528C614B5600B0DCEDFD205F20361B33

round [9].s_box:

75104A47656860B18A1CFCD39264F3D8
D90A361D0D54F6F691A148B3A8FA774E
5E90287D5A10F1ACFD4D81944EDC2B7B
E20E818523CE73A5D6C049713E44D445

round [9].s_row:

75C081945AF6D88A1049854E1077F6
D91C4A7123DCF14E910AFC473ECE2BAC
5EA136D36544737BFD90481D9268D4A5
E24D28B30D646045D60E817DA854F3B1

round [9].m_col:

ED93B8E48E3725FDE2F9F75D9656F531
F4DB6FEF5F18D619DF57C12AD400FB99
FD7ECC323ABCC4893409791191329F2B
8D1EDF0D0F025B88CB76F004C69BB892

round [9].r_key:

BB87D2771FB7FE9EB2B4BA760739F0DB
9731E9F802E821E1BD930060E1FC3825
3AD84043C78FFE6A9AA58562820B4189
3222373E1053852CE52AECAA6D56AD4

round [9].xor_rkey:

56146A939180DB63504D4D2B916F05EA
63EA86175DF0F7F862C4C14A35FCC3BC
C7A68C71FD333AE3AEACFC731339DEA2
BF3CE8331F51DEA42E5C1CAE604ED246

round [10].s_box:

23652FD7842A68FD2E957D5E842022E3

B7C68883A9B6AA7FFC9AB6D663C7F369
7F70ECBC8BF70E76A2A9F80CCB14E8F8
2654C5453963E8F6936FCD42349179F9

round [10].s_row:

236FC50C8BC7AAE32E65CD45CBF7F37F
B7952F4239140E69FCC67DD73463E876
7F9A885E8491E8F8A270B683842A79F6
26A9ECD6A92068F99354F8BC63B622FD

round [10].m_col:

E8AF9273BCCF6A4BCC0C287F25E26AF6
CDB4F3BB2274A8E2F4DEE6DD466669F3
5928E2AADC273C6520FBC45B8F480833
05780A1798A18376D513AA29931B84FC

round [10].r_key:

B253F7958C9781BBC97F923194B2A4FA
F3950141E3D2E39C27D7846C8B0AFDFF
10E0EDA1E34515415844E5D7CCC409F1
AF08B30428D74108AE1339748912EE52

round [10].xor_rkey:

5AFC65E63058EBF00573BA4EB150CE0C
3E21F2FAC1A64B7ED30962B1CD6C940C
49C80F0B3F62292478BF218C438C01C2
AA70B913B076C27E7B00935D1A096AAE

round [11].s_box:

66C79C7D92816164756CF232BE4C8454
BBF6A0B8EF7012AC0D3A8F9020895054
CC4F59B3A148A1ED8E053C21370ED993
A630FA3DB33F08ACF5CEA8C4973A2F42

round [11].s_row:

66CEFA21A189125475C7A83D374850AC
BB6C9CC4B30EA1540DF6F27D973FD9ED
CC3AA032923A08938E4F8FB8BE812FAC
A6055990EF4C6142F5303CB320708464

round [11].m_col:

FF540849F7A5703D92BC2EF072859872
1D463C94F6B5C4C573834FF2B468157F
E8C6F3182EDD8E6D0FE3CC6AEB8CD8D5
A2290EC4B6730D60AC237FD983439B0B

round [11].r_key:

41E3D2E39C27D7846C8B0AFDFF10E0ED
A1E34515415844E5D7CCC409F1AF08B3
0428D74108AE1339748912EE52B253F7
958C9781BBC97F923194B2A4FAF39501

round [11].xor_rkey:

BEB7DAAA6B82A7B9FE37240D8D95789F
BCA57981B7ED8020A44F8BFB45C71DCC
ECEE245926739D547B6ADE84B93E8B22
37A599450DBA72F29DB7CD7D79B00E0A

round [12].s_box:

F6A83DE4DBC9BC47563E5C1E1B4766B2
943BFD7E31FB875800EEE9C9E4A3706A
CFDB5C929A6C5BC8F579E87BECD8E90D
EE3B30F4F02305DC30A864DD778B5126

round [12].s_row:

F6A8307B9AA387B256A864F4EC6C7058
943E3DDDF0D85B6A003B5CE47723E9C8
CFEEFD1EDB8B050DF5DBE97E1BC951DC
EE795CC93147BC26303BE892E4FB6647

round [12].m_col:

DC0A853B7F3559AA9589C848FE62853D
AE559F8FD8655DFA1948501752527675
B5A436CE957EE0DC9392D3EC5D3710C1
FE1E336E841052B68B1D36A46C0AFF90

round [12].r_key:

9C3B87B9EC223BC65BF1A4153B6FA7DA
62B9B72AFCEA375F34CD656C4857294F
0601C04788B80F27C19D7EE1FB81B710
CF7F61BD66447F10E34CDA0E63E32104

round [12].xor_rkey:

403102829317626CCE786C5DC50D22E7
CCEC28A5248F6AA52D85357B1A055F3A
B3A5F6891DC6EFFB520FAD0DA6B6A7D1
316152D3E2542DA66851ECAA0FE9DE94

round [13].s_box:

DC269A103A438F893DD4A4C40390C078
90345375B4512F75D2A2787C97CB48CE
BD3B549A4BE844C9E2F8EE1E98B8BCB0
722B4FF764CCE00786635AE40904E829

round [13].s_row:

DC634F1E4BCB2F783D265AF798E84875
90D49AE464B844CED234A41009CCBCC9
BDA253C43A04E0B0E23B78750343E807
72F8547CB4908F29862BEE9A9751C089

round [13].m_col:

1DD737BA1A565EB911F4F5CE316858AF
067F0B9B3B23895332628488077EFD79
6C9B335230133707182E38DE4DC0459C
4F729856451527B915289284F41C051A

round [13].r_key:

2AFCEA375F34CD656C4857294F0601C0
4788B80F27C19D7EE1FB81B710CF7F61
BD66447F10E34CDA0E63E321049C3B87
B9EC223BC65BF1A4153B6FA7DA62B9B7

round [13].xor_rkey:

372BDD8D456293DC7DBCA2E77E6E596F
41F7B3941CE2142DD399053F17B18218
D1FD772D20F07BDD164DDBFF495C7E1B
F69EBA6D834ED61D0013FD232E7EBCAD

round [14].s_box:

EEB165BFE448A8A59F1D577808E37B60
F2663A296FDD94160D8F22DFAF46F013
EAC07E163EB6E5FC2C956861CC6F5ED5
A7B0F29C60917579A8B40C029383BDD0

round [14].s_row:

EEB4F2613E4694609FB10C9CCCB6F016
F21D6502606FE5130D6657BF93915EFC
EA8F3A78E48375D52CC022290848BD79
A7957EDF6FE3A8D0A8B06816AFDD7BA5

round [14].m_col:
 1477C03527DC162C81405E2118BA3D0E
 94BF741DE91F69033F04C26E9A7D7A2C
 B405739E53E83A6E6F76021CC72466DE
 413043425A187832EC5E0950AE657682

round [14].r_key:
 39E087E636B3E6949C744EACB4DDCF4E
 603C95652731D549E70C5200F1D95095
 B04E404E675B56F93CBEC44AF7512C38
 8E1A3DDEFB8C30FADE3BDCFDB12BF4

round [14].xor_rkey:
 2D9747D3116FF0B81D34108DAC67F240
 F483E178CE2EBC4AD808906E6BA42AB9
 044B33D034B36C9753C8C65630754AE6
 CF2A7E9CA1A4F4021680328C53D45D76

round [15].s_box:
 D2862EF7F32042DA4B084ABF2D41A0B5
 4E00FF673D73BDD6C4E927FADBEF7A47
 6B4EE3E7D11EA4C05A4F19D392B54E7D
 82025EFB11EF39CA2C2AC4215A5336A8

round [15].s_row:
 D22A5ED3D1EFBDB54B86C4FB921E7AD6
 4E082E2111B5A447C4004AF75AEF4EC0
 6BE9FFBFF353397D5A4E27672D2036CA
 824FE3FA3D4142A82C0219E7DB73A0DA

round [15].m_col:
 74DC646F362F13C8613836AE29C9BF92
 BA41FEF4D91EB2FA2EC3EB4E60A91FF6
 637742A13247CB42F0326C680E8DB415
 584AE48404A9D2651D485E22EDE8AE90

round [15].r_key:
 652731D549E70C5200F1D95095B04E40
 4E675B56F93CBEC44AF7512C388E1A3D
 DEFBBC8C30FADE3BDCFDB12BF439E087
 E636B3E6949C744EACB4DDCF4E603C95

round [15].xor_rkey:
 11FB55BA7FC81F9A61C9EFFEBC79F1D2
 F426A5A220220C3E6434BA62582705CB
 BD8CFE2D02BD15792CCFDD43FAB45492
 BE7C57629035A62BB1FC83EDA3889205

round [16].s_box:
 F327A93F554FE18C487744E094620482
 4E221CF83E649FE16A08F215C2AA22AF
 AA0E74165F25F4204982650EE6384DB6
 F6A4C615EB5D8A5EBEC75D98E511994B

round [16].s_row:
 F3C7C60E5FAA9F8248275D15E62522E1
 4E77A998EB38F4AF6A22443FE55D4D20
 AA081CE055118AB6490EF2F8944F995E
 F68274153E62E14BBEA46516C264048C

round [16].m_col:
 127623D29DE58AD3BE843C0AFA2F21FA
 7D67693138815A55E874613C7A5CE082
 A922172090BE64FD44DA043F377ABAB1
 C8D1F33598DDF7C5ED13625C261FD26E

round [16].r_key:
 E0FC0D1B3FE4FBC87FAC3DB5112BCB96
 D8F23E593F85C1CC45D9D2AA23DC4D05
 6C6FEB08C3341F8BAF7AE2F89B2B5943
 549E109F03281BB8B91ED201C1E4012E

round [16].xor_rkey:
 F28A2EC9A201711BC12801BFEB04EA6C
 A595576807049B99ADADB3965980AD87
 C54DFC28538A7B76EBA0E6C7AC51E3F2
 9C4FE3AA9BF5EC7D540DB05DE7FBD340

round [17].s_box:
 C09CD1A301BB0BD5EF75D97AB9EAE789
 6847C69B59EAD28B0BE63AEB652AEEA0
 0395F8F25A9CE5A8B9180A2B2D6358DC
 5DEE58E4DEED5ADD969073C40C27BFB5

round [17].s_row:
 C090582B5A2AD289EF9C73E42D9CEE8B
 6875D1C4DE63E5A00B47D9A30CED58A8
 03E6C67A01275ADCB9953A9BB9BBBFD
 5D18F8EB59EA0BB596EE0AF265EAE7D5

round [17].m_col:
 5231B90D74321FC6895651A7FC91D930
 B928A73C359E30B24E22B611381C4CA1
 706830893E478B3130387EC3AE4BFE78
 FAA5F641FADF5C281D840B38454FC7AF

round [17].r_key:
 593F85C1CC45D9D2AA23DC4D056C6FEB
 08C3341F8BAF7AE2F89B2B5943549E10
 9F03281BB8B91ED201C1E4012EE0FC0D
 1B3FE4FBC87FAC3DB5112BCB96D8F23E

round [17].xor_rkey:
 0B0E3CCCB877C61423758DEAF9FDB6DB
 B1EB9323BE314A50B6B99D487B48D2B1
 EF6B189286FE95E331F99AC280AB0275
 E19A12BA32A0F015A89520F3D3973591

round [18].s_box:
 95174C6A1C97192D4FB5EDE325C00DB4
 BE03A802F6264E318A0C5BE9F5D17990
 8DE562B618290F76727F95939BC39AA6
 529D2B3F9E18424AC54749F00D86789F

round [18].s_row:
 95472B9318D14EB44F17493F9B297931
 BEB54CF09EC30F908A03ED6A0D189A76
 8D0CA8E31C8642A672E55B022597784A
 527F62E9F6C0199FC59D95B6F5260D2D

round [18].m_col:
 C7AB0983E21265D8FBEE77262D1283C2
 F9116FD044C0C681CAB69389C86E5D
 F27ECCF78B19441C9F6EC9053AC403C4
 6336AD69D1865A3AAD5AAABBE6646DB5

round [18].add_rkey:
 4A26E31B811C356AA61DD6CA0596231A
 67BA8354AA47F3A13E1DEEC320EB56B8
 95D0F417175BAB662FD6F134BB15C86C

CB906A26856EFEB7C5BC6472940DD9D9

CIPHERTEXT:

4A26E31B811C356AA61DD6CA0596231A
67BA8354AA47F3A13E1DEEC320EB56B8
95D0F417175BAB662FD6F134BB15C86C
CB906A26856EFEB7C5BC6472940DD9D9

ТЕСТ РОЗШИФРУВАННЯ КАЛИНА-512/512

KEY:

3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

CIPHERTEXT:

7F7E7D7C7B7A79787776757473727170
6F6E6D6C6B6A69686766656463626160
5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140

round [18].rkey:

98C03D94F13E485F1255DF35C843E984
8DD15AF5F69849047E6913E2E46A7FD4
40A845AB822D1D4C42897479DF3DC41B
5CC9C594575686CEFFDD939BB3CA2590

round [18].sub_rkey:

E7BD3FE8893B31196521963EAB2E88EB
E29C127774D11F64E9FC51827EF7E18B
1FB617B1D82C3C0C15CDE0DA73148D34
F38487B7F3F3C2794868B1A88F771BB0

round [18].m_col:

FE8350F9596E1B29F02AD90C1FC24A23
08EB11FB6F49E5B81D1453A3F5D02762
A75D4C9C5C0911E9254E1D991C9728F1
C4C333C0944BD7E0A554FF1D6488B52F

round [18].s_row:

FE2A11A35C97D72FF0EB539C1C4BB529
08144C9994881B231D5D1DC0646E4AB8
A74E331D59C2E56225C3FFF91F4927E9
C454500C6FD011F1A583D9FBF50928E0

round [18].s_box:

828044C9847742210D02286DB8A30394
7E393C4FBC16D84C12358A97E2C110FA
F64B7F9B07F17B72F9ABE14628599048
D83C94731CE34483667E019C7B9698FE

round [17].r_key:

E6D9AE46A5FAEA88FE56376A8A4D5AB0
B4A5B46E8CBB3BD751EAD50A09D14C9F
7340196B009EC79D5399E502FE9FCF2A
27676CADCB56DC151F0CF11858600B0

round [17].xor_rkey:

6459EA8F218DA8A9F3541F0732EE5924
CA9C882130ADE39B43DF5F9DEB105C65
850B66F0076FBCEFAA320444D6C65F62
FF5BF8DED7562942378ECE8DFE10984E

round [17].m_col:

3C0ABA664B6FED3E842C45AA41065484
CE6FE982DF6CA245D6B036B613FABB76
87190FF0BBB09F0531D1048865ED3AC3
9FB48D44DA7E7C78651EED63FD15B52E

round [17].s_row:

3C2CE9B6BBED7C2E846F36F0657EB53E
CEB00F88DA15ED84D6190444FD6F5445
87D18D634B06A27631B4ED66416CBB05
9F1EBAAADFFA9FC3650A458213B03A78

round [17].s_box:

DCE18B923EF56DA1915C5DF359840329
B29E956985118DCEED56F1611B5CF633
0A4887861D7BAFE3B7138D2F5F731688
7DB3086709470C90598D06D2E69EB3E7

round [16].r_key:

9FCF2A27676CADCB56DC151F0CF1185
8600B0E6D9AE46A5FAEA88FE56376A8A
4D5AB0B4A5B46E8CBB3BD751EAD50A09
D14C9F7340196B009EC79D5399E502FE

round [16].xor_rkey:

432EA1B55999C06A24319CA2A94B12AC
349E258F5CBFCB6B17BC799F4D6B9CB9
47123732B8CFC16F0C285A7EB5A61C81
ACFF9714495E6790C74A9B817F7BB119

round [16].m_col:

CF1A62802AB0AA985FCE5479EC888D5A
71D233D412306F274976B13BC57C89E4
16CACCC918128166556BED8D1C7A5DA5
BA0D07CF0ADD30F7A110FE0D38716725

round [16].s_row:

CFCE333B187A30255FD2B1C91CDD6798
7176CC8D0A71AA5A49CAEDCF38B08D27
166B070D2A886FE4550DFE80EC308966
BA106279127C81A5A11A54D4C5125DF7

round [16].s_box:

EC007FEE86D1991C020C7AFBB8E2FFED
08BB6401D2A2F7E52C5F8D4D6C9E878E
5541A422F716BBAA7F69B8DEB970C72F
7A3D181DE83061DC3F40F608A86883D3

round [15].r_key:

6EE6585393E1EE1B135205F0A2AA9DCB
7261FD305AF67A44615EECA32F1AF6DC
3E9ED8552F8E2184212A29ADAD8BFAAF
395EC388282AD278E2B3C8BB565E14CA

round [15].xor_rkey:

82E627BD15307707115E7F0B1A486226
7ADA993188548DA14D0161EE43847152
6BDF7C77D8989A2E5E43917314FB3D80
4363DB95C01AB3A4DDF33EB3FE369719

round [15].m_col:

1E967AF412155E06D9EEF54E351FEE4D
3F895FFA41C692548D072B28FE44CB46
7E0123010E9ACBB0CBA22BCB1046AC43
2AAC6E7C10367D0A47D003B38E28BF06

round [15].s_row:
 1EEE5F280E467D06D9892B011036BF06
 3F0723CB10285E4D8D012B7C8E15EE54
 7EA26EB3121F9246CBAC03F435C6CBB0
 2AD07A4E4144CB434796F5FAFE9AAC0A

round [15].s_box:
 6F4FD57C27B14DC5E56C12B6E31AD3C5
 8C9CD9E0E3C37E03EFF2127B7811AD0C
 D485750BE8DC481213DE4345C4EA4ED1
 F7E32A065F364E8A5E64D16E82C468C4

round [14].r_key:
 8BFAAF395EC388282AD278E2B3C8BB56
 5E14CA6EE6585393E1EE1B135205F0A2
 AA9DCB7261FD305AF67A44615EECA32F
 1AF6DC3E9ED8552F8E2184212A29ADAD

round [14].xor_rkey:
 E4B57A457972C5EDCFBE6A5450D26893
 D288138E059B2D900E1C09682A145DAE
 7E18BE7989217848E5A407249A06EDFE
 ED15F638C1EE1BA5D045554FA8EDC569

round [14].m_col:
 779EDA9AF81061FB18756FC4EF00153A
 F49ADA1377BBF638DC9C033A3D2E37F2
 CE0DBE23DAFE0E1A2E20E44B0D8666E8
 5F840FF7D4279EC5292E84CB00E29B86

round [14].s_row:
 7775DA3ADA869E86189A03230D279BFB
 F49CBE4BD4E2613ADC0DE4F700101538
 CE200FCBF800F6F22E84849AEFBB371A
 5F2EDAC4772E0EE8299E6F133DFE66C5

round [14].s_box:
 79286E3C8597534786C4434CD3FB259C
 388AC505C6CCEB3C406919D3A43D6B41
 B26F95E0D583E02850C5CE89C101963B
 02326E5D79323A36E924BB18CE9378B7

round [13].r_key:
 960C0ED1D55D6345CEC2D12BE6F9A433
 EAF35706A8BFB92B1AC05DCE9641701
 AA2A7035EB4ADB4611540BDAE457EF2C
 9F46A4B2131CE39F641F95399AC82BE8

round [13].xor_rkey:
 EF2460ED50CA300248069267350281AF
 D275F075AC4710AEF1C51C0F4D597C40
 1845E5D53EC93B6E4191C55325567917
 9D74CAEF6A2ED9A98D3B2E21545B535F

round [13].m_col:
 CCF07F22784BF5B91D6C5FF525A11611
 80239CE20E8B27709188F8E811CAA10
 E26AC5B4C813E00B9216A874C5C332FB
 35FCBADB4BCB502A013610BCC67E0AC8

round [13].s_row:
 CC6C9CE8C8C350C81D23F8B4C5CB0AB9
 8088C5744B7EF511916AA8DBC64B1670
 E216BABC78A1271092FC1022258BAA0B
 35367FF50ECAE0FB01F05FE21113322A

round [13].s_box:
 49736536DFAB945412BAFCDBA805E6AC
 FF16E8EC1D84D1279E9B937A2FA31E30
 524C0871A057908230665010F9B0F7E8
 C41AE71E275F2D9CA2F3D5BEA106C807

round [12].r_key:
 57EF2C9F46A4B2131CE39F641F95399A
 C82BE8960C0ED1D55D6345CEC2D12BE6
 F9A433EAF35706A8BFB92B1AC05DCE9
 641701AA2A7035EB4ADB4611540BDAE4

round [12].xor_rkey:
 1E9C49A9990F26470E5963BFB790DF36
 373D007A118A00F2C3F8D6B4ED7235D6
 ABE83B9B5F62E0E8BB9DC2A155B52B01
 A00DE6B40D2F1877E82893AFF50D12E3

round [12].m_col:
 BB8FDBD2C9C5E81A55FCFDC17935C25C
 C694D50DDFC4E752C945BBE799B52742
 C65BDA251CCA772EFEC97772BA742687
 BF0DEAE431E91A03551B43ADB896B82B

round [12].s_row:
 BBFCD5E71C741A2B5594BB25BAE9B81A
 C645DA723196E85CC95B77E4B8C5C252
 C6C9EAADC935E742FE0D43D279C4272E
 BF1BDBC1DFB57787558FFD0D99CA2603

round [12].s_box:
 3E6651D0B8D3B4C77FC2161C7A08693B
 2F656E60B764DED7145363AADB181309
 2F82CBEB14D9EAAE8269BF3D189490A1
 2992F39E097563D67F997922BB5FC911

round [11].r_key:
 5BF6FA6800DDB7EAB72207EDCAEA4BE0
 32B17BD159F53409557B3D5937AC33BD
 7108908144534C705F59BD1325EE3A7A
 0DD48DC1DE569F3C558DE51DAD7BC277

round [11].xor_rkey:
 6590ABB8B80E032DC8E011F1B0E222DB
 1DD415B1EE91EAD41285EF3ECB420B4
 5E8A5B6A508AA6DEDD30022E3D7AAADB
 24467E5FD723FCEA2A149C3F16240B66

round [11].m_col:
 76FCFEBC24B47325BBD30462B2F782AD
 9AD30988A97D152AF045660D4F777E04
 1C7E08BF776EB61AA284D1FB25FBEB03
 4A4E31E79E1F06B795650FFB07407CB9

round [11].s_row:
 76D3090D77FB06B9BBD366BF251F7C25
 9A4508FB9E4073ADF07ED1E707B4822A
 1C8431FB24F71504A24E0FBCB27D7E1A
 4A65FE62A977B60395FC04884F6EEBB7

round [11].s_box:
 AFCA382279EDEDAC3ECA788DF9DC6D1C
 2665C29C32A9B0EB0D842ED0D913CF07
 B8C5AE9C72336BA7AE4B95717690773B

4B14B8725DC9C1110B66F16923C1A91A

round [10].r_key:

EE3A7A0DD48DC1DE569F3C558DE51DAD
7BC2775BF6FA6800DDB7EAB72207EDCA
EA4BE032B17BD159F53409557B3D5937
AC33BD7108908144534C705F59BD1325

round [10].xor_rkey:

41F0422FAD602C72685544D8743970B1
5DA7B5C7C453D8EBD033C467FB1422CD
528E4EAEC348BAFE5B7F9C240DAD2E0C
E727050355594055582A81367A7CBA3F

round [10].m_col:

2640074EBA5EB18614269F1D21D4C787
23EFFF860A055371493FA5BBE6F458B6
EF31726B2D1ACA4EF5F4B6C76F1A9C49
618B8BD11F39BDC7592F28CCF607BC22

round [10].s_row:

2626FFBB2D1ABD2214EFA56B6F39BC86
233F72C71F07B1874931B6D1F65EC771
EFF48BCCBAD453B6F58B284E2105584E
612F071D0AF4CA4959409F86E61A9CC7

round [10].s_box:

BF31E1E1AC40BC107CA441E21CD8A747
56762FAF289C7AD62C20C12CBEE6885F
C125FB357A7828927BB098068ABFE306
33D2A49BD225B2A807A90C47FA4065AF

round [9].r_key:

34844549D7CCD2614CAF999621D04AE6
E4E761902EAE3200BD7272547B0D5F3E
E6D1D63DDE071BFF1AAE96D187DCF1F4
BA9B849636BB67541B02E47B4263A81E

round [9].xor_rkey:

8BB5A4A87B8C6E71300BD8743D08EDA1
B2914E3F063248D69152B378C5EBD761
27F42D08A47F336D611E0ED70D6312F2
8949200DE49ED5FC1CABE83CB823CDB1

round [9].m_col:

8EB026A5F50087F0B90DA3B63BB26F59
11373C833B855A2FED1194C7A02CFCCF
7C9FDD92C02B2C2A2037E2063544CB9F
7187E71A7CBE482E3FF813FE03A520D7

round [9].s_row:

8E0D3CC7C04448D7B937949235BE20F0
1111DD067CA58759ED9FE21A03006F2F
7C37E7FEF5B25ACF208713A53B85FC2A
71F826B63B2C2C9F3FB0A383A02BCB2E

round [9].s_box:

786921AFF2365F93EB5D1459C4E5A8F3
A188BEC5FC7D80F4F338673BC583BB21
FC5DEAD47B0BEC4DCDE4E2DC77CB0707
080FC99277E131918C9E1717A7614EA1

round [8].r_key:

DCF1F4BA9B849636BB67541B02E47B42
63A81E34844549D7CCD2614CAF999621

D04AE6E4E761902EAE3200BD7272547B
0D5F3EE6D1D63DDE071BFF1AAE96D187

round [8].xor_rkey:

A498D51569B2C9A5503A4042C601D3B1
C220A0F17838C9233FEA06776A1A2D00
2C170C309C6A7C6363D6E26105B9537C
0550F774A6370C4F8B85E80D09F79F26

round [8].m_col:

4EAC3060E2D37F4EA3FC395DDEF0AB50
0234EB5BF58B2AF6D960C42A6C71F075
62AB2207CF1193BF5686EF58E678683D
DB5495B6E0A141E282FDDE2B93C7B2C1

round [8].s_row:

4EFCEB2ACF7841C1A334C407E6A1B24E
02602258E0C77F50D9ABEFB693D3ABF6
6286952BE2F02A755654DE60DE8BF0BF
DBFD305DF571933D82AC395B6C1168E2

round [8].s_box:

F466A907ECAE3B9E22EC32A6FA573E06
A95E052019FCE7B5E54649922ECAACA4
DD979AC752F3DCA5FE3C3D6F9BB0828D
6B6399317BA20013CFDEF47F0688DBBE

round [7].r_key:

6AF398D679DD5E44373F6E0046EF7D2C
1811C3EEB79C3C3C318798F419843CCC
1A3B0E81E3EB16993DB77B793D20870D
454F42C076BA2CAD468083096A305939

round [7].xor_rkey:

9E9531D1957365DA15D35CA6BCB8432A
B14FC6CEAE60DB89D4C1D166374E9068
C7AC9446B118CA3CC38B4616A6900580
2E2CDBF10D182CBE895E77766CB88287

round [7].m_col:

EF6AF2CE89C438B1617B597D5E9078A4
645A3056497B202F98AB079FDDA59BB8
E5495503A338E1021EFE133E0B5A589D
CCF445EF8531794836949D634E0ADD31

round [7].s_row:

EF7B309FA35A7931615A07030B31DDB1
64AB553E850A38A4984913EF4EC4782F
E5FE4563899020B81EF49DCE5E7B9B02
CC94F27D49A5E19D366A5956DD385848

round [7].s_box:

C15A999122F4D25033F4A411AD20BE5B
E2465629F88D6F98A659E2DFF4943521
A39306868E0DA8FA6F254C3ACB5A2523
49C2BAE62C7D1FD5749B0F3821B4E355

round [6].r_key:

20870D454F42C076BA2CAD468083096A
3059396AF398D679DD5E44373F6E0046
EF7D2C1811C3EEB79C3C3C318798F419
843CCC1A3B0E81E3EB16993DB77B793D

round [6].xor_rkey:

E1DD94D46DB6122689D809572DA3B731

D21F6F430B15B9E17B07A6E8CBFA3567
4CEE2A9E9FCE464DF319700B4CC2D13A
CDFE76FC17739E369F8D960596CF9A68

round [6].m_col:

BDA6ADC29293AC73F5FBFF8BE4A26DA5
F19C5306C0282C77E762F357506A99AE
C01C87484B84D943007EC3658D37F416
24D338A0072EE28C27A40CA11BDE455F

round [6].s_row:

BDFB53574B37E25FF59CF3488D2E4573
F162876507DEACA5E71CC3A01B936D77
C07E38A192A22CAE00D30CC2E4289943
24A4AD8BC06AD91627A6FF065084F48C

round [6].s_box:

B3ED28FC1D5D67667B8AC355EF320604
BA7980A3D9DA68DC511546878D91848B
F2846F5830853152A4CAF9545C3928A
727C2699F29B012D4FE7E1C5D6C5159A

round [5].r_key:

7ABF1C948560329A3ADB72EAF96939C6
C32280C2190892662B53B1C4BE93FAAC
278CD9FB41142C97E6C4C075C03AB865
3D55C6C2361C0FB381BB07F3EE5509ED

round [5].xor_rkey:

C9523468983D55FC4151B1BF165B3FC2
795B0061C0D2FABA7A46F74333027E27
D508B6A371911DC5420E3DE085F92AEF
4F29E05BC4870E9ECE5CE63638901C77

round [5].m_col:

A4C9D5EF4942C81326DD46DA423CA635
70A253EE8435187E0B97D60FD61A2D4F
29E427A5E9EA27A53ED0D92FDEBA7AD0
CC3B5F9BBCAA18C87BDBE8461DF887C4

round [5].s_row:

A4DD530FE9BA18C426A2D6A5DEAA8713
7097272FBCF8C8350BE4D99B1D42A67E
29D05F46493C184F3E3BE8EF42352DA5
CCDBD5DA841A27D07BC946EED6EA7AC8

round [5].s_box:

3DE228C3B51B5A5DBF8573DC9B278018
977790215C0F2BD9ADA8016812103081
E9E3D5122C555A4920A5DEDF44D92CDC
49EE51B8914090AD6D82EE53ED042A54

round [4].r_key:

3AB8653D55C6C2361C0FB381BB07F3EE
5509ED7ABF1C948560329A3ADB72EAF9
6939C6C32280C2190892662B53B1C4BE
93FAAC278CD9FB41142C97E6C4C075C0

round [4].xor_rkey:

075A4DFEE0DD986BA38AC05D202073F6
C27E7D5BE313BF5CCD9A9B52C962DA78
80DA13D10ED598502837B8F41768E862
DA14FD9F1D996BEC79AE79B529C45F94

round [4].m_col:

283615ED7BEE50691B2ABF01D4F5D08C
C78311AE6BADAEEA74976F1789CA93453
DAEB896FEF0D4C6AC8B0DC7F1D2127D6
7B38D106002839922CD01A59B5A4850B

round [4].s_row:

282A1178EF21390B1B83F16F1D288569
C776897F00A4508C49EBDC06B5EED0A7
DAB0D1597BF5AE53C8381AEDD4AD346A
7BD015016BA94CD62C36BFAE9C0D2792

round [4].s_box:

738044E7C1F8F4E88D7EE4B412C327BC
75BBC7F8A47C949A2C020DC59A4F58C0
859E2EF46D1CC416DFB4B424C6DFF9CC
6DE36BB604AC3C4A161AD35248699059

round [3].r_key:

AAC40DA0DFE7DD98A3C0E63B2B40CD20
F474D504D7C2076D2C7A0E475E355CE3
029B22C288AC137514446EC52D75BF56
5AD96E1C1A6BDA477636C46E069EA5A6

round [3].xor_rkey:

D94449471E1F29702EBE028F3983EA9C
81CF12FC73BE93F700780382C47A0423
87050C36E5B0D763CBF0DAE1EBAA469A
373A05AA1EC7E60D602C173C4EF735FF

round [3].m_col:

22DA1D793AAB119B190A728DDFFD5A8D
CA6FAADDF75AF18F7674CF0E4142011F
A8D24A5551DB5C03ABFE407FB0F17C08
1DBB694315FD3145E6C7E2BF0BEB30C7

round [3].s_row:

220AAA0E51F131C7196FCF55B0FD309B
CA744A7F15EB118D76D240430BAB5A8F
A8FE69BF3AFDF11FABBBE279DF5A0103
1DC71D8DF7425C08E6DA72DD41DB7C45

round [3].s_box:

708DF743EAC0AEAF395C912A8B639968
FBD310F82A024401AF0C9E8AAD46EC85
0093A18D9363E40F4A01671D09F4D411
12FC8A01D0102439FA812F7D5FEE6D33

round [2].r_key:

75BF565AD96E1C1A6BDA477636C46E06
9EA5A6AAC40DA0DFE7DD98A3C0E63B2B
40CD20F474D504D7C2076D2C7A0E475E
355CE3029B22C288AC137514446EC52D

round [2].xor_rkey:

0532A11933AEB2B55286D65CBDA7F76E
6576B652EE0FE4DE48D106296DA0D7AE
405E8179E7B6E0D888060A3173FA934F
27A069034B32E6B156925A691B80A81E

round [2].m_col:

F77F3AFE062C0191640A11BF3D750F4C
03A17B2D1DBFE52BC722D00A8A617C8F
032B2E66D052D46BA98B66D626B5977D
1C366C3248DA6F923F2F35AE59E26F60

```
round [2].s_row:
F70A7B0AD0B56F6064A1D06626DA6F91
03222ED648E2014CC72B6632592C0F2B
038B6CAE0675E58FA93635FE3DBF7C6B
1C2F3ABF1D61D47D3F7F112D8A529792
```

```
round [2].s_box:
D08D59C4E475BB6FE257582FBF81BBF9
C526474A61CCD4F67561784E07E195C7
C5B0765203287B855D1A4FD4CE876DE2
B8D2B38D12D61BE68CF94414B6CD5B59
```

```
round [1].r_key:
A18071E1A12F9FA68E67BAB6699A6A0A
81E8161C01BD0D7CEB155308A72773FC
96E926C9E7392C3EF6E7FE7353D0BD18
C6CD8929062FBC7B491C04FE6AD7C797
```

```
round [1].xor_rkey:
710D2825455A24C96C30E299D61BD1F3
44CE51566071D98A9E742B46A0C6E63B
5359509BE41157BBABFDB1A79D57D0FA
7E1F3AA414F9A79DC5E540EADC1A9CCE
```

```
round [1].m_col:
916E9E60C3E18529ABD8346EE78E0C71
7E705B52B14F6454EFCE9E91694C46F0
094B0D2CC049F10396C661C75F0FD60F
5090346BF97860A8BF387118DC3675A1
```

```
round [1].s_row:
91D85B91C00F60A1AB709E2C5F787529
7ECE0DC7F9368571EF4B616BDCE10C54
09C63418C38E64F096907160E74F4603
50389E6EB14CF10FBF6E34526949D6A8
```

```
round [1].s_box:
9E3E9DF9F2297C584AA6535E02AED694
D400B6AF691A275FC1A3EBE240B5FD0C
0FEAF95C6E52CDF3540D1A6F51C8EE11
D6B453429F50E4C329C1F90992597376
```

```
round [0].sub_rkey:
CE80843325A052521BEAD714E6A9D829
FD381E0EE9A845BD92044554D9FA46A3
757FEFDB853BB1F297FF9D833B75E66A
AF4157ABB5291BDCF094BB13AA5AFF22
```

```
PLAINTEXT:
CE80843325A052521BEAD714E6A9D829
FD381E0EE9A845BD92044554D9FA46A3
757FEFDB853BB1F297FF9D833B75E66A
AF4157ABB5291BDCF094BB13AA5AFF22
```

В.3 Гамування

В.3.1 Зашифрування з використанням 128-бітного блоку і 128-бітового ключа базового перетворення

```
KEY:
000102030405060708090A0B0C0D0E0F
```

```
IV:
101112131415161718191A1B1C1D1E1F
```

```

PLAINTEXT (N = 328):
  202122232425262728292A2B2C2D2E2F
  303132333435363738393A3B3C3D3E3F
  404142434445464748
ctr:
  81BF1C7D779BAC20E1C9EA39B4D2AD06

ctr + 1:
  82BF1C7D779BAC20
gamma [0]:
  892B49B4A48EF9F8DE643EDE6FB3A6DD

CIPHERTEXT [0]:
  A90A6B9780ABDFDFF64D14F5439E88F2

ctr + 2:
  83BF1C7D779BAC20
gamma [1]:
  56ED62DEE77464BAEDDFA2D9CC3DF01E

CIPHERTEXT [1]:
  66DC50EDD341528DD5E698E2F000CE21

ctr + 3:
  84BF1C7D779BAC20
gamma [2]:
  B83398BABA5D57C302
CIPHERTEXT [2]:
  F872DAF9FE1811844A
CIPHERTEXT:
  A90A6B9780ABDFDFF64D14F5439E88F2
  66DC50EDD341528DD5E698E2F000CE21
  F872DAF9FE1811844A

```

В.3.2 Розшифрування з використанням 128-бітного блоку і 128-бітового ключа базового перетворення

```

KEY:
  0F0E0D0C0B0A09080706050403020100

IV:
  1F1E1D1C1B1A19181716151413121110

CIPHERTEXT (N = 20):
  2F2E2
ctr:
  2BD453E6AA2AE668B2F5AA6B1B942D51

ctr + 1:
  2CD453E6AA2AE668
gamma [0]:
  88907
PLAINTEXT [0]:
  A7BE5
PLAINTEXT:
  A7BE5

```

В.3.3 Зашифрування з використанням 128-бітного блоку і 256-бітового ключа базового перетворення

```

KEY:
  000102030405060708090A0B0C0D0E0F
  101112131415161718191A1B1C1D1E1F

```

```

IV:
    202122232425262728292A2B2C2D2E2F

PLAINTEXT (N = 259):
    303132333435363738393A3B3C3D3E3F
    404142434445464748494A4B4C4D4E4F
    4
ctr:
    58EC3E091000158A1148F7166F334F14

ctr + 1:
    59EC3E091000158A
gamma [0]:
    AFD2A02F391BF43659E8C23969DE4A59

CIPHERTEXT [0]:
    9FE3921C0D2EC20161D1F80255E37466

ctr + 2:
    5AEC3E091000158A
gamma [1]:
    C2F6F66E086B0F32FEBF7809526312B3

CIPHERTEXT [1]:
    82B7B42D4C2E4975B6F632421E2E5CFC

ctr + 3:
    5BEC3E091000158A
gamma [2]:
    6
CIPHERTEXT [2]:
    2
CIPHERTEXT:
    9FE3921C0D2EC20161D1F80255E37466
    82B7B42D4C2E4975B6F632421E2E5CFC
    2
    
```

В.3.4 Розшифрування з використанням 128-бітного блоку і 256-бітового ключа базового перетворення

```

KEY:
    1F1E1D1C1B1A19181716151413121110
    0F0E0D0C0B0A09080706050403020100

IV:
    2F2E2D2C2B2A29282726252423222120

CIPHERTEXT (N = 327):
    5F5E5D5C5B5A59585756555453525150
    4F4E4D4C4B4A49484746454443424140
    3F3E3D3C3B3A393836
ctr:
    453892E3B75A9F8D796FC76AD6DF871B

ctr + 1:
    463892E3B75A9F8D
gamma [0]:
    D898141C5044B97AA536A091D901CD06

PLAINTEXT [0]:
    87C649400B1EE022F260F5C58A539C56

ctr + 2:
    
```

473892E3B75A9F8D
 gamma [1]:
 44C541D6046612B6751D5B71AF376017

PLAINTEXT [1]:
 0B8B0C9A4F2C5BFE325B1E35EC752157

ctr + 3:
 483892E3B75A9F8D
 gamma [2]:
 30E809ED407F4927FE
 PLAINTEXT [2]:
 0FD634D17B45701FC8
 PLAINTEXT:
 87C649400B1EE022F260F5C58A539C56
 0B8B0C9A4F2C5BFE325B1E35EC752157
 0FD634D17B45701FC8

В.3.5 Зашифрування з використанням 256-бітного блоку і 256-бітового ключа базового перетворення

KEY:
 000102030405060708090A0B0C0D0E0F
 101112131415161718191A1B1C1D1E1F

IV:
 202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 641):
 404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F
 808182838485868788898A8B8C8D8E8F
 8

ctr:
 F66E3D570EC92135AEDAE323DCBD2A8C
 A03963EC206A0D5A88385C24617FD92C

ctr + 1:
 F76E3D570EC92135AEDAE323DCBD2A8C

gamma [0]:
 1EA03E37DF305AD62B128A84B143EF60
 10293B0DC89136FD70DE45D68F8927AA

CIPHERTEXT [0]:
 5EE17C749B751C91635BC0CFFD0EA12F
 4078695E9CC460AA28871F8DD3D479F5

ctr + 2:
 F86E3D570EC92135AEDAE323DCBD2A8C

gamma [1]:
 EB8081F3A9962DF4245B61B824386740
 6FCF208BF133220E59951B97D733201F

CIPHERTEXT [1]:
 8BE1E390CDF34B934C320BD34855092F
 1FBE52F88546547921EC61ECAB4E5E60

ctr + 3:
 F96E3D570EC92135AEDAE323DCBD2A8C

```

gamma [2]:
  06F09C24195E25B3FB60BA8E624731E1
  0
CIPHERTEXT [2]:
  86711EA79DDBA33473E93005EECABF6E
  8
CIPHERTEXT:
  5EE17C749B751C91635BC0CFFD0EA12F
  4078695E9CC460AA28871F8DD3D479F5
  8BE1E390CDF34B934C320BD34855092F
  1FBE52F88546547921EC61ECAB4E5E60
  86711EA79DDBA33473E93005EECABF6E
  8

```

В.3.6 Розшифрування з використанням 256-бітного блоку і 256-бітового ключа базового перетворення

```

KEY:
  1F1E1D1C1B1A19181716151413121110
  0F0E0D0C0B0A09080706050403020100

IV:
  3F3E3D3C3B3A39383736353433323130
  2F2E2D2C2B2A29282726252423222120

CIPHERTEXT (N = 646):
  9F9E9D9C9B9A99989796959493929190
  8F8E8D8C8B8A89888786858483828180
  7F7E7D7C7B7A79787776757473727170
  6F6E6D6C6B6A69686766656463626160
  5F5E5D5C5B5A59585756555453525150
  4C
ctr:
  E8C634A546F149943807C671364737F1
  A69ED12D61DE20F4817CCFC41588870F

ctr + 1:
  E9C634A546F149943807C671364737F1

gamma [0]:
  1F135C5BB16357AD286515D37A649E8A
  D19DF9C138EB5DEDABE4204551D762BD

PLAINTEXT [0]:
  808DC1C72AF9CE35BFF38047E9F60F1A
  5E13744DB361D4652C62A5C1D255E33D

ctr + 2:
  EAC634A546F149943807C671364737F1

gamma [1]:
  36FA8214B0E26378F30EBF4B22F337D2
  8D108DD56436453520634225DE1B5780

PLAINTEXT [1]:
  4984FF68CB981A008478CA3F518146A2
  E27EE0B90F5C2C5D47052741BD7936E0

ctr + 3:
  EBC634A546F149943807C671364737F1

gamma [2]:
  E7BBCFA4C9D4F3490BC298ECAB17AA1D

```

90

PLAINTEXT [2]:

B8E592F8928EAA115C94CDB8F845FB4D
DC

PLAINTEXT:

808DC1C72AF9CE35BFF38047E9F60F1A
5E13744DB361D4652C62A5C1D255E33D
4984FF68CB981A008478CA3F518146A2
E27EE0B90F5C2C5D47052741BD7936E0
B8E592F8928EAA115C94CDB8F845FB4D
DC

В.3.7 Зашифрування з використанням 256-бітного блоку і 512-бітового ключа базового перетворення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

PLAINTEXT (N = 643):

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFA
A

ctr:

606990E9E6B7B67A4BD6D893D72268B7
8E02C83C3CD7E102FD2E74A8FDFE5DD9

ctr + 1:

616990E9E6B7B67A4BD6D893D72268B7

gamma [0]:

BE3C36DBC4EF25E73730891939ACB0
C8444A33A567039D85EEFE6125E63EC7

CIPHERTEXT [0]:

DE5D54B8ABB189428F5E5AE27554C2DF
B8353840D11275EAFD97841A599B40B8

ctr + 2:

626990E9E6B7B67A4BD6D893D72268B7

gamma [1]:

4943781AAB5563BE0221E9FAF90AB5D4
E30AA2BCE995194D78EC95E494AE6057

CIPHERTEXT [1]:

C9C2FA992FD0E5398AA8637175873B5B
739B302F7D008FDAE0750F7F0833FEC8

ctr + 3:

636990E9E6B7B67A4BD6D893D72268B7

gamma [2]:

4F79F37B7F138C34CF954DAB337F77C3
E

CIPHERTEXT [2]:
EFD851D8DBB62A93673CE7009FD2D96C
4
CIPHERTEXT:
DE5D54B8ABB189428F5E5AE27554C2DF
B8353840D11275EAFD97841A599B40B8
C9C2FA992FD0E5398AA8637175873B5B
739B302F7D008FDAE0750F7F0833FEC8
EFD851D8DBB62A93673CE7009FD2D96C
4

В.3.8 Розшифрування з використанням 256-бітного блоку і 512-бітового ключа базового перетворення

KEY:
3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:
5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140

CIPHERTEXT (N = 645):
BFBEBCB9B8B7B6B5B4B3B2B1B0
AFAEADACABAAA9A8A7A6A5A4A3A2A1A0
9F9E9D9C9B9A99989796959493929190
8F8E8D8C8B8A89888786858483828180
7F7E7D7C7B7A79787776757473727170
68

ctr:
275F9FCC346002A3ADE1D077256EC867
F89C8C40E3C0740376D1AEB0D9CF71AB

ctr + 1:
285F9FCC346002A3ADE1D077256EC867

gamma [0]:
A5FC3EBA0B43CFA98F49212B49ECE2B3
9DAAE95FADC65BD4771D5F6BCD128DE6

PLAINTEXT [0]:
1A428306B0F9761138FF949FFA5E5303
320444F3066CF27CD0BBFACF6EB02C46

ctr + 2:
295F9FCC346002A3ADE1D077256EC867

gamma [1]:
762F7DF339C6FF1B110202FB9ABBE157
1C1CFA6E36D52B2751B5AE505D50E15C

PLAINTEXT [1]:
E9B1E06FA25C66838694976F092970C7
939277E2BD5FA2AFD6332BD4DED260DC

ctr + 3:
2A5F9FCC346002A3ADE1D077256EC867

gamma [2]:
D2613EEB3B2DA009E3A9CE191B30C8E9
98

PLAINTEXT [2]:

AD1F43974057D97194DFBB6D6842B999
F0

PLAINTEXT:

1A428306B0F9761138FF949FFA5E5303
320444F3066CF27CD0BBFACF6EB02C46
E9B1E06FA25C66838694976F092970C7
939277E2BD5FA2AFD6332BD4DED260DC
AD1F43974057D97194DFBB6D6842B999
F0

В.3.9 Зашифрування з використанням 512-бітного блоку і 512-бітового ключа базового перетворення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

PLAINTEXT (N = 770):

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
C

ctr:

4A26E31B811C356AA61DD6CA0596231A
67BA8354AA47F3A13E1DEEC320EB56B8
95D0F417175BAB662FD6F134BB15C86C
CB906A26856EFEB7C5BC6472940DD9D9

ctr + 1:

4B26E31B811C356AA61DD6CA0596231A
67BA8354AA47F3A13E1DEEC320EB56B8

gamma [0]:

E2C78014E3B8D68040065D7ACEDD5680
80B5E782FBAE27841D14712510CD716B
42031EB212F349671734ECEC16391BAD
481EF4948589151D527646CBC01A9266

CIPHERTEXT [0]:

62460297673D5007C88FD7F14250D80F
102475116F3BB113858DEBBE8C50EFF4
E2A2BC11B656EFC0BF9D4647BA94B502
F8AF4627313CA3AAEACFFC707CA72CD9

ctr + 2:

4C26E31B811C356AA61DD6CA0596231A
67BA8354AA47F3A13E1DEEC320EB56B8

gamma [1]:

699ADE0DCC198B136023CDAE54ACCD0D
CBADDF632F63D425A1687AD6829224C7
4

CIPHERTEXT [1]:

A95B1CCE08DC4DD4A8EA0765986103C2
1B7C0DB0FBB602F279B1A00D5E4FFA18
8

CIPHERTEXT:

62460297673D5007C88FD7F14250D80F
102475116F3BB113858DEBBE8C50EFF4
E2A2BC11B656EFC0BF9D4647BA94B502
F8AF4627313CA3AAEACFFC707CA72CD9
A95B1CCE08DC4DD4A8EA0765986103C2
1B7C0DB0FBB602F279B1A00D5E4FFA18
8

В.3.10 Розшифрування з використанням 512-бітного блоку і 512-бітового ключа базового перетворення

KEY:

3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:

7F7E7D7C7B7A79787776757473727170
6F6E6D6C6B6A69686766656463626160
5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140

CIPHERTEXT (N = 775):

EFEEDECEBEAE9E8E7E6E5E4E3E2E1E0
DFDEDDDCDBDAD9D8D7D6D5D4D3D2D1D0
CFCECDCCBCAC9C8C7C6C5C4C3C2C1C0
BFBEBDBCBBBAB9B8B7B6B5B4B3B2B1B0
AFAEADACABAAA9A8A7A6A5A4A3A2A1A0
9F9E9D9C9B9A99989796959493929190
8E

ctr:

E92E8C484D8715E1F7E5AED8183EA3E6
074E5F9D1EB12DC496D51A020CE0F3C0
77B19A262233644999A6AFB9DD4CAA17
74A00201070A3C7A67DD4678A6347A9E

ctr + 1:

EA2E8C484D8715E1F7E5AED8183EA3E6
074E5F9D1EB12DC496D51A020CE0F3C0

gamma [0]:

90F979181E67FFE6BE669FAFE8351C12
D4DCC6BB51DB9E28208D9F9F7F29940F
4B89F63062D04706497E7284883B350F
9519009D975F843FBD4F1116B0C6BE19

PLAINTEXT [0]:

7F1794F4F58D160E59807A4B0BD7FDF2
0B021B678A0147F0F75B4A4BACFB45DF
84473BFCA91A8ECE8EB8B7404BF9F4CF
2AA7BD212CE53D870AF9A4A203740FA9

ctr + 2:

EB2E8C484D8715E1F7E5AED8183EA3E6
074E5F9D1EB12DC496D51A020CE0F3C0

gamma [1]:

86842D287BB08EDEC83B14ED50E2A4E9
2ECE14076C11F2BB19490B423746EE06

50
 PLAINTEXT [1]:
 292A8084D01A27766F9DB149F3400549
 B150899BF78B6B238EDF9ED6A4D47F96
 DE
 PLAINTEXT:
 7F1794F4F58D160E59807A4B0BD7FDF2
 0B021B678A0147F0F75B4A4BACFB45DF
 84473BFCA91A8ECE8EB8B7404BF9F4CF
 2AA7BD212CE53D870AF9A4A203740FA9
 292A8084D01A27766F9DB149F3400549
 B150899BF78B6B238EDF9ED6A4D47F96
 DE

В.4 Гамування зі зворотнім зв'язком за шифртекстом

В.4.1 Зашифрування з використанням 128-бітного блоку і 128-бітового ключа базового перетворення, $q = 128$ (Калина-128/128-CFB-128)

$q = 128$
 KEY:
 000102030405060708090A0B0C0D0E0F
 IV:
 101112131415161718191A1B1C1D1E1F
 PLAINTEXT (N = 384):
 202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F
 404142434445464748494A4B4C4D4E4F
 gamma [1]:
 81BF1C7D779BAC20E1C9EA39B4D2AD06
 CIPHERTEXT [1]:
 A19E3E5E53BE8A07C9E0C01298FF8329
 ctr + 1:
 A19E3E5E53BE8A07C9E0C01298FF8329
 gamma [2]:
 2FBFD412152588089DFE16B39CBF6C34
 CIPHERTEXT [2]:
 1F8EE6212110BE3FA5C72C88A082520B
 ctr + 2:
 1F8EE6212110BE3FA5C72C88A082520B
 gamma [3]:
 661432BD6C2D415E91FD0C155AD68D35
 CIPHERTEXT [3]:
 265570FE28680719D9B4465E169BC37A
 ctr + 3:
 265570FE28680719D9B4465E169BC37A
 CIPHERTEXT:
 A19E3E5E53BE8A07C9E0C01298FF8329
 1F8EE6212110BE3FA5C72C88A082520B
 265570FE28680719D9B4465E169BC37A

В.4.2 Розшифрування з використанням 128-бітного блоку і 128-бітового ключа базового перетворення, $q = 1$ (Калина-128/128-CFB-1)

```

q = 1
KEY:
    0F0E0D0C0B0A09080706050403020100

IV:
    1F1E1D1C1B1A19181716151413121110

CIPHERTEXT (N = 10):
    FF4
gamma [1]:
    2BD453E6AA2AE668B2F5AA6B1B942D51

PLAINTEXT [1]:
    0
ctr + 1:
    2BD453E6AA2AE668B2F5AA6B1B942D51

gamma [2]:
    4786133CE9550950ABB8F71ABDB4D8FB

PLAINTEXT [2]:
    0
ctr + 2:
    4786133CE9550950ABB8F71ABDB4D8FB

gamma [3]:
    9F9362D2C8B498140437024EB34FF716

PLAINTEXT [3]:
    1
ctr + 3:
    9F9362D2C8B498140437024EB34FF717

gamma [4]:
    423CE86C7B0B32573A5E54E3049D89AB

PLAINTEXT [4]:
    0
ctr + 4:
    423CE86C7B0B32573A5E54E3049D89AB

gamma [5]:
    B04B9F47D0B232C7358650A32B25A838

PLAINTEXT [5]:
    1
ctr + 5:
    B04B9F47D0B232C7358650A32B25A839

gamma [6]:
    D37DE19FFA289B6909EA63173C9E8BD6

PLAINTEXT [6]:
    1
ctr + 6:
    D37DE19FFA289B6909EA63173C9E8BD7

gamma [7]:
    6A156BEA70FD049472AB4AE54F20C8DD

PLAINTEXT [7]:

```

```

0
ctr + 7:
6A156BEA70FD049472AB4AE54F20C8DD

gamma [8]:
8BBAE40D95E653A2124BDE763509250B

PLAINTEXT [8]:
0
ctr + 8:
8BBAE40D95E653A2124BDE763509250B

gamma [9]:
D41F5AFEC704D54C840867B6E6A05E84

PLAINTEXT [9]:
0
ctr + 9:
D41F5AFEC704D54C840867B6E6A05E84

gamma [10]:
331E88173C8CF63554ADE06263B53613

PLAINTEXT [10]:
0
ctr + 10:
331E88173C8CF63554ADE06263B53613

PLAINTEXT:
2C0

```

В.4.3 Зашифрування з використанням 128-бітного блоку і 256-бітового ключа базового перетворення, $q = 8$ (Калина-128/256-CFB-8)

```

q = 8
KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F

PLAINTEXT (N = 85):
3031323334353637383938
gamma [1]:
58EC3E091000158A1148F7166F334F14

CIPHERTEXT [1]:
24
ctr + 1:
58EC3E091000158A1148F7166F334F24

gamma [2]:
C1E2FF52D37E2816D7F7D465162FDD0C

CIPHERTEXT [2]:
3D
ctr + 2:
C1E2FF52D37E2816D7F7D465162FDD3D

gamma [3]:
CDF601E6C4F6B8A9B98F477DD9CF24AF

CIPHERTEXT [3]:

```

9D
ctr + 3:
CDF601E6C4F6B8A9B98F477DD9CF249D

gamma [4]:
DC3499D3AFC718027230995862B81533

CIPHERTEXT [4]:
00
ctr + 4:
DC3499D3AFC718027230995862B81500

gamma [5]:
055D77C627CBDD1EBBFEA437FE486F97

CIPHERTEXT [5]:
A3
ctr + 5:
055D77C627CBDD1EBBFEA437FE486FA3

gamma [6]:
0D38C8E88D7C3CDE3485D2E706E7150E

CIPHERTEXT [6]:
3B
ctr + 6:
0D38C8E88D7C3CDE3485D2E706E7153B

gamma [7]:
7876EB5A68A00E9C31C0F833250D5516

CIPHERTEXT [7]:
20
ctr + 7:
7876EB5A68A00E9C31C0F833250D5520

gamma [8]:
288105EB601546035C6EA45EA0233573

CIPHERTEXT [8]:
44
ctr + 8:
288105EB601546035C6EA45EA0233544

gamma [9]:
0448F352D1BF1ED91DF10E8F0383E16D

CIPHERTEXT [9]:
55
ctr + 9:
0448F352D1BF1ED91DF10E8F0383E155

gamma [10]:
29AE426DD01AF6771E50950CFA12828A

CIPHERTEXT [10]:
B3
ctr + 10:
29AE426DD01AF6771E50950CFA1282B3

gamma [11]:
1B3EE1FE1B64B6F4F6EB85040FEBBC691

CIPHERTEXT [11]:
B0

CIPHERTEXT:
243D9D00A33B204455B3B0

В.4.4 Розшифрування з використанням 128-бітного блоку і 256-бітового ключа базового перетворення, $q = 64$ (Калина-128/256-CFB-64)

$q = 64$
KEY:
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:
2F2E2D2C2B2A29282726252423222120

CIPHERTEXT (N = 328):
5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140
3F3E3D3C3B3A393837

gamma [1]:
453892E3B75A9F8D796FC76AD6DF871B

PLAINTEXT [1]:
26319A368D85DE43
ctr + 1:
453892E3B75A9F8D5F5E5D5C5B5A5958

gamma [2]:
9806980BFBC1B8A78A098EC6DEC3F511

PLAINTEXT [2]:
DD5FDB928D91A441
ctr + 2:
9806980BFBC1B8A75756555453525150

gamma [3]:
2FE7FD2940D018150673C1AC302E3034

PLAINTEXT [3]:
493D8CE07B64797C
ctr + 3:
2FE7FD2940D018154F4E4D4C4B4A4948

gamma [4]:
9D7D5DC9813A6222C8D03381D15E90AA

PLAINTEXT [4]:
8F9676C5921CD1EA
ctr + 4:
9D7D5DC9813A62224746454443424140

gamma [5]:
F1E6711892A1BB824B01631B4CF91E94

PLAINTEXT [5]:
743F5E2777C327AC
ctr + 5:
F1E6711892A1BB823F3E3D3C3B3A3938

gamma [6]:
8EDE57E8E52E163DCA874FD22929DD6F

PLAINTEXT [6]:
58
PLAINTEXT:

26319A368D85DE43DD5FDB928D91A441
493D8CE07B64797C8F9676C5921CD1EA
743F5E2777C327AC58

В.4.5 Зашифрування з використанням 256-бітного блоку і 256-бітового ключа базового перетворення, $q = 128$ (Калина-256/256-CFB-128)

$q = 128$

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 648):

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
90

gamma [1]:

F66E3D570EC92135AEDAE323DCBD2A8C
A03963EC206A0D5A88385C24617FD92C

CIPHERTEXT [1]:

E07821AF642F4B1DC071166F2D329763

ctr + 1:

F66E3D570EC92135AEDAE323DCBD2A8C
E07821AF642F4B1DC071166F2D329763

gamma [2]:

C4B7C95E72472807FC401E39DD2D76EB
929E69CD6D985D05E58A60569BEBE8E4

CIPHERTEXT [2]:

C2CF3B9E39CD0B52BDD33A0DC7B6B6BB

ctr + 2:

C4B7C95E72472807FC401E39DD2D76EB
C2CF3B9E39CD0B52BDD33A0DC7B6B6BB

gamma [3]:

CDCA2A7F68903E5AE027DF92D2960514
407D287FB490BAD1FBC284CA4CB7A455

CIPHERTEXT [3]:

201C4A1CD0F5DCB693ABEEA120DACA3A

ctr + 3:

CDCA2A7F68903E5AE027DF92D2960514
201C4A1CD0F5DCB693ABEEA120DACA3A

gamma [4]:

F6D2EBEB6A5E85F86DDCE1B2DB37A3AB
59B64F6E1AF28B02CFA7E44098AF2806

CIPHERTEXT [4]:

29C73D1D6E87FD75B7DE9E3BE4D25679

ctr + 4:

F6D2EBEB6A5E85F86DDCE1B2DB37A3AB
29C73D1D6E87FD75B7DE9E3BE4D25679

gamma [5]:

756C7F19A6784C7EA2493FD26CFEC022
9CAFC6DBB96D66E66CD1BE29CEEF3364

CIPHERTEXT [5]:

1C2E44583DE8E061E45834A24262BDEB

ctr + 5:

756C7F19A6784C7EA2493FD26CFEC022
1C2E44583DE8E061E45834A24262BDEB

gamma [6]:

32BCEAC69FA7AA0182499C3AA983D069
3492FF4D09193597944B5609CE2A3B2E

CIPHERTEXT [6]:

BE

CIPHERTEXT:

E07821AF642F4B1DC071166F2D329763
C2CF3B9E39CD0B52BDD33A0DC7B6B6BB
201C4A1CD0F5DCB693ABEEA120DACA3A
29C73D1D6E87FD75B7DE9E3BE4D25679
1C2E44583DE8E061E45834A24262BDEB
BE

В.4.6 Розшифрування з використанням 256-бітного блоку і 256-бітового ключа базового перетворення, $q = 256$ (Калина-256/256-CFB-256)

$q = 256$

KEY:

1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:

3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120

CIPHERTEXT (N = 648):

9F9E9D9C9B9A99989796959493929190
8F8E8D8C8B8A89888786858483828180
7F7E7D7C7B7A79787776757473727170
6F6E6D6C6B6A69686766656463626160
5F5E5D5C5B5A59585756555453525150
4F

gamma [1]:

E8C634A546F149943807C671364737F1
A69ED12D61DE20F4817CCFC41588870F

PLAINTEXT [1]:

7758A939DD6BD00CAF9153E5A5D5A661
29105CA1EA54A97C06FA4A40960A068F

ctr + 1:

9F9E9D9C9B9A99989796959493929190
8F8E8D8C8B8A89888786858483828180

gamma [2]:

1EBD9958A5EF7829DB30F2E9F7D1CDB2
21A696056BE7C669099FE64B9E5FD2FD

PLAINTEXT [2]:

61C3E424DE950151AC46879D84A3BCC2
4EC8FB69008DAF016EF9832FFD3DB39D

ctr + 2:

7F7E7D7C7B7A79787776757473727170
6F6E6D6C6B6A69686766656463626160

gamma [3]:

DFA97B79861220F3AF644E5CCFC3B15D
46028723779BD6FB71E6052AAEF5560F

PLAINTEXT [3]:

02185FDB782DC28EAC27B35179FCA406
40

PLAINTEXT:

7758A939DD6BD00CAF9153E5A5D5A661
29105CA1EA54A97C06FA4A40960A068F
61C3E424DE950151AC46879D84A3BCC2
4EC8FB69008DAF016EF9832FFD3DB39D
02185FDB782DC28EAC27B35179FCA406
40

В.4.7 Зашифрування з використанням 256-бітного блоку і 512-бітового ключа базового перетворення, $q = 256$ (Калина-256/512-CFB-256)

$q = 256$

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

PLAINTEXT (N = 648):

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0

gamma [1]:

606990E9E6B7B67A4BD6D893D72268B7
8E02C83C3CD7E102FD2E74A8FDFE5DD9

CIPHERTEXT [1]:

0008F28A82D2D01D23BFB2F8BB4F06D8
FE73BA4F48A2977585570ED3818323A6

ctr + 1:

0008F28A82D2D01D23BFB2F8BB4F06D8
FE73BA4F48A2977585570ED3818323A6

gamma [2]:

5B2CBF1E51055F5F7F0E44DE763489BA
66234486B9C356501F7F6E2D3E68C940

CIPHERTEXT [2]:

DBAD3D9DD580D9D8F787CE55FAB90735
F6B2D6152D56C0C787E6F4B6A2F557DF

ctr + 2:

DBAD3D9DD580D9D8F787CE55FAB90735
F6B2D6152D56C0C787E6F4B6A2F557DF

gamma [3]:

38A2B66381721C5698CCCD74CD535ED0
DBC5BEA20B773175D4D4888C754AF3FC

CIPHERTEXT [3]:

707A671D06AED196DD7D7E2320D8E45C
4C

CIPHERTEXT:

0008F28A82D2D01D23BFB2F8BB4F06D8
FE73BA4F48A2977585570ED3818323A6
DBAD3D9DD580D9D8F787CE55FAB90735
F6B2D6152D56C0C787E6F4B6A2F557DF
707A671D06AED196DD7D7E2320D8E45C
4C

В.4.8 Розшифрування з використанням 256-бітного блоку і 512-бітового ключа базового перетворення, $q = 256$ (Калина-256/512-CFB-256)

$q = 256$

KEY:

3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:

5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140

CIPHERTEXT (N = 648):

BFBEBCBDBB9B8B7B6B5B4B3B2B1B0
AFAEADACABAAA9A8A7A6A5A4A3A2A1A0
9F9E9D9C9B9A99989796959493929190
8F8E8D8C8B8A89888786858483828180
7F7E7D7C7B7A79787776757473727170
6F

gamma [1]:

275F9FCC346002A3ADE1D077256EC867
F89C8C40E3C0740376D1AEB0D9CF71AB

PLAINTEXT [1]:

98E122708FDABB1B1A5765C396DC79D7
573221EC486ADDABD1770B147A6DD00B

ctr + 1:

BFBEBCBDBB9B8B7B6B5B4B3B2B1B0
AFAEADACABAAA9A8A7A6A5A4A3A2A1A0

gamma [2]:

42C0D2880D4E4CEB05A90D9D7D7C65FB
89B2E92963FF6EF6E26AEDB66F6143CA

PLAINTEXT [2]:

DD5E4F1496D4D573923F9809EEEF46B
063C64A5E875E77E65EC6832ECE3C24A

ctr + 2:

9F9E9D9C9B9A99989796959493929190
8F8E8D8C8B8A89888786858483828180

gamma [3]:

5AC2C4162FC700CA11DC8952F0569534
F1A9777F72F5C695BB9990AF4EB42755

PLAINTEXT [3]:

4B8FD40B04088CBEE2CDECE4DC3CC557
3A

PLAINTEXT:

98E122708FDABB1B1A5765C396DC79D7
573221EC486ADDABD1770B147A6DD00B
DD5E4F1496D4D573923F9809EEEEF46B
063C64A5E875E77E65EC6832ECE3C24A
4B8FD40B04088CBEE2CDECE4DC3CC557
3A

В.4.9 Зашифрування з використанням 512-бітного блоку і 512-бітового ключа базового перетворення, $q = 512$ (Калина-512/512-CFB-512)

$q = 512$

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

PLAINTEXT (N = 776):

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0

gamma [1]:

4A26E31B811C356AA61DD6CA0596231A
67BA8354AA47F3A13E1DEEC320EB56B8
95D0F417175BAB662FD6F134BB15C86C
CB906A26856EFEB7C5BC6472940DD9D9

CIPHERTEXT [1]:

CAA761980599B3ED2E945C41891BAD95
F72B11C73ED26536A6847458BC76C827
357156B4B3FE0DC1877F5B9F17B866C3
7B21D89531DB48007D05DEC928B06766

ctr + 1:

CAA761980599B3ED2E945C41891BAD95
F72B11C73ED26536A6847458BC76C827
357156B4B3FE0DC1877F5B9F17B866C3
7B21D89531DB48007D05DEC928B06766

gamma [2]:

F45B94A54B775CD1D77A65223222DC7F
EC2F8C14D235FC77753C34846F673906
BCADFC88EE441060FF301AAC5D92D3A5
A7F6EBA309EC0992798D4DB2DDFD2F89

CIPHERTEXT [2]:

C67D6F3F4C2B82D7A836FAD160905C1C

7576243877DC3ADE4AA057966E0023F0
69

CIPHERTEXT:

CAA761980599B3ED2E945C41891BAD95
F72B11C73ED26536A6847458BC76C827
357156B4B3FE0DC1877F5B9F17B866C3
7B21D89531DB48007D05DEC928B06766
C67D6F3F4C2B82D7A836FAD160905C1C
7576243877DC3ADE4AA057966E0023F0
69

В.4.10 Розшифрування з використанням 512-бітного блоку і 512-бітового ключа базового перетворення, $q = 512$ (Калина-512/512-CFB-512)

$q = 512$

KEY:

3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:

7F7E7D7C7B7A79787776757473727170
6F6E6D6C6B6A69686766656463626160
5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140

CIPHERTEXT (N = 776):

EFEEEEDECEBEAE9E8E7E6E5E4E3E2E1E0
DFDEDDDCDBDAD9D8D7D6D5D4D3D2D1D0
CFCECDCCBCAC9C8C7C6C5C4C3C2C1C0
BFBEBDBCBBBAB9B8B7B6B5B4B3B2B1B0
AFAEADACABAAA9A8A7A6A5A4A3A2A1A0
9F9E9D9C9B9A99989796959493929190
8F

gamma [1]:

E92E8C484D8715E1F7E5AED8183EA3E6
074E5F9D1EB12DC496D51A020CE0F3C0
77B19A262233644999A6AFB9DD4CAA17
74A00201070A3C7A67DD4678A6347A9E

PLAINTEXT [1]:

06C061A4A66DFC0910034B3CFBDC4206
D8908241C56BF41C4103CFD6DF322210
B87F57EAE9F9AD815E606A7D1E8E6BD7
CB1EBFBDBC085C2D06BF3CC1586CB2E

ctr + 1:

EFEEEEDECEBEAE9E8E7E6E5E4E3E2E1E0
DFDEDDDCDBDAD9D8D7D6D5D4D3D2D1D0
CFCECDCCBCAC9C8C7C6C5C4C3C2C1C0
BFBEBDBCBBBAB9B8B7B6B5B4B3B2B1B0

gamma [2]:

E070DFDD5A3D2CFD54C2D0AF9D89071C
A2430412540737049119EB365D897D27
67B8F23E1E2E852112382456D6FAC0C1
31D5163EBA3E8F3EB9D8FC101CD3591A

PLAINTEXT [2]:

88C9155E95B4872D86B49D80F5745B60
5EAF488AA520A717A92F4D68838E42C9
95

PLAINTEXT:

06C061A4A66DFC0910034B3CFBDC4206
D8908241C56BF41C4103CFD6DF322210
B87F57EAE9F9AD815E606A7D1E8E6BD7
CB1EBFBDBC085C2D06BF3CC1586CB2E
88C9155E95B4872D86B49D80F5745B60
5EAF488AA520A717A92F4D68838E42C9
95

В.5 Вироблення імітовставки

В.5.1 Вироблення імітовставки з використанням 128-бітного блоку і 128-бітового ключа базового перетворення, $q = 128$ (Калина-128/128-СМАС-128), без доповнення

KEY:

000102030405060708090A0B0C0D0E0F

AUTHTEXT (N = 384):

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F

padded:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F

KD:

EA4597A6DE4C4012F150277CA1A6CF3A

CIPHERTEXT [0]:

7FB209ECDB6909FEF24DF84E78A5B873

CIPHERTEXT [1]:

80F7C9867E5E2802A4DE7AF3B7780F95

CIPHERTEXT [2]:

123B4EAB8E63ECF3E645A99C1115E241

h:

123B4EAB8E63ECF3E645A99C1115E241

В.5.2 Вироблення імітовставки з використанням 128-бітного блоку і 256-бітового ключа базового перетворення, $q = 128$ (Калина-128/256-СМАС-128), із застосуванням доповнення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

AUTHTEXT (N = 752):

303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D

padded:

303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8000

KD:
EB8F5DFF4C2D2BBF7F5841DEE2577C7D

CIPHERTEXT [0]:
5564CBDDCD0CBF0FE6419BD727E65DB0

CIPHERTEXT [1]:
A7FF71CCC29CDCDCF3084206A01A49F

CIPHERTEXT [2]:
E60DD90AD10BE8C12103F47D2D357AFA

CIPHERTEXT [3]:
695F549C6D1C4156580BE13DCE35A4F3

CIPHERTEXT [4]:
941BD41BA0299B7CB5159385FA6F9FFA

CIPHERTEXT [5]:
4CF52D7D5B0C47F05F6F5F5E73C3B508

h:
4CF52D7D5B0C47F05F6F5F5E73C3B508

В.5.3 Вироблення імітовставки з використанням 256-бітного блоку і 256-бітового ключа базового перетворення, $q = 128$ (Калина-256/256-СМАС-128), із застосуванням доповнення

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

AUTHTEXT (N = 570):
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465664

padded:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
60616263646566600000000000000000
000000000000000000000000000000

KD:
ECE5516BDFD28E91907D5C390D513F9D
A5BEB8CB6E89DFCBD479A3CBDA8CDED

CIPHERTEXT [0]:
F66E3D570EC92135AEDAE323DCBD2A8C
A03963EC206A0D5A88385C24617FD92C

CIPHERTEXT [1]:
88408EFA416618D8DAA4525A0A11C0C9
FC6401B6807234523A71051E3419DEF5

CIPHERTEXT [2]:
CA99CB52DDF2AA392A97159456485AA7
886475E9C0F8C3B102E4E9C2ADB66698

h:

CA99CB52DDF2AA392A97159456485AA7

В.5.4 Вироблення імітовставки з використанням 256-бітного блоку і 512-бітового ключа базового перетворення, $q = 128$ (Калина-256/512-СМАС-128), із застосуванням доповнення

KEY:
 000102030405060708090A0B0C0D0E0F
 101112131415161718191A1B1C1D1E1F
 202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F

AUTHTEXT (N = 265):
 303132333435363738393A3B3C3D3E3F
 404142434445464748494A4B4C4D4E4F
 508

padded:
 303132333435363738393A3B3C3D3E3F
 404142434445464748494A4B4C4D4E4F
 50C00000000000000000000000000000
 00000000000000000000000000000000

KD:
 B1801C0939CBC4AD6F29C35EC01B649F
 44AB51A4FB86E58FD41E5D23E5A4C92E

CIPHERTEXT [0]:
 41CA4044E240DBA1B2E311C49EE16C97
 5BE0098DDAD2D1FCA8504C8655729BEC

CIPHERTEXT [1]:
 B49BC6CAAE6F177F04BAFBEF4666CD1E
 DA89BFB7B6B212BF168C9337423EDC31

h:
 B49BC6CAAE6F177F04BAFBEF4666CD1E

В.5.5 Вироблення імітовставки з використанням 512-бітного блоку і 512-бітового ключа базового перетворення, $q = 128$ (Калина-512/512-СМАС-128), без доповнення

KEY:
 000102030405060708090A0B0C0D0E0F
 101112131415161718191A1B1C1D1E1F
 202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F

AUTHTEXT (N = 1024):
 404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F
 808182838485868788898A8B8C8D8E8F
 909192939495969798999A9B9C9D9E9F
 A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
 B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

padded:
 404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F
 808182838485868788898A8B8C8D8E8F
 909192939495969798999A9B9C9D9E9F
 A0A1A2A3A4A5A6A7A8A9AAABACADAFAF

B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

KD:

F48190172CE2353FF6C36DA511D0647C
7275BEF716DC369849144D6794C8A53B
6F200E010F87D1C10D94065C7BDE30B5
B6846A621E7B0E2347BE891C54FAF0D3

CIPHERTEXT [0]:

4A26E31B811C356AA61DD6CA0596231A
67BA8354AA47F3A13E1DEEC320EB56B8
95D0F417175BAB662FD6F134BB15C86C
CB906A26856EFEB7C5BC6472940DD9D9

CIPHERTEXT [1]:

7279FA6BC8EF7525B2B35260D00A1743
AE7A228DEF1BD7AA0C87FD116D70F875
6B7E6D18E8C5874934A524DB75DE28A7
8737557140079D0A7DE3945AD1E354F2

h:

7279FA6BC8EF7525B2B35260D00A1743

В.6 Зчеплення шифрблоків

В.6.1 Зашифрування з використанням 128-бітного блоку і 128-бітового ключа базового перетворення (Калина-128/128-СВС), без доповнення

KEY:

000102030405060708090A0B0C0D0E0F

IV:

101112131415161718191A1B1C1D1E1F

PLAINTEXT (N = 384):

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F

CIPHERTEXT [0]:

A73625D7BE994E85469A9FAABCEDAAB6

CIPHERTEXT [1]:

DBC5F65DD77BB35E06BD7D1D8EAF862

CIPHERTEXT [2]:

4D6CB31CE189C82B8979F2936DE9BF14

CIPHERTEXT:

A73625D7BE994E85469A9FAABCEDAAB6
DBC5F65DD77BB35E06BD7D1D8EAF862
4D6CB31CE189C82B8979F2936DE9BF14

В.6.2 Розшифрування з використанням 128-бітного блоку і 128-бітового ключа базового перетворення (Калина-128/128-СВС), без доповнення

KEY:

0F0E0D0C0B0A09080706050403020100

IV:

1F1E1D1C1B1A19181716151413121110

CIPHERTEXT (N = 384):

4F4E4D4C4B4A49484746454443424140
3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120

PLAINTEXT [0]:
88F2F048BA696170E3818915E0DBC0AF

PLAINTEXT [1]:
A6F141FEB2C2F817138DA4AAB2DBF9CE4

PLAINTEXT [2]:
90A488C9C82AC83FB0A6C0EEB64CFD22

PLAINTEXT:
88F2F048BA696170E3818915E0DBC0AF
A6F141FEB2C2F817138DA4AAB2DBF9CE4
90A488C9C82AC83FB0A6C0EEB64CFD22

В.6.3 Зашифрування з використанням 128-бітного блоку і 256-бітового ключа базового перетворення (Калина-128/256-CBC), із застосуванням доповнення

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F

PLAINTEXT (N = 368):
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D
padded:
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D8000

CIPHERTEXT [0]:
13EA15843AD14C50BC03ECEF1F43E398

CIPHERTEXT [1]:
E4217752D3EB046AC393DACC5CA1D6FA

CIPHERTEXT [2]:
0EB9FCEB229362B4F1565527EE3D8433

CIPHERTEXT:
13EA15843AD14C50BC03ECEF1F43E398
E4217752D3EB046AC393DACC5CA1D6FA
0EB9FCEB229362B4F1565527EE3D8433

В.6.4 Розшифрування з використанням 128-бітного блоку і 256-бітового ключа базового перетворення (Калина-128/256-CBC), без доповнення

KEY:
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:
2F2E2D2C2B2A29282726252423222120

CIPHERTEXT (N = 384):
5F5E5D5C5B5A59585756555453525150

4F4E4D4C4B4A49484746454443424140
3F3E3D3C3B3A39383736353433323130

PLAINTEXT [0]:
BC8F026FC603ECE05C24FDE875427309

PLAINTEXT [1]:
99B381870882AC0535D4368C4BABD81B

PLAINTEXT [2]:
884E96E853EE7E055262D9D204FBE212

PLAINTEXT:
BC8F026FC603ECE05C24FDE875427309
99B381870882AC0535D4368C4BABD81B
884E96E853EE7E055262D9D204FBE212

В.6.5 Зашифрування з використанням 256-бітного блоку і 256-бітового ключа базового перетворення (Калина-256/256-СВС), без доповнення

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 768):
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

CIPHERTEXT [0]:
9CDFDAA75929E7C2A5CFC1BF16B42C5A
E3886D0258E8C577DC01DAF62D185FB9

CIPHERTEXT [1]:
99B9867736B87110F5F1BC7481912C59
3F48FF79E2AFDFAB9F704A277EC3E557

CIPHERTEXT [2]:
B1B0A9F223DAE6ED5AF591C4F2D6FB22
E48334F5E9B96B1A2EA5200F30A406CE

CIPHERTEXT:
9CDFDAA75929E7C2A5CFC1BF16B42C5A
E3886D0258E8C577DC01DAF62D185FB9
99B9867736B87110F5F1BC7481912C59
3F48FF79E2AFDFAB9F704A277EC3E557
B1B0A9F223DAE6ED5AF591C4F2D6FB22
E48334F5E9B96B1A2EA5200F30A406CE

В.6.6 Розшифрування з використанням 256-бітного блоку і 256-бітового ключа базового перетворення (Калина-256/256-СВС), без доповнення

KEY:
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:

3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120

CIPHERTEXT (N = 768):

9F9E9D9C9B9A99989796959493929190
8F8E8D8C8B8A89888786858483828180
7F7E7D7C7B7A79787776757473727170
6F6E6D6C6B6A69686766656463626160
5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140

PLAINTEXT [0]:

AD1C64FFA7EC7C733B1857C08BC76E3F
CFA60629913AFDDC6DF5F06498D0664E

PLAINTEXT [1]:

68B0C2DAD5986FDBF0C8204BD7FECC39
3AE5FE473ED5EA4D8D08FC414634A2B6

PLAINTEXT [2]:

88954443C979ABF9224D09DD2F6CD436
CBB2857DF85A12AD8DCA0AEEE997C18B

PLAINTEXT:

AD1C64FFA7EC7C733B1857C08BC76E3F
CFA60629913AFDDC6DF5F06498D0664E
68B0C2DAD5986FDBF0C8204BD7FECC39
3AE5FE473ED5EA4D8D08FC414634A2B6
88954443C979ABF9224D09DD2F6CD436
CBB2857DF85A12AD8DCA0AEEE997C18B

В.6.7 Зашифрування з використанням 256-бітного блоку і 512-бітового ключа базового перетворення (Калина-256/512-CBC), без доповнення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

PLAINTEXT (N = 768):

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBCBDBEBF

CIPHERTEXT [0]:

B8A2474578C2FEBF3F94703587BD5FDC
3F4A4D2F43575B6144A1E1031FB3D145

CIPHERTEXT [1]:

2B7FD52F5E3411461DAC506869FF8D2F
AEF4FEE60379AE00B33AA3EAF911645A

CIPHERTEXT [2]:

F8091CD8A45D141D1FB150E5A01C1F26
FF3DBD26AC4225EC7577B2CE57A5B0FF

CIPHERTEXT:

B8A2474578C2FEBF3F94703587BD5FDC
 3F4A4D2F43575B6144A1E1031FB3D145
 2B7FD52F5E3411461DAC506869FF8D2F
 AEF4FEE60379AE00B33AA3EAF911645A
 F8091CD8A45D141D1FB150E5A01C1F26
 FF3DBD26AC4225EC7577B2CE57A5B0FF

В.6.8 Розшифрування з використанням 256-бітного блоку і 512-бітового ключа базового перетворення (Калина-256/512-СВС), без доповнення

KEY:

3F3E3D3C3B3A39383736353433323130
 2F2E2D2C2B2A29282726252423222120
 1F1E1D1C1B1A19181716151413121110
 0F0E0D0C0B0A09080706050403020100

IV:

5F5E5D5C5B5A59585756555453525150
 4F4E4D4C4B4A49484746454443424140

CIPHERTEXT (N = 768):

BFBEBDBCBBAB9B8B7B6B5B4B3B2B1B0
 AFAEADACABAAA9A8A7A6A5A4A3A2A1A0
 9F9E9D9C9B9A99989796959493929190
 8F8E8D8C8B8A89888786858483828180
 7F7E7D7C7B7A79787776757473727170
 6F6E6D6C6B6A69686766656463626160

PLAINTEXT [0]:

C69A59E10D00F087319B62288A57417C
 074EAD07C732A87055F0A5AD2BB28810

PLAINTEXT [1]:

5705C45E091A9A6726E9672DC7D8C76F
 C45C782BCFEF7C39D94DEB84B17035BC

PLAINTEXT [2]:

8651255A0D34373451B6E1A2C827DB97
 566C9FF5506C5579F982A0EFC5BA7C28

PLAINTEXT:

C69A59E10D00F087319B62288A57417C
 074EAD07C732A87055F0A5AD2BB28810
 5705C45E091A9A6726E9672DC7D8C76F
 C45C782BCFEF7C39D94DEB84B17035BC
 8651255A0D34373451B6E1A2C827DB97
 566C9FF5506C5579F982A0EFC5BA7C28

В.6.9 Зашифрування з використанням 512-бітного блоку і 512-бітового ключа базового перетворення (Калина-512/512-СВС), без доповнення

KEY:

000102030405060708090A0B0C0D0E0F
 101112131415161718191A1B1C1D1E1F
 202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F

707172737475767778797A7B7C7D7E7F

PLAINTEXT (N = 1024):

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCDCCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEF
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

CIPHERTEXT [0]:

D4739B829EF901B24C1162AE4FDEF897
EDA41FAC7F5770CDC90E1D1CDF124E8D
7831E06B4498A4B6F6EC815DF2461DC9
9BB0449B0F09FCAA2C84090534BCC932

CIPHERTEXT [1]:

9626FD74EF8F0A0BCB5765184629C3CB
F53B0FB134F6D0421174B1C4E884D1CD
1069A7AD19752DCEBF655842E79B7858
BDE01390A760D85E88925BFE38B0FA57

CIPHERTEXT:

D4739B829EF901B24C1162AE4FDEF897
EDA41FAC7F5770CDC90E1D1CDF124E8D
7831E06B4498A4B6F6EC815DF2461DC9
9BB0449B0F09FCAA2C84090534BCC932
9626FD74EF8F0A0BCB5765184629C3CB
F53B0FB134F6D0421174B1C4E884D1CD
1069A7AD19752DCEBF655842E79B7858
BDE01390A760D85E88925BFE38B0FA57

В.6.10 Розшифрування з використанням 512-бітного блоку і 512-бітового ключа базового перетворення (Калина-512/512-CBC), без доповнення

KEY:

3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:

7F7E7D7C7B7A79787776757473727170
6F6E6D6C6B6A69686766656463626160
5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140

CIPHERTEXT (N = 1024):

FFFEFD FCFBFAF9F8F7F6F5F4F3F2F1F0
EFFFFE DECEBEAE9E8E7E6E5E4E3E2E1E0
DFDEDD DCDBDAD9D8D7D6D5D4D3D2D1D0
CFCECD CCCBCAC9C8C7C6C5C4C3C2C1C0
BFBEBC BCBAB9B8B7B6B5B4B3B2B1B0
AFAEAD ACABAAA9A8A7A6A5A4A3A2A1A0
9F9E9D 9C9B9A99989796959493929190
8F8E8D 8C8B8A89888786858483828180

PLAINTEXT [0]:

5D5B3E3DE5BAA70E0A0684D458856CE7
59C6018D0B3F087FC1DAC101D380236D
D934F2880B02D56A575BCA35A0CE4B0D
9BA1F4A39C16CA7D80D59956630F09E5

PLAINTEXT [1]:

4EC91E32B6830FE08323ED393F8028D1
50BF03CAD0629A5AFEEFF6E442579806
18DB2F32B7B2B65B96E8451F1090829D
2FFFC615CC1581E9221438DCEAD1FD12

PLAINTEXT:

5D5B3E3DE5BAA70E0A0684D458856CE7
59C6018D0B3F087FC1DAC101D380236D
D934F2880B02D56A575BCA35A0CE4B0D
9BA1F4A39C16CA7D80D59956630F09E5
4EC91E32B6830FE08323ED393F8028D1
50BF03CAD0629A5AFEEFF6E442579806
18DB2F32B7B2B65B96E8451F1090829D
2FFFC615CC1581E9221438DCEAD1FD12

В.7 Гамування зі зворотнім зв'язком за шифрною

В.7.1 Зашифрування з використанням 128-бітного блоку і 128-бітового ключа базового перетворення (Калина-128/128-OFB)

KEY:

000102030405060708090A0B0C0D0E0F

IV:

101112131415161718191A1B1C1D1E1F

PLAINTEXT (N = 384):

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F

gamma [0]:

81BF1C7D779BAC20E1C9EA39B4D2AD06

CIPHERTEXT [0]:

A19E3E5E53BE8A07C9E0C01298FF8329

gamma [1]:

63116E552FED6C66CB907B2880456294

CIPHERTEXT [1]:

53205C661BD85A51F3A94113BC785CAB

gamma [2]:

230A74ABDECA9B51E9670E2CB9811469

CIPHERTEXT [2]:

634B36E89A8FDD16A12E4467F5CC5A26

CIPHERTEXT:

A19E3E5E53BE8A07C9E0C01298FF8329
53205C661BD85A51F3A94113BC785CAB
634B36E89A8FDD16A12E4467F5CC5A26

В.7.2 Розшифрування з використанням 128-бітного блоку і 128-бітового ключа базового перетворення (Калина-128/128- OFB)

KEY:

0F0E0D0C0B0A09080706050403020100

IV:

1F1E1D1C1B1A19181716151413121110

CIPHERTEXT (N = 384):

4F4E4D4C4B4A49484746454443424140

3F3E3D3C3B3A39383736353433323130

2F2E2D2C2B2A29282726252423222120

gamma [0]:

2BD453E6AA2AE668B2F5AA6B1B942D51

PLAINTEXT [0]:

649A1EAAE160AF20F5B3EF2F58D66C11

gamma [1]:

4786133CE9550950ABB8F71ABDB4D8FB

PLAINTEXT [1]:

78B82E00D26F30689C8EC22E8E86E9CB

gamma [2]:

9F9362D2C8B498140437024EB34FF716

PLAINTEXT [2]:

B0BD4FFEE39EB13C2311276A906DD636

PLAINTEXT:

649A1EAAE160AF20F5B3EF2F58D66C11

78B82E00D26F30689C8EC22E8E86E9CB

B0BD4FFEE39EB13C2311276A906DD636

В.7.3 Зашифрування з використанням 128-бітного блоку і 256-бітового ключа базового перетворення (Калина-128/256-OFB)

KEY:

000102030405060708090A0B0C0D0E0F

101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F

PLAINTEXT (N = 154):

303132333435363738393A3B3C3D3E3F

404142C

gamma [0]:

58EC3E091000158A1148F7166F334F14

CIPHERTEXT [0]:

68DD0C3A243523BD2971CD2D530E712B

gamma [1]:

6C12FC5B3AF0DE52C6A6C19716FE0AF4

CIPHERTEXT [1]:

2C53BE8

CIPHERTEXT:

68DD0C3A243523BD2971CD2D530E712B

2C53BE8

В.7.4 Розшифрування з використанням 128-бітного блоку і 256-бітового ключа базового перетворення (Калина-128/256-OFB)

KEY:

1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:

2F2E2D2C2B2A29282726252423222120

CIPHERTEXT (N = 328):

5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140
3F3E3D3C3B3A393837

gamma [0]:

453892E3B75A9F8D796FC76AD6DF871B

PLAINTEXT [0]:

1A66CFBFEC00C6D52E39923E858DD64B

gamma [1]:

6E04FACB32C774181EE0F1DCEE24F20E

PLAINTEXT [1]:

214AB787798D3D5059A6B498AD66B34E

gamma [2]:

9376F93B70D634A0F1A337D65DFBD1E9

PLAINTEXT [2]:

AC48C4074BEC0D98C6

PLAINTEXT:

1A66CFBFEC00C6D52E39923E858DD64B
214AB787798D3D5059A6B498AD66B34E
AC48C4074BEC0D98C6

В.7.5 Зашифрування з використанням 256-бітного блоку і 256-бітового ключа базового перетворення (Калина-256/256-OFB)

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 648):

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
90

gamma [0]:

F66E3D570EC92135AEDAE323DCBD2A8C
A03963EC206A0D5A88385C24617FD92C

CIPHERTEXT [0]:

B62F7F144A8C6772E693A96890F064C3
F06831BF743F5B0DD061067F3D228773

gamma [1]:

51CB08FABD5C963C1D39832B47BC0F33
B7C3A6D2139D48B7A0D1EE82500F9F09

CIPHERTEXT [1]:

31AA6A99D939F05B7550E9402BD1615C

C7B2D4A167E83EC0D8A894F92C72E176

gamma [2]:

730989E24794501B69A886D294C30F01
8995EBB6DBC022CA0820436E3902778B

CIPHERTEXT [2]:

F3880B61C311D69CE1210C59184E818E
19

CIPHERTEXT:

B62F7F144A8C6772E693A96890F064C3
F06831BF743F5B0DD061067F3D228773
31AA6A99D939F05B7550E9402BD1615C
C7B2D4A167E83EC0D8A894F92C72E176
F3880B61C311D69CE1210C59184E818E
19

В.7.6 Розшифрування з використанням 256-бітного блоку і 256-бітового ключа базового перетворення (Калина-256/256-OFB)

KEY:

1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100

IV:

3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120

CIPHERTEXT (N = 648):

9F9E9D9C9B9A99989796959493929190
8F8E8D8C8B8A89888786858483828180
7F7E7D7C7B7A79787776757473727170
6F6E6D6C6B6A69686766656463626160
5F5E5D5C5B5A59585756555453525150
4F

gamma [0]:

E8C634A546F149943807C671364737F1
A69ED12D61DE20F4817CCFC41588870F

PLAINTEXT [0]:

7758A939DD6BD00CAF9153E5A5D5A661
29105CA1EA54A97C06FA4A40960A068F

gamma [1]:

2A9D32EF42DB3D4E561F3D8D5CD08A22
E9BDC672EA3E56A866EC692AEF2B5515

PLAINTEXT [1]:

55E34F9339A14436216948F92FA2FB52
86D3AB1E81543FC0018A0C4E8C493475

gamma [2]:

AB8D0093EBFDFC6F28303CEC049F9828
AB4A7BC648E249EA6BBE07E8A52940C0

PLAINTEXT [2]:

F4D35DCFB0A7A5377F6669B857CDC978
E4

PLAINTEXT:

7758A939DD6BD00CAF9153E5A5D5A661
29105CA1EA54A97C06FA4A40960A068F
55E34F9339A14436216948F92FA2FB52
86D3AB1E81543FC0018A0C4E8C493475
F4D35DCFB0A7A5377F6669B857CDC978

E4

В.7.7 Зашифрування з використанням 256-бітного блоку і 512-бітового ключа базового перетворення (Калина-256/512-OFB)

KEY:

```
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
```

IV:

```
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
```

PLAINTEXT (N = 648):

```
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0
```

gamma [0]:

```
606990E9E6B7B67A4BD6D893D72268B7
8E02C83C3CD7E102FD2E74A8FDFE5DD9
```

CIPHERTEXT [0]:

```
0008F28A82D2D01D23BFB2F8BB4F06D8
FE73BA4F48A2977585570ED3818323A6
```

gamma [1]:

```
E809BE1E4B73964BF6B72F4BA97632D3
36C39D1C855FA3592129EAAA7A466421
```

CIPHERTEXT [1]:

```
68883C9DCFF610CC7E3EA5C025FBBC5C
A6520F8F11CA35CEB9B07031E6DBFABE
```

gamma [2]:

```
99A1BC39986504EC14FFF392F586E342
0D42DD8B855F1E984B2643573EF77226
```

CIPHERTEXT [2]:

```
39001E9A3CC0A24BBC565939592B4DED
BD
```

CIPHERTEXT:

```
0008F28A82D2D01D23BFB2F8BB4F06D8
FE73BA4F48A2977585570ED3818323A6
68883C9DCFF610CC7E3EA5C025FBBC5C
A6520F8F11CA35CEB9B07031E6DBFABE
39001E9A3CC0A24BBC565939592B4DED
BD
```

В.7.8 Розшифрування з використанням 256-бітного блоку і 512-бітового ключа базового перетворення (Калина-256/512-OFB)

KEY:

```
3F3E3D3C3B3A39383736353433323130
2F2E2D2C2B2A29282726252423222120
1F1E1D1C1B1A19181716151413121110
0F0E0D0C0B0A09080706050403020100
```

IV:

5F5E5D5C5B5A59585756555453525150
4F4E4D4C4B4A49484746454443424140

CIPHERTEXT (N = 648):

BFBEBCBDBB9B8B7B6B5B4B3B2B1B0
AFAEADACABAAA9A8A7A6A5A4A3A2A1A0
9F9E9D9C9B9A99989796959493929190
8F8E8D8C8B8A89888786858483828180
7F7E7D7C7B7A79787776757473727170
6F

gamma [0]:

275F9FCC346002A3ADE1D077256EC867
F89C8C40E3C0740376D1AEB0D9CF71AB

PLAINTEXT [0]:

98E122708FDABB1B1A5765C396DC79D7
573221EC486ADDABD1770B147A6DD00B

gamma [1]:

C022D2825D16C0EFCCEC3FD9D0565D74
7C18540E54EE5A838469E9BF1AF9216D

PLAINTEXT [1]:

5FBC4F1EC68C59775B7AAA4D43C4CCE4
F396D982DF64D30B03EF6C3B997BA0ED

gamma [2]:

EB75C12570A9741CC2D8550534A561F6
DAF8A1E0B1F1695A9900E884CFA3F8DE

PLAINTEXT [2]:

940BBC590BD30D64B5AE207147D71086
B5

PLAINTEXT:

98E122708FDABB1B1A5765C396DC79D7
573221EC486ADDABD1770B147A6DD00B
5FBC4F1EC68C59775B7AAA4D43C4CCE4
F396D982DF64D30B03EF6C3B997BA0ED
940BBC590BD30D64B5AE207147D71086
B5

В.7.9 Зашифрування з використанням 512-бітного блоку і 512-бітового ключа базового перетворення (Калина-512/512-OFB)

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

PLAINTEXT (N = 776):

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0

gamma [0]:

4A26E31B811C356AA61DD6CA0596231A
 67BA8354AA47F3A13E1DEEC320EB56B8
 95D0F417175BAB662FD6F134BB15C86C
 CB906A26856EFEB7C5BC6472940DD9D9

CIPHERTEXT [0]:

CAA761980599B3ED2E945C41891BAD95
 F72B11C73ED26536A6847458BC76C827
 357156B4B3FE0DC1877F5B9F17B866C3
 7B21D89531DB48007D05DEC928B06766

gamma [1]:

00D5795344FD9818CEBE2E41C6F47B28
 984FFA3BFB2A072F9E4D2BA94A16AEC9
 B6DA0A749C63FAEA8E64A9396442EF65
 2C544C6A883BB7683ED2413BA671D550

CIPHERTEXT [1]:

C014BB9080385EDF0677E48A0A39B5E7
 489E28E82FFFD1F84694F17296CB7016
 56

CIPHERTEXT:

CAA761980599B3ED2E945C41891BAD95
 F72B11C73ED26536A6847458BC76C827
 357156B4B3FE0DC1877F5B9F17B866C3
 7B21D89531DB48007D05DEC928B06766
 C014BB9080385EDF0677E48A0A39B5E7
 489E28E82FFFD1F84694F17296CB7016
 56

В.7.10 Розшифрування з використанням 512-бітного блоку і 512-бітового ключа базового перетворення (Калина-512/512-OFB)

KEY:

3F3E3D3C3B3A39383736353433323130
 2F2E2D2C2B2A29282726252423222120
 1F1E1D1C1B1A19181716151413121110
 0F0E0D0C0B0A09080706050403020100

IV:

7F7E7D7C7B7A79787776757473727170
 6F6E6D6C6B6A69686766656463626160
 5F5E5D5C5B5A59585756555453525150
 4F4E4D4C4B4A49484746454443424140

CIPHERTEXT (N = 776):

EFEEEECEBEAE9E8E7E6E5E4E3E2E1E0
 DFDEDDDCBDAD9D8D7D6D5D4D3D2D1D0
 CFCECDCCBCAC9C8C7C6C5C4C3C2C1C0
 BFBEBDBCBBAB9B8B7B6B5B4B3B2B1B0
 AFAEADACABAAA9A8A7A6A5A4A3A2A1A0
 9F9E9D9C9B9A99989796959493929190
 8F

gamma [0]:

E92E8C484D8715E1F7E5AED8183EA3E6
 074E5F9D1EB12DC496D51A020CE0F3C0
 77B19A262233644999A6AFB9DD4CAA17
 74A00201070A3C7A67DD4678A6347A9E

PLAINTEXT [0]:

06C061A4A66DFC0910034B3CFBDC4206
 D8908241C56BF41C4103CFD6DF322210
 B87F57EAE9F9AD815E606A7D1E8E6BD7

CB1EBFBDBC085C2D06BF3CC1586CB2E

gamma [1]:

4E76B094E8D5EBF99694B3E3478DFC43
964DA2B923077AE9B3FEABDFD710DE55
E25FFE842F0C6E25E7828BFC327610CE
28E69D575C7C562ED6B50DADC0D947DA

PLAINTEXT [1]:

E1D81D38437F425131321647E42F5DE3
09D33F25B89DE37124683E4B44824FC5
6D

PLAINTEXT:

06C061A4A66DFC0910034B3CFBDC4206
D8908241C56BF41C4103CFD6DF322210
B87F57EAE9F9AD815E606A7D1E8E6BD7
CB1EBFBDBC085C2D06BF3CC1586CB2E
E1D81D38437F425131321647E42F5DE3
09D33F25B89DE37124683E4B44824FC5
6D

В.8 Вибіркове гамування із прискореним виробленням імітовставки

В.8.1 Зашифрування та забезпечення цілісності з використанням 128-бітного блоку і 128-бітового ключа базового перетворення, $q = 128$ (Калина-128/128-GCM-128)

В.8.1.1 Вироблення імітовставки для відкритої частини повідомлення та шифртексту

KEY:

000102030405060708090A0B0C0D0E0F

IV:

101112131415161718191A1B1C1D1E1F

AUTHTEXT:

202122232425262728292A2B2C2D2E2F

CIPHERTEXT:

B91A7B8790BBCFCFE65D04E5538E98E2
16AC209DA33122FDA596E8928070BE51

H:

EA4597A6DE4C4012F150277CA1A6CF3A

b [1]:

8AA939CEA57EEA92D2519642F33513C5

bs [0]:

8AA939CEA57EEA92D2519642F33513C5

bs [1]:

1F3D3194D231468B65E5BA5A0108B4CC

bs [2]:

923DFA511FFB25F852B5BF349BA31DD8

B:

923DFA511FFB25F852B5BF349BA31DD8

lambda_o:

8000000000000000

lambda_c:

0001000000000000

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F

AUTHTEXT:
303132333435363738393A3B3C3D3E3F

CIPHERTEXT:
FF83F27C6D4EA26101B1986235831406
A297940D6C0E695596D612623E0E7CDC

H:
C98021FE11626E6924BF8A334C526C05

b [1]:
296D5135414F6526F193D10CACA0EE49

bs [0]:
296D5135414F6526F193D10CACA0EE49

bs [1]:
B046F0A42C9B6FDBA21B51BA5ADF33BC

bs [2]:
2C4B1E257F9AA09F23F4716E02BDC537

B:
2C4B1E257F9AA09F23F4716E02BDC537

lambda_o:
8000000000000000
lambda_c:
0001000000000000
lambda_o_lambda_c:
8000000000000000100000000000

h:
3C474281AFEAE4FD6D61E995258747AB

В.8.2.2 Зашифрування та забезпечення цілісності

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F

PLAINTEXT (N = 256):
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F

CIPHERTEXT:
FF83F27C6D4EA26101B1986235831406
A297940D6C0E695596D612623E0E7CDC

В.8.2.3 Вироблення імітовставки для відкритого повідомлення, $q = 128$ (Калина-128/256-GMAC-128)

KEY:
000102030405060708090A0B0C0D0E0F

101112131415161718191A1B1C1D1E1F

AUTHTEXT:

303132333435363738393A3B3C3D3E3F

H:

C98021FE11626E6924BF8A334C526C05

b [1]:

296D5135414F6526F193D10CACA0EE49

lambda_o:

8000000000000000

lambda_c:

0000000000000000

lambda_o_lambda_c:

80000000000000000000000000000000

h:

5AE309EE80B583C6523397ADCB5704C4

В.8.3 Зашифрування та забезпечення цілісності з використанням 256-бітного блоку і 256-бітового ключа базового перетворення, $q = 128$ (Калина-256/256-GCM-128)

В.8.3.1 Вироблення імітовставки для відкритої частини повідомлення та шифртексту

KEY:

000102030405060708090A0B0C0D0E0F

101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F

303132333435363738393A3B3C3D3E3F

AUTHTEXT:

404142434445464748494A4B4C4D4E4F

505152535455565758595A5B5C5D5E5F

CIPHERTEXT:

7EC15C54BB553CB1437BE0EFDD2E810F

6058497EBCE4408A08A73FADF3F459D5

6B0103702D13AB73ACD2EB33A8B5E9CF

FF5EB21865A6B499C10C810C4BAEBE80

H:

674960E64862084766A9AB4F8A4DD73A

B0F60CA5B3F00344A36B6183B52F1BB2

b [1]:

4A321AAFD7B5EFB65B6C66DD96D852D9

F234ADE9731907F89710C98AE541CBE3

bs [0]:

4A321AAFD7B5EFB65B6C66DD96D852D9

F234ADE9731907F89710C98AE541CBE3

bs [1]:

AB6CC56DB9F2E019A7FB7AF11E6492F4

3B7E7C8249D1C2A927CEEDC88D0323AB

bs [2]:

AEA1D414C4131CF5ED38D15500AC1A8E

A1D02C566E6542EDE4A3C64E41B7288A

B:
AEA1D414C4131CF5ED38D15500AC1A8E
A1D02C566E6542EDE4A3C64E41B7288A

lambda_o:
00010000000000000000000000000000

lambda_c:
00020000000000000000000000000000

lambda_o_lambda_c:
00010000000000000000000000000000
00020000000000000000000000000000

h:
1D61B0A3018F6B849CBA20AF1DDDA245

В.8.3.2 Зашифрування та забезпечення цілісності

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 512):
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

CIPHERTEXT:
7EC15C54BB553CB1437BE0EFDD2E810F
6058497EBCE4408A08A73FADF3F459D5
6B0103702D13AB73ACD2EB33A8B5E9CF
FF5EB21865A6B499C10C810C4BAEBE80

В.8.3.3 Вироблення імітовставки для відкритого повідомлення, $q = 128$ (Калина-256/256-GMAC-128)

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

AUTHTEXT:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

H:
674960E64862084766A9AB4F8A4DD73A
B0F60CA5B3F00344A36B6183B52F1BB2

b [1]:
4A321AAFD7B5EFB65B6C66DD96D852D9
F234ADE9731907F89710C98AE541CBE3

lambda_o:
00010000000000000000000000000000

lambda_c:
00000000000000000000000000000000

```

lampda_o_lambda_c:
00010000000000000000000000000000
00000000000000000000000000000000

```

```

h:
FF48B56F2C26CC484B8F5952D7B3E1FE

```

В.8.4 Зашифрування та забезпечення цілісності з використанням 256-бітного блоку і 256-бітового ключа базового перетворення, $q = 256$ (Калина-256/256-GCM-256)

В.8.4.1 Вироблення імітовставки для відкритої частини повідомлення та шифртексту

```

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

```

```

IV:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

```

```

AUTHTEXT:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

```

```

CIPHERTEXT:
7EC15C54BB553CB1437BE0EFDD2E810F
6058497EBCE4408A08A73FADF3F459D5
6B0103702D13AB73ACD2EB33A8B5E9CF
FF5EB21865A6B499C10C810C4BAEBE80

```

```

H:
674960E64862084766A9AB4F8A4DD73A
B0F60CA5B3F00344A36B6183B52F1BB2

```

```

b [1]:
4A321AAFD7B5EFB65B6C66DD96D852D9
F234ADE9731907F89710C98AE541CBE3

```

```

bs [0]:
4A321AAFD7B5EFB65B6C66DD96D852D9
F234ADE9731907F89710C98AE541CBE3

```

```

bs [1]:
AB6CC56DB9F2E019A7FB7AF11E6492F4
3B7E7C8249D1C2A927CEEDC88D0323AB

```

```

bs [2]:
AEA1D414C4131CF5ED38D15500AC1A8E
A1D02C566E6542EDE4A3C64E41B7288A

```

```

B:
AEA1D414C4131CF5ED38D15500AC1A8E
A1D02C566E6542EDE4A3C64E41B7288A

```

```

lambda_o:
00010000000000000000000000000000

```

```

lambda_c:
00020000000000000000000000000000

```

```

lampda_o_lambda_c:

```

00010000000000000000000000000000
00020000000000000000000000000000

h:

1D61B0A3018F6B849CBA20AF1DDDA245
B1B296258AC0352A52D3F372E72224CE

В.8.4.2 Зашифрування та забезпечення цілісності

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 512):

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

CIPHERTEXT:

7EC15C54BB553CB1437BE0EFDD2E810F
6058497EBCE4408A08A73FADF3F459D5
6B0103702D13AB73ACD2EB33A8B5E9CF
FF5EB21865A6B499C10C810C4BAEBE80

В.8.4.3 Вироблення імітовставки для відкритого повідомлення, $q = 256$ (Калина-256/256-GMAC-256)

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

AUTHTEXT:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

H:

674960E64862084766A9AB4F8A4DD73A
B0F60CA5B3F00344A36B6183B52F1BB2

b [1]:

4A321AAFD7B5EFB65B6C66DD96D852D9
F234ADE9731907F89710C98AE541CBE3

lambda_o:

00010000000000000000000000000000

lambda_c:

00000000000000000000000000000000

lambda_o_lambda_c:

00010000000000000000000000000000
00000000000000000000000000000000

h:

FF48B56F2C26CC484B8F5952D7B3E1FE
69577701C50BE96517B33921E44634CD

В.8.5 Зашифрування та забезпечення цілісності з використанням 256-бітного блоку і 512-бітового ключа базового перетворення, $q = 256$ (Калина-256/512-GCM-256)

В.8.5.1 Вироблення імітовставки для відкритої частини повідомлення та шифртексту

KEY:

```
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
```

IV:

```
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
```

AUTHTEXT:

```
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
```

CIPHERTEXT:

```
3EBDB4584B5169A26FBEBAA0295B4223F
58D5D8A031F2950A1D7764FAB97BA058
E9E2DAB90FF0C519AA88435155A71B7B
53BB100F5D20AFFAC0552F5F2813DEE8
```

H:

```
2F90AF04B8E6F3C320D70B2247129AA4
244A048B1518CB1F616128308EF62C2D
```

b [1]:

```
F47268FA9A0944C370B8C360D4068706
ADF440D476620023F0FFEC78D642D72D
```

bs [0]:

```
F47268FA9A0944C370B8C360D4068706
ADF440D476620023F0FFEC78D642D72D
```

bs [1]:

```
D3517E699429BA5BAA3DDC86D375053F
3CA49B5E5454448B602D86480C7898C8
```

bs [2]:

```
B35D78B571942D2CB91B654A40616CC0
59464BEDFC410058757B1A8E7CA1AF5D
```

B:

```
B35D78B571942D2CB91B654A40616CC0
59464BEDFC410058757B1A8E7CA1AF5D
```

lambda_o:

```
00010000000000000000000000000000
```

lambda_c:

```
00020000000000000000000000000000
```

lampda_o_lambda_c:

```
00010000000000000000000000000000
00020000000000000000000000000000
```

h:

```
8555FD3D9B02C2325ACA3CC9309D6B4B
9AFC697D13BBBFF067198D5D86CB9820
```

В.8.5.2 Зашифрування та забезпечення цілісності

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

PLAINTEXT (N = 512):
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

CIPHERTEXT:
3EBDB4584B5169A26FBEBAA0295B4223F
58D5D8A031F2950A1D7764FAB97BA058
E9E2DAB90FF0C519AA88435155A71B7B
53BB100F5D20AFFAC0552F5F2813DEE8

В.8.5.3 Вироблення імітовставки для відкритого повідомлення, $q = 256$ (Калина-256/512-GMAC-256)

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

AUTHTEXT:
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

H:
2F90AF04B8E6F3C320D70B2247129AA4
244A048B1518CB1F616128308EF62C2D

b [1]:
F47268FA9A0944C370B8C360D4068706
ADF440D476620023F0FFEC78D642D72D

lambda_o:
00010000000000000000000000000000

lambda_c:
00000000000000000000000000000000

lambda_o_lambda_c:
00010000000000000000000000000000
00000000000000000000000000000000

h:
96F61FA0FDE92883C5041D748F9AE91F
3A0A50415BFA1466855340A5714DC01F

В.8.6 Зашифрування та забезпечення цілісності з використанням 512-бітного блоку і 512-бітового ключа базового перетворення, $q = 512$ (Калина-512/512-GCM-512)

В.8.6.1 Вироблення імітовставки для відкритої частини повідомлення та шифртексту

KEY:

```
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
```

IV:

```
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
```

AUTHTEXT:

```
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF
```

CIPHERTEXT:

```
220642D7277D104788CF97B10210984F
506435512F7BF153C5CDABFECC10AFB4
A2E2FC51F616AF80FFDD0607FAD4F542
B8EF0667717CE3EAAA8FBC303CE76C99
```

H:

```
F48190172CE2353FF6C36DA511D0647C
7275BEF716DC369849144D6794C8A53B
6F200E010F87D1C10D94065C7BDE30B5
B6846A621E7B0E2347BE891C54FAF0D3
```

b [1]:

```
DF99EBBC2802E7596ECCE2D5528B5CB2
137283183FBD22B31EBC0FC05E16F8C4
9464EC5DA0691272953822D035C6A9CC
F119D132C975EF99F69E0C19885D76B7
```

bs [0]:

```
DF99EBBC2802E7596ECCE2D5528B5CB2
137283183FBD22B31EBC0FC05E16F8C4
9464EC5DA0691272953822D035C6A9CC
F119D132C975EF99F69E0C19885D76B7
```

bs [1]:

```
B6C6604069C19744FAA89A0CFD299D26
CE34B2BD0C10388CCDB1671E6D711972
52511B0CC8F076EBAABF947E50334B67
41051C91BF769246EB9479DB2DC977F5
```

B:

```
B6C6604069C19744FAA89A0CFD299D26
CE34B2BD0C10388CCDB1671E6D711972
52511B0CC8F076EBAABF947E50334B67
41051C91BF769246EB9479DB2DC977F5
```

lambda_o:

```
00020000000000000000000000000000
00000000000000000000000000000000
```

lambda_c:

```
00020000000000000000000000000000
00000000000000000000000000000000
```


lambda_o_lambda_c:
 00020000000000000000000000000000
 00000000000000000000000000000000
 00020000000000000000000000000000
 00000000000000000000000000000000

h:
 78A77E5948F5DC05F551486FDBB44898
 C9AB1BD439D7519841AE31007C09E1B3
 12E5EA5929F952F6A3EEF5CBEAEF262B
 8EC1884DFCF4BAAF7B5C9291A22489E1

В.8.6.2 Зашифрування та забезпечення цілісності

KEY:
 000102030405060708090A0B0C0D0E0F
 101112131415161718191A1B1C1D1E1F
 202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F

IV:
 404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F

PLAINTEXT (N = 512):
 C0C1C2C3C4C5C6C7C8C9CACBCCDCCECF
 D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
 E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEF
 F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

CIPHERTEXT:
 220642D7277D104788CF97B10210984F
 506435512F7BF153C5CDABFECC10AFB4
 A2E2FC51F616AF80FFDD0607FAD4F542
 B8EF0667717CE3EAAA8FBC303CE76C99

В.8.6.3 Вироблення імітовставки для відкритого повідомлення, $q = 512$ (Калина-512/512-GMAC-512)

KEY:
 000102030405060708090A0B0C0D0E0F
 101112131415161718191A1B1C1D1E1F
 202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F

AUTHTEXT:
 808182838485868788898A8B8C8D8E8F
 909192939495969798999A9B9C9D9E9F
 A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
 B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF

H:
 F48190172CE2353FF6C36DA511D0647C
 7275BEF716DC369849144D6794C8A53B
 6F200E010F87D1C10D94065C7BDE30B5
 B6846A621E7B0E2347BE891C54FAF0D3

b [1]:
 DF99EBBC2802E7596ECCE2D5528B5CB2
 137283183FBD22B31EBC0FC05E16F8C4
 9464EC5DA0691272953822D035C6A9CC
 F119D132C975EF99F69E0C19885D76B7

```

lambda_o:
000200000000000000000000000000000000
000000000000000000000000000000000000

lambda_c:
000000000000000000000000000000000000
000000000000000000000000000000000000

lampda_o_lambda_c:
000200000000000000000000000000000000
000000000000000000000000000000000000
000000000000000000000000000000000000
000000000000000000000000000000000000

h:
897C32E05E776FD988C5171FE70BB729
49172E514E3308A871BA5BD898FB6EBD
6E3897D2D55697D90D6428216C08052E
3A5E7D4626F4DBBF1546CE21637357A3

```

В.9 Вироблення імітовставки і гамування

В.9.1 Перетворення $N_B = 4$, $q = 128$ (Калина-128/128-ССМ-32,128)

В.9.1.1 Вироблення імітовставки для відкритої та конфіденційної частини повідомлення

```

KEY:
000102030405060708090A0B0C0D0E0F

IV:
101112131415161718191A1B1C1D1E1F

AUTHTEXT:
202122232425262728292A2B2C2D2E2F

PLAINTEXT (N = 128):
303132333435363738393A3B3C3D3E3F

G1:
101112131415161718191A10000000B3

lambda_o:
10000000
padded:
101112131415161718191A10000000B3

100000000000000000000000000000000000
202122232425262728292A2B2C2D2E2F

b [1]:
0C5EC98C81929257F2CA491219D8924E

b [2]:
4B86CC2BC0A2A8010CFB536DC06AA138

B:
4B86CC2BC0A2A8010CFB536DC06AA138

bs [0]:
4B86CC2BC0A2A8010CFB536DC06AA138

bs [1]:

```

26A936173A4DC9160D6E3FDA3A974060

h:

26A936173A4DC9160D6E3FDA3A974060

В.9.1.2 Пряме перетворення

KEY:

000102030405060708090A0B0C0D0E0F

IV:

101112131415161718191A1B1C1D1E1F

PLAINTEXT (N = 128):

303132333435363738393A3B3C3D3E3F

h:

26A936173A4DC9160D6E3FDA3A974060

CIPHERTEXT:

B91A7B8790BBCFCFE65D04E5538E98E2
704454C9DD39ADACE0B19D03F6AAB07E

В.9.1.3 Обернене перетворення

KEY:

000102030405060708090A0B0C0D0E0F

IV:

101112131415161718191A1B1C1D1E1F

AUTHTEXT:

202122232425262728292A2B2C2D2E2F

CIPHERTEXT (N = 256):

B91A7B8790BBCFCFE65D04E5538E98E2
704454C9DD39ADACE0B19D03F6AAB07E

PLAINTEXT:

303132333435363738393A3B3C3D3E3F
26A936173A4DC9160D6E3FDA3A974060

h:

26A936173A4DC9160D6E3FDA3A974060

PLAINTEXT:

303132333435363738393A3B3C3D3E3F

В.9.2 Перетворення $N_B = 4$, $q = 128$ (Калина-128/256-ССМ-32,128)

В.9.2.1 Вироблення імітовставки для відкритої та конфіденційної частини повідомлення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F

AUTHTEXT:

303132333435363738393A3B

PLAINTEXT (N = 120):

```

404142434445464748494A4B4C4D4E
G1:
202122232425262728292A0F000000B3

lambda_o:
0C000000
padded:
202122232425262728292A0F000000B3
0C000000303132333435363738393A3B

b [1]:
E1E35176A6E3B5E1347920B2BF9ABE2C

B:
E1E35176A6E3B5E1347920B2BF9ABE2C

bs [0]:
E1E35176A6E3B5E1347920B2BF9ABE2C

bs [1]:
6C47296FF6F64D3FB8351B8407E791D5

h:
6C47296FF6F64D3FB8351B8407E791D5

```

В.9.2.2 Пряме перетворення

```

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F

PLAINTEXT (N = 120):
404142434445464748494A4B4C4D4E

h:
6C47296FF6F64D3FB8351B8407E791D5

CIPHERTEXT:
EF93E26C7D5EB27111A1887225930435
85DF9998FE26308ACBA4FC0EB5F2C7

```

В.9.2.3 Обернене перетворення

```

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F

AUTHTEXT:
303132333435363738393A3B

CIPHERTEXT (N = 248):
EF93E26C7D5EB27111A1887225930435
85DF9998FE26308ACBA4FC0EB5F2C7
PLAINTEXT:
404142434445464748494A4B4C4D4E6C
47296FF6F64D3FB8351B8407E791D5

h:
6C47296FF6F64D3FB8351B8407E791D5

```

PLAINTEXT:

404142434445464748494A4B4C4D4E

В.9.3 Перетворення $N_B = 4$, $q = 128$ (Калина-256/256-ССМ-32,128)

В.9.3.1 Вироблення імітовставки для відкритої та конфіденційної частини повідомлення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

AUTHTEXT:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

PLAINTEXT (N = 512):

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

G1:

202122232425262728292A2B2C2D2E2F
303132333435363738393A40000000B3

lambda_o:

20000000

padded:

202122232425262728292A2B2C2D2E2F
303132333435363738393A40000000B3

20000000000000000000000000000000
00000000000000000000000000000000
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

b [1]:

F1C2965D7AD62B60D8CA14D7B9537F23
6F2CC6130F7ADBB5E070B3EBC99E1EED

b [2]:

648C0AD4F4E9F222FC11430250D4F6BA
F915F567DA45A47915CAD11AEE2C5083

B:

648C0AD4F4E9F222FC11430250D4F6BA
F915F567DA45A47915CAD11AEE2C5083

bs [0]:

648C0AD4F4E9F222FC11430250D4F6BA
F915F567DA45A47915CAD11AEE2C5083

bs [1]:

981DD6AB44A5A1EB5ADD36F6D5A89C63
0261C964D49FD49EC17DB3F054D56535

bs [2]:

9AB831B4B0BF0FDBC36E4B4FD58F0F00

20D08410987B083FECB37F1EAF231E95

h:

9AB831B4B0BF0FDBC36E4B4FD58F0F00

В.9.3.2 Пряме перетворення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 512):

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

h:

9AB831B4B0BF0FDBC36E4B4FD58F0F00

CIPHERTEXT:

7EC15C54BB553CB1437BE0EFDD2E810F
6058497EBCE4408A08A73FADF3F459D5
6B0103702D13AB73ACD2EB33A8B5E9CF
FF5EB21865A6B499C10C810C4BAEBE80
9C48AD90A9E12A68380EF1C1B7C83EE1

В.9.3.3 Обернене перетворення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

AUTHTEXT:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

CIPHERTEXT (N = 640):

7EC15C54BB553CB1437BE0EFDD2E810F
6058497EBCE4408A08A73FADF3F459D5
6B0103702D13AB73ACD2EB33A8B5E9CF
FF5EB21865A6B499C10C810C4BAEBE80
9C48AD90A9E12A68380EF1C1B7C83EE1

PLAINTEXT:

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
9AB831B4B0BF0FDBC36E4B4FD58F0F00

h:

9AB831B4B0BF0FDBC36E4B4FD58F0F00

PLAINTEXT:

606162636465666768696A6B6C6D6E6F

707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

В.9.4 Перетворення $N_B = 6$, $q = 256$ (Калина-256/512-ССМ-48,256)

В.9.4.1 Вироблення імітовставки для відкритої та конфіденційної частини повідомлення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

AUTHTEXT:

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

PLAINTEXT (N = 512):

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

G1:

404142434445464748494A4B4C4D4E4F
505152535455565758400000000000C5

lambda_o:

200000000000

padded:

404142434445464748494A4B4C4D4E4F
505152535455565758400000000000C5

20000000000000000000000000000000
00000000000000000000000000000000
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

b [1]:

76FB1CB905D163DF25DBEB3DF644551
335E079369F6C57481B8DA5B52C2DC2F

b [2]:

88F83C8FA49038EDCF01B6B1DD385BBF
2E6AEE3F08E076F298C64EB604AAA62B

B:

88F83C8FA49038EDCF01B6B1DD385BBF
2E6AEE3F08E076F298C64EB604AAA62B

bs [0]:

88F83C8FA49038EDCF01B6B1DD385BBF
2E6AEE3F08E076F298C64EB604AAA62B

bs [1]:

AA140A717AAD00E6C2D08B7E5FACDC0F
7B48BB2A91A37697F89D81F9F2BF485A

bs [2]:

924FA0326824355595C98028E84D8627
9CEA9135FAB35F22054AE3203E68AE46

h:

924FA0326824355595C98028E84D8627
9CEA9135FAB35F22054AE3203E68AE46

В.9.4.2 Пряме перетворення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

PLAINTEXT (N = 512):

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

h:

924FA0326824355595C98028E84D8627
9CEA9135FAB35F22054AE3203E68AE46

CIPHERTEXT:

3EBDB4584B5169A26FBEB0295B4223F
58D5D8A031F2950A1D7764FAB97BA058
E9E2DAB90FF0C519AA88435155A71B7B
53BB100F5D20AFFAC0552F5F2813DEE8
DD3653491737B9615A5CCD83DB32F1E4
79BF227C050325BBBFF60BCA9558D7FE

В.9.4.3 Обернене перетворення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

AUTHTEXT:

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

CIPHERTEXT (N = 768):

3EBDB4584B5169A26FBEB0295B4223F
58D5D8A031F2950A1D7764FAB97BA058
E9E2DAB90FF0C519AA88435155A71B7B
53BB100F5D20AFFAC0552F5F2813DEE8
DD3653491737B9615A5CCD83DB32F1E4
79BF227C050325BBBFF60BCA9558D7FE

PLAINTEXT:

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
924FA0326824355595C98028E84D8627
9CEA9135FAB35F22054AE3203E68AE46

h:

924FA0326824355595C98028E84D8627
9CEA9135FAB35F22054AE3203E68AE46

PLAINTEXT:

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF

В.9.5 Перетворення $N_B = 8$, $q = 512$ (Калина-512/512-CCM-64,512)

В.9.5.1 Вироблення імітовставки для відкритої та конфіденційної частини повідомлення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

AUTHTEXT:

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF

PLAINTEXT (N = 512):

C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEFF
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

G1:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475764000000000000000E7

lambda_o:

4000000000000000

padded:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475764000000000000000E7

40000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF

B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

b [1]:

6AC7549BD6938E63C49C1D8B8B36C96B
7F097D75247B19B82AAFC59763A49E3F
1212E3F9CCE3DC32FE9873F08CB29228
E71F24F1FF11010816CD2F0FBCE672DD

b [2]:

495AC38C32F0D3B13CA82A3CC8F075D4
27616C87C870AF6E3BCAC79B35FE9762
2817DD4DD6F5AC554F08AC32B40AFA3B
04797B9EA123711D463431B0077822A3

B:

495AC38C32F0D3B13CA82A3CC8F075D4
27616C87C870AF6E3BCAC79B35FE9762
2817DD4DD6F5AC554F08AC32B40AFA3B
04797B9EA123711D463431B0077822A3

bs [0]:

495AC38C32F0D3B13CA82A3CC8F075D4
27616C87C870AF6E3BCAC79B35FE9762
2817DD4DD6F5AC554F08AC32B40AFA3B
04797B9EA123711D463431B0077822A3

bs [1]:

D4155EC3D888C8D32FE184AC260FD60F
567705E1DF362A6F1F9C287156AA96D9
1BC4C56F9709E72F3D79CF0A9AC8BDC2
BA836BE50E823AB50FB1B39080390923

h:

D4155EC3D888C8D32FE184AC260FD60F
567705E1DF362A6F1F9C287156AA96D9
1BC4C56F9709E72F3D79CF0A9AC8BDC2
BA836BE50E823AB50FB1B39080390923

В.9.5.2 Пряме перетворення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

PLAINTEXT (N = 512):

C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEF
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

h:

D4155EC3D888C8D32FE184AC260FD60F
567705E1DF362A6F1F9C287156AA96D9
1BC4C56F9709E72F3D79CF0A9AC8BDC2
BA836BE50E823AB50FB1B39080390923

CIPHERTEXT:

220642D7277D104788CF97B10210984F
506435512F7BF153C5CDABFECC10AFB4
A2E2FC51F616AF80FFDD0607FAD4F542
B8EF0667717CE3EAAA8FBC303CE76C99
BD8F80CE149143C04FC2490272A31B02
9DDADA82F055FE4ABEF452A7D438B21E
59C1D8B3DD4606BAD66A6F36300EF3CE
0E5F3BB59F11416E80B7FC5A8E8B057A

В.9.5.3 Обернене перетворення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

AUTHTEXT:

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF

CIPHERTEXT (N = 1024):

220642D7277D104788CF97B10210984F
506435512F7BF153C5CDABFECC10AFB4
A2E2FC51F616AF80FFDD0607FAD4F542
B8EF0667717CE3EAAA8FBC303CE76C99
BD8F80CE149143C04FC2490272A31B02
9DDADA82F055FE4ABEF452A7D438B21E
59C1D8B3DD4606BAD66A6F36300EF3CE
0E5F3BB59F11416E80B7FC5A8E8B057A

PLAINTEXT:

C0C1C2C3C4C5C6C7C8C9CACBCCDCCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEF
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
D4155EC3D888C8D32FE184AC260FD60F
567705E1DF362A6F1F9C287156AA96D9
1BC4C56F9709E72F3D79CF0A9AC8BDC2
BA836BE50E823AB50FB1B39080390923

h:

D4155EC3D888C8D32FE184AC260FD60F
567705E1DF362A6F1F9C287156AA96D9
1BC4C56F9709E72F3D79CF0A9AC8BDC2
BA836BE50E823AB50FB1B39080390923

PLAINTEXT:

C0C1C2C3C4C5C6C7C8C9CACBCCDCCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEF
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

В.10 Індексована заміна

В.10.1 Перетворення Калина-128/128-XTS та Калина-128/128-XTS-p

В.10.1.1 Зашифрування без доповнення

```

KEY:
  000102030405060708090A0B0C0D0E0F

IV:
  101112131415161718191A1B1C1D1E1F

PLAINTEXT (N = 256):
  202122232425262728292A2B2C2D2E2F
  303132333435363738393A3B3C3D3E3F

ctr:
  81BF1C7D779BAC20E1C9EA39B4D2AD06

alpha_^_1:
  02000000000000000000000000000000

alpha_^_mult_s:
  027F39FAEE365941C293D57368A55B0D

CIPHERTEXT [1]:
  B3E431B3FBAF31108C302669EE7116D1

alpha_^_2:
  04000000000000000000000000000000

alpha_^_mult_s:
  04FE72F4DD6DB2828427ABE7D04AB71A

CIPHERTEXT [2]:
  CF518B6D329D30618DF5628E426BDEF1

CIPHERTEXT:
  B3E431B3FBAF31108C302669EE7116D1
  CF518B6D329D30618DF5628E426BDEF1

```

В.10.1.2 Розшифрування без доповнення

```

KEY:
  000102030405060708090A0B0C0D0E0F

IV:
  101112131415161718191A1B1C1D1E1F

CIPHERTEXT (N = 256):
  B3E431B3FBAF31108C302669EE7116D1
  CF518B6D329D30618DF5628E426BDEF1

ctr:
  81BF1C7D779BAC20E1C9EA39B4D2AD06

alpha_^_1:
  02000000000000000000000000000000

alpha_^_mult_s:
  027F39FAEE365941C293D57368A55B0D

```

PLAINTEXT [1]:
202122232425262728292A2B2C2D2E2F

alpha_^_2:
04000000000000000000000000000000

alpha_^_mult_s:
04FE72F4DD6DB2828427ABE7D04AB71A

PLAINTEXT [2]:
303132333435363738393A3B3C3D3E3F

PLAINTEXT:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

В.10.1.3 Зашифрування із доповненням

KEY:
000102030405060708090A0B0C0D0E0F

IV:
101112131415161718191A1B1C1D1E1F

PLAINTEXT (N = 240):
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D

ctr:
81BF1C7D779BAC20E1C9EA39B4D2AD06

alpha_^_1:
02000000000000000000000000000000

alpha_^_mult_s:
027F39FAEE365941C293D57368A55B0D

CIPHERTEXT [1]:
B3E431B3FBAF31108C302669EE7116D1

alpha_^_2:
04000000000000000000000000000000

alpha_^_mult_s:
04FE72F4DD6DB2828427ABE7D04AB71A

PLAINTEXT [2]:
303132333435363738393A3B3C3D

padded:
303132333435363738393A3B3C3D16D1

CIPHERTEXT [2]:
48F3055ED2832222085005209C9D4D41

CIPHERTEXT:
48F3055ED2832222085005209C9D4D41
B3E431B3FBAF31108C302669EE71

В.10.1.4 Розшифрування із доповненням

KEY:
000102030405060708090A0B0C0D0E0F

```

IV:
  101112131415161718191A1B1C1D1E1F

CIPHERTEXT (N = 240):
  48F3055ED283222085005209C9D4D41
  B3E431B3FBAF31108C302669EE71
ctr:
  81BF1C7D779BAC20E1C9EA39B4D2AD06

alpha_^_2:
  04000000000000000000000000000000

alpha_^_mult_s:
  04FE72F4DD6DB2828427ABE7D04AB71A

PLAINTEXT [1]:
  303132333435363738393A3B3C3D16D1

CIPHERTEXT [1]:
  16D1
alpha_^_1:
  02000000000000000000000000000000

alpha_^_mult_s:
  027F39FAEE365941C293D57368A55B0D

CIPHERTEXT [0]:
  B3E431B3FBAF31108C302669EE71
padded:
  B3E431B3FBAF31108C302669EE7116D1

PLAINTEXT [0]:
  202122232425262728292A2B2C2D2E2F

PLAINTEXT:
  202122232425262728292A2B2C2D2E2F
  303132333435363738393A3B3C3D

```

В.10.2 Перетворення Калина-128/256-XTS та Калина-128/256-XTS-p

В.10.2.1 Зашифрування без доповнення

```

KEY:
  000102030405060708090A0B0C0D0E0F
  101112131415161718191A1B1C1D1E1F

IV:
  202122232425262728292A2B2C2D2E2F

PLAINTEXT (N = 256):
  303132333435363738393A3B3C3D3E3F
  404142434445464748494A4B4C4D4E4F

ctr:
  58EC3E091000158A1148F7166F334F14

alpha_^_1:
  02000000000000000000000000000000

alpha_^_mult_s:
  B0D87D1220002A142390EE2DDE669E28

```

CIPHERTEXT [1]:
830AC78A6F629CB4C7D5D156FD84955B

alpha_^_2:
04000000000000000000000000000000

alpha_^_mult_s:
60B1FB24400054284620DD5BBCCD3C51

CIPHERTEXT [2]:
D0998CA1E0BC1FF135676BF2A2598FA1

CIPHERTEXT:
830AC78A6F629CB4C7D5D156FD84955B
D0998CA1E0BC1FF135676BF2A2598FA1

В.10.2.2 Розшифрування без доповнення

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F

CIPHERTEXT (N = 256):
830AC78A6F629CB4C7D5D156FD84955B
D0998CA1E0BC1FF135676BF2A2598FA1

ctr:
58EC3E091000158A1148F7166F334F14

alpha_^_1:
02000000000000000000000000000000

alpha_^_mult_s:
B0D87D1220002A142390EE2DDE669E28

PLAINTEXT [1]:
303132333435363738393A3B3C3D3E3F

alpha_^_2:
04000000000000000000000000000000

alpha_^_mult_s:
60B1FB24400054284620DD5BBCCD3C51

PLAINTEXT [2]:
404142434445464748494A4B4C4D4E4F

PLAINTEXT:
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F

В.10.2.3 Зашифрування із доповненням

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F

```

PLAINTEXT (N = 328):
  303132333435363738393A3B3C3D3E3F
  404142434445464748494A4B4C4D4E4F
  505152535455565758
ctr:
  58EC3E091000158A1148F7166F334F14

alpha_^_1:
  02000000000000000000000000000000

alpha_^_mult_s:
  B0D87D1220002A142390EE2DDE669E28

CIPHERTEXT [1]:
  830AC78A6F629CB4C7D5D156FD84955B

alpha_^_2:
  04000000000000000000000000000000

alpha_^_mult_s:
  60B1FB24400054284620DD5BBCCD3C51

CIPHERTEXT [2]:
  D0998CA1E0BC1FF135676BF2A2598FA1

alpha_^_3:
  08000000000000000000000000000000

alpha_^_mult_s:
  C062F7498000A8508C40BAB7789B79A2

PLAINTEXT [3]:
  505152535455565758
padded:
  505152535455565758676BF2A2598FA1

CIPHERTEXT [3]:
  470EEFDDEE38B59F0D836B65635B0A63

CIPHERTEXT:
  830AC78A6F629CB4C7D5D156FD84955B
  470EEFDDEE38B59F0D836B65635B0A63
  D0998CA1E0BC1FF135

```

В.10.2.4 Розшифрування із доповненням

```

KEY:
  000102030405060708090A0B0C0D0E0F
  101112131415161718191A1B1C1D1E1F

IV:
  202122232425262728292A2B2C2D2E2F

CIPHERTEXT (N = 328):
  830AC78A6F629CB4C7D5D156FD84955B
  470EEFDDEE38B59F0D836B65635B0A63
  D0998CA1E0BC1FF135
ctr:
  58EC3E091000158A1148F7166F334F14

alpha_^_1:
  02000000000000000000000000000000

alpha_^_mult_s:

```


B0D87D1220002A142390EE2DDE669E28

PLAINTEXT [1]:
303132333435363738393A3B3C3D3E3F

alpha_[^]_3:
08000000000000000000000000000000

alpha_[^]_mult_s:
C062F7498000A8508C40BAB7789B79A2

PLAINTEXT [2]:
505152535455565758676BF2A2598FA1

CIPHERTEXT [2]:
676BF2A2598FA1

alpha_[^]_2:
04000000000000000000000000000000

alpha_[^]_mult_s:
60B1FB24400054284620DD5BBCCD3C51

CIPHERTEXT [1]:
D0998CA1E0BC1FF135

padding:
D0998CA1E0BC1FF135676BF2A2598FA1

PLAINTEXT [1]:
404142434445464748494A4B4C4D4E4F

PLAINTEXT:
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758

В.10.3 Перетворення Калина-256/256-XTS та Калина-256/256-XTS-p

В.10.3.1 Зашифрування без доповнення

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 768):
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

ctr:
F66E3D570EC92135AEDAE323DCBD2A8C
A03963EC206A0D5A88385C24617FD92C

alpha_[^]_1:
02000000000000000000000000000000
00000000000000000000000000000000

alpha_[^]_mult_s:

ECDD7AAE1C92436A5CB5C747B87B5518
4173C6D841D41AB41071B848C2FEB259

CIPHERTEXT [1]:

E0E51EAEA6A3134600758EA7F87E8802
5D8B82897C8DB099B843054C3A518837

alpha_^_2:

04000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:

D8BBF55C392487D4B86A8F8F70F7AA30
82E68CB183A8356821E2709184FD65B3

CIPHERTEXT [2]:

56913571530BA8FA23003E337627E698
674B807E847EC6B2292627736562F9F6

alpha_^_3:

08000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:

9573EBB972480EA971D51E1FE1EE5561
04CD196307516BD042C4E12209FBCB66

CIPHERTEXT [3]:

2B2DE9E6AAC5DF74C09A0C5CF8028017
4AEC9BDD4E73F7D63EDBC29A6922637A

CIPHERTEXT:

E0E51EAEA6A3134600758EA7F87E8802
5D8B82897C8DB099B843054C3A518837
56913571530BA8FA23003E337627E698
674B807E847EC6B2292627736562F9F6
2B2DE9E6AAC5DF74C09A0C5CF8028017
4AEC9BDD4E73F7D63EDBC29A6922637A

В.10.3.2 Розшифрування без доповнення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

CIPHERTEXT (N = 768):

E0E51EAEA6A3134600758EA7F87E8802
5D8B82897C8DB099B843054C3A518837
56913571530BA8FA23003E337627E698
674B807E847EC6B2292627736562F9F6
2B2DE9E6AAC5DF74C09A0C5CF8028017
4AEC9BDD4E73F7D63EDBC29A6922637A

ctr:

F66E3D570EC92135AEDAE323DCBD2A8C
A03963EC206A0D5A88385C24617FD92C

alpha_^_1:

02000000000000000000000000000000

00000000000000000000000000000000

alpha_^_mult_s:
ECDD7AAE1C92436A5CB5C747B87B5518
4173C6D841D41AB41071B848C2FEB259

PLAINTEXT [1]:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

alpha_^_2:
04000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:
D8BBF55C392487D4B86A8F8F70F7AA30
82E68CB183A8356821E2709184FD65B3

PLAINTEXT [2]:
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

alpha_^_3:
08000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:
9573EBB972480EA971D51E1FE1EE5561
04CD196307516BD042C4E12209FBCB66

PLAINTEXT [3]:
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

PLAINTEXT:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

В.10.3.3 Зашифрування із доповненням

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 520):
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
80

ctr:
F66E3D570EC92135AEDAE323DCBD2A8C
A03963EC206A0D5A88385C24617FD92C

alpha_^_1:
02000000000000000000000000000000

00000000000000000000000000000000

alpha_^_mult_s:
ECDD7AAE1C92436A5CB5C747B87B5518
4173C6D841D41AB41071B848C2FEB259

CIPHERTEXT [1]:
E0E51EAEA6A3134600758EA7F87E8802
5D8B82897C8DB099B843054C3A518837

alpha_^_2:
04000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:
D8BBF55C392487D4B86A8F8F70F7AA30
82E68CB183A8356821E2709184FD65B3

CIPHERTEXT [2]:
56913571530BA8FA23003E337627E698
674B807E847EC6B2292627736562F9F6

alpha_^_3:
08000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:
9573EBB972480EA971D51E1FE1EE5561
04CD196307516BD042C4E12209FBCB66

PLAINTEXT [3]:
80
padded:
80913571530BA8FA23003E337627E698
674B807E847EC6B2292627736562F9F6

CIPHERTEXT [3]:
4F5254E38066B77FA14FEE3292464B60
7E8AF1398B2A91C4480B698D64D13AE8

CIPHERTEXT:
E0E51EAEA6A3134600758EA7F87E8802
5D8B82897C8DB099B843054C3A518837
4F5254E38066B77FA14FEE3292464B60
7E8AF1398B2A91C4480B698D64D13AE8
56

В.10.3.4 Розшифрування із доповненням

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

IV:
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

CIPHERTEXT (N = 520):
E0E51EAEA6A3134600758EA7F87E8802
5D8B82897C8DB099B843054C3A518837
4F5254E38066B77FA14FEE3292464B60
7E8AF1398B2A91C4480B698D64D13AE8
56

ctr:

F66E3D570EC92135AEDAE323DCBD2A8C
A03963EC206A0D5A88385C24617FD92C

alpha_^_1:
02000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:
ECDD7AAE1C92436A5CB5C747B87B5518
4173C6D841D41AB41071B848C2FEB259

PLAINTEXT [1]:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

alpha_^_3:
08000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:
9573EBB972480EA971D51E1FE1EE5561
04CD196307516BD042C4E12209FBCB66

PLAINTEXT [2]:
80913571530BA8FA23003E337627E698
674B807E847EC6B2292627736562F9F6

CIPHERTEXT [2]:
913571530BA8FA23003E337627E69867
4B807E847EC6B2292627736562F9F6

alpha_^_2:
04000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:
D8BBF55C392487D4B86A8F8F70F7AA30
82E68CB183A8356821E2709184FD65B3

CIPHERTEXT [1]:
56
padded:
56913571530BA8FA23003E337627E698
674B807E847EC6B2292627736562F9F6

PLAINTEXT [1]:
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

PLAINTEXT:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
80

В.10.4 Перетворення Калина-256/512-XTS та Калина-256/512-XTS-p

В.10.4.1 Зашифрування без доповнення

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F

303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

PLAINTEXT (N = 768):

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

ctr:

606990E9E6B7B67A4BD6D893D72268B7
8E02C83C3CD7E102FD2E74A8FDFE5DD9

alpha_^_1:

02000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:

E5D620D3CD6F6DF596ACB127AF45D06E
1D05907978AEC305FA5DE850FBFDBBB2

CIPHERTEXT [1]:

30663E4686574B343A1898E46973CD37
DB9D775D356512EB59E723397F2A333C

alpha_^_2:

04000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:

EFA941A69BDFDAEA2D59634F5E8BA0DD
3A0A20F3F05C870BF4BBD0A1F6FB7765

CIPHERTEXT [2]:

E2C0E96538781FF48EA1D93BDF88FFF8
BB7BC4FB80A609881220C7FE21881C73

alpha_^_3:

08000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:

DE53834C37BFB5D55BB2C69EBC1641BB
751440E6E1B90E17E877A143EDF7EFCA

CIPHERTEXT [3]:

74F65B232A8F94CD0E3DDC7614830C23
CFCE98ADC5113496F9E106E8C8BFF3AB

CIPHERTEXT:

30663E4686574B343A1898E46973CD37
DB9D775D356512EB59E723397F2A333C
E2C0E96538781FF48EA1D93BDF88FFF8
BB7BC4FB80A609881220C7FE21881C73
74F65B232A8F94CD0E3DDC7614830C23
CFCE98ADC5113496F9E106E8C8BFF3AB

В.10.4.2 Розшифрування без доповнення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

CIPHERTEXT (N = 768):

30663E4686574B343A1898E46973CD37
DB9D775D356512EB59E723397F2A333C
E2C0E96538781FF48EA1D93BDF88FFF8
BB7BC4FB80A609881220C7FE21881C73
74F65B232A8F94CD0E3DDC7614830C23
CFCE98ADC5113496F9E106E8C8BFF3AB

ctr:

606990E9E6B7B67A4BD6D893D72268B7
8E02C83C3CD7E102FD2E74A8FDFE5DD9

alpha_[^]_1:

02000000000000000000000000000000
00000000000000000000000000000000

alpha_[^]_mult_s:

E5D620D3CD6F6DF596ACB127AF45D06E
1D05907978AEC305FA5DE850FBFDBBB2

PLAINTEXT [1]:

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

alpha_[^]_2:

04000000000000000000000000000000
00000000000000000000000000000000

alpha_[^]_mult_s:

EFA941A69BDFDAEA2D59634F5E8BA0DD
3A0A20F3F05C870BF4BBD0A1F6FB7765

PLAINTEXT [2]:

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

alpha_[^]_3:

08000000000000000000000000000000
00000000000000000000000000000000

alpha_[^]_mult_s:

DE53834C37BFB5D55BB2C69EBC1641BB
751440E6E1B90E17E877A143EDF7EFCA

PLAINTEXT [3]:

A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF

PLAINTEXT:

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F

```

909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

```

В.10.4.3 Зашифрування із доповненням

KEY:

```

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

```

IV:

```

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

```

PLAINTEXT (N = 520):

```

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0

```

ctr:

```

606990E9E6B7B67A4BD6D893D72268B7
8E02C83C3CD7E102FD2E74A8FDFE5DD9

```

alpha_[^]_1:

```

02000000000000000000000000000000
00000000000000000000000000000000

```

alpha_[^]_mult_s:

```

E5D620D3CD6F6DF596ACB127AF45D06E
1D05907978AEC305FA5DE850FBFDBBB2

```

CIPHERTEXT [1]:

```

30663E4686574B343A1898E46973CD37
DB9D775D356512EB59E723397F2A333C

```

alpha_[^]_2:

```

04000000000000000000000000000000
00000000000000000000000000000000

```

alpha_[^]_mult_s:

```

EFA941A69BDFDAEA2D59634F5E8BA0DD
3A0A20F3F05C870BF4BBD0A1F6FB7765

```

CIPHERTEXT [2]:

```

E2C0E96538781FF48EA1D93BDF88FFF8
BB7BC4FB80A609881220C7FE21881C73

```

alpha_[^]_3:

```

08000000000000000000000000000000
00000000000000000000000000000000

```

alpha_[^]_mult_s:

```

DE53834C37BFB5D55BB2C69EBC1641BB
751440E6E1B90E17E877A143EDF7EFCA

```

PLAINTEXT [3]:

A0

padded:

```

A0C0E96538781FF48EA1D93BDF88FFF8
BB7BC4FB80A609881220C7FE21881C73

```


CIPHERTEXT [3]:

6DE04CB3235A2DA92493537248DE4368
879A7CC4166B25C9BFD1AD8EAEA3484B

CIPHERTEXT:

30663E4686574B343A1898E46973CD37
DB9D775D356512EB59E723397F2A333C
6DE04CB3235A2DA92493537248DE4368
879A7CC4166B25C9BFD1AD8EAEA3484B
E2

В.10.4.4 Розшифрування із доповненням

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

CIPHERTEXT (N = 520):

30663E4686574B343A1898E46973CD37
DB9D775D356512EB59E723397F2A333C
6DE04CB3235A2DA92493537248DE4368
879A7CC4166B25C9BFD1AD8EAEA3484B
E2

ctr:

606990E9E6B7B67A4BD6D893D72268B7
8E02C83C3CD7E102FD2E74A8FDFE5DD9

alpha_¹:

02000000000000000000000000000000
00000000000000000000000000000000

alpha_^{mult}:

E5D620D3CD6F6DF596ACB127AF45D06E
1D05907978AEC305FA5DE850FBFDBBB2

PLAINTEXT [1]:

606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

alpha_³:

08000000000000000000000000000000
00000000000000000000000000000000

alpha_^{mult}:

DE53834C37BFB5D55BB2C69EBC1641BB
751440E6E1B90E17E877A143EDF7EFCA

PLAINTEXT [2]:

A0C0E96538781FF48EA1D93BDF88FFF8
BB7BC4FB80A609881220C7FE21881C73

CIPHERTEXT [2]:

C0E96538781FF48EA1D93BDF88FFF8BB
7BC4FB80A609881220C7FE21881C73

alpha_²:

04000000000000000000000000000000
00000000000000000000000000000000

```
alpha_^_mult_s:
EFA941A69BDFDAEA2D59634F5E8BA0DD
3A0A20F3F05C870BF4BBD0A1F6FB7765
```

```
CIPHERTEXT [1]:
E2
padded:
E2C0E96538781FF48EA1D93BDF88FFF8
BB7BC4FB80A609881220C7FE21881C73
```

```
PLAINTEXT [1]:
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
```

```
PLAINTEXT:
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0
```

В.10.5 Перетворення Калина-512/512-XTS та Калина-512/512-XTS-p

В.10.5.1 Зашифрування без доповнення

```
KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
```

```
IV:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
```

```
PLAINTEXT (N = 1024):
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEF
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
```

```
ctr:
4A26E31B811C356AA61DD6CA0596231A
67BA8354AA47F3A13E1DEEC320EB56B8
95D0F417175BAB662FD6F134BB15C86C
CB906A26856EFEB7C5BC6472940DD9D9
```

```
alpha_^_1:
02000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
```

```
alpha_^_mult_s:
B14DC63702396AD44C3BAC950B2C4734
CE7407A9548FE6437D3ADC8741D6AD70
2BA1E92F2EB656CD5EACE369762B90D9
```

9621D54C0ADDFC6F8B79C9E4281BB2B3

CIPHERTEXT [1]:

5C6250BD2E40AAE27E1E57512CD38E6A
51D0C2B04F0D6A50E0CB43358B8C4E8B
A361331436C6FFD38D77BBBBF5FEC56A
234108A6CC8CB298360943E849E5BD64

alpha_^_2:

04000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000

alpha_^_mult_s:

479A8C6F0472D4A89976582B17588E68
9CE90E52A91ECD87FA74B80F83AC5BE1
5642D35F5C6CAD9ABD58C7D3EC5620B3
2D43AA9914BAF9DF16F392C951366467

CIPHERTEXT [2]:

D26ECA2FA8AEAD070656C3777BA412BC
AF3D2F08C26CF86CA8F0921043A15D70
9AE1112611E22D4396E582CCB661E0F7
78B6F38561BC338AFD5D1036ED8B322D

CIPHERTEXT:

5C6250BD2E40AAE27E1E57512CD38E6A
51D0C2B04F0D6A50E0CB43358B8C4E8B
A361331436C6FFD38D77BBBBF5FEC56A
234108A6CC8CB298360943E849E5BD64
D26ECA2FA8AEAD070656C3777BA412BC
AF3D2F08C26CF86CA8F0921043A15D70
9AE1112611E22D4396E582CCB661E0F7
78B6F38561BC338AFD5D1036ED8B322D

В.10.5.2 Розшифрування без доповнення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

CIPHERTEXT (N = 1024):

5C6250BD2E40AAE27E1E57512CD38E6A
51D0C2B04F0D6A50E0CB43358B8C4E8B
A361331436C6FFD38D77BBBBF5FEC56A
234108A6CC8CB298360943E849E5BD64
D26ECA2FA8AEAD070656C3777BA412BC
AF3D2F08C26CF86CA8F0921043A15D70
9AE1112611E22D4396E582CCB661E0F7
78B6F38561BC338AFD5D1036ED8B322D

ctr:

4A26E31B811C356AA61DD6CA0596231A
67BA8354AA47F3A13E1DEEC320EB56B8

95D0F417175BAB662FD6F134BB15C86C
CB906A26856EFEB7C5BC6472940DD9D9

alpha_[^]_1:

02000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000

alpha_[^]_mult_s:

B14DC63702396AD44C3BAC950B2C4734
CE7407A9548FE6437D3ADC8741D6AD70
2BA1E92F2EB656CD5EACE369762B90D9
9621D54C0ADDFC6F8B79C9E4281BB2B3

PLAINTEXT [1]:

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF

alpha_[^]_2:

04000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000

alpha_[^]_mult_s:

479A8C6F0472D4A89976582B17588E68
9CE90E52A91ECD87FA74B80F83AC5BE1
5642D35F5C6CAD9ABD58C7D3EC5620B3
2D43AA9914BAF9DF16F392C951366467

PLAINTEXT [2]:

C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEF
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

PLAINTEXT:

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEF
F0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

В.10.5.3 Зашифрування із доповненням

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F

PLAINTEXT (N = 776):

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0

ctr:

4A26E31B811C356AA61DD6CA0596231A
67BA8354AA47F3A13E1DEEC320EB56B8
95D0F417175BAB662FD6F134BB15C86C
CB906A26856EFEB7C5BC6472940DD9D9

alpha_¹:

020000000000000000000000000000
000000000000000000000000000000
000000000000000000000000000000
000000000000000000000000000000

alpha_^{mult}__s:

B14DC63702396AD44C3BAC950B2C4734
CE7407A9548FE6437D3ADC8741D6AD70
2BA1E92F2EB656CD5EACE369762B90D9
9621D54C0ADDFC6F8B79C9E4281BB2B3

CIPHERTEXT [1]:

5C6250BD2E40AAE27E1E57512CD38E6A
51D0C2B04F0D6A50E0CB43358B8C4E8B
A361331436C6FFD38D77BBBF5FEC56A
234108A6CC8CB298360943E849E5BD64

alpha_²:

040000000000000000000000000000
000000000000000000000000000000
000000000000000000000000000000
000000000000000000000000000000

alpha_^{mult}__s:

479A8C6F0472D4A89976582B17588E68
9CE90E52A91ECD87FA74B80F83AC5BE1
5642D35F5C6CAD9ABD58C7D3EC5620B3
2D43AA9914BAF9DF16F392C951366467

PLAINTEXT [2]:

C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0

padded:

C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E061331436C6FFD38D77BBBF5FEC56A
234108A6CC8CB298360943E849E5BD64

CIPHERTEXT [2]:

C2822787D3CB2D13168B126583CF28E3
B194F153088CF46BD745B22D1776BCB0
35C6CB17D8C1FBD127954C2A5D5F5AFB
ECF976E34966AB85142192A2463A541F

CIPHERTEXT:

C2822787D3CB2D13168B126583CF28E3
B194F153088CF46BD745B22D1776BCB0
35C6CB17D8C1FBD127954C2A5D5F5AFB
ECF976E34966AB85142192A2463A541F

5C6250BD2E40AAE27E1E57512CD38E6A
 51D0C2B04F0D6A50E0CB43358B8C4E8B
 A3

В.10.5.4 Розшифрування із доповненням

KEY:

000102030405060708090A0B0C0D0E0F
 101112131415161718191A1B1C1D1E1F
 202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F

IV:

404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F

CIPHERTEXT (N = 776):

C2822787D3CB2D13168B126583CF28E3
 B194F153088CF46BD745B22D1776BCB0
 35C6CB17D8C1FBD127954C2A5D5F5AFB
 ECF976E34966AB85142192A2463A541F
 5C6250BD2E40AAE27E1E57512CD38E6A
 51D0C2B04F0D6A50E0CB43358B8C4E8B
 A3

ctr:

4A26E31B811C356AA61DD6CA0596231A
 67BA8354AA47F3A13E1DEEC320EB56B8
 95D0F417175BAB662FD6F134BB15C86C
 CB906A26856EFEB7C5BC6472940DD9D9

alpha_²:

040000000000000000000000000000
 000000000000000000000000000000
 000000000000000000000000000000
 000000000000000000000000000000

alpha_^{mult}_s:

479A8C6F0472D4A89976582B17588E68
 9CE90E52A91ECD87FA74B80F83AC5BE1
 5642D35F5C6CAD9ABD58C7D3EC5620B3
 2D43AA9914BAF9DF16F392C951366467

PLAINTEXT [1]:

C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
 D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
 E061331436C6FFD38D77BBBF5FEC56A
 234108A6CC8CB298360943E849E5BD64

CIPHERTEXT [1]:

61331436C6FFD38D77BBBF5FEC56A23
 4108A6CC8CB298360943E849E5BD64

alpha_¹:

020000000000000000000000000000
 000000000000000000000000000000
 000000000000000000000000000000
 000000000000000000000000000000

alpha_^{mult}_s:

B14DC63702396AD44C3BAC950B2C4734
 CE7407A9548FE6437D3ADC8741D6AD70
 2BA1E92F2EB656CD5EACE369762B90D9
 9621D54C0ADDFC6F8B79C9E4281BB2B3

CIPHERTEXT [0]:

5C6250BD2E40AAE27E1E57512CD38E6A
51D0C2B04F0D6A50E0CB43358B8C4E8B
A3

padded:

5C6250BD2E40AAE27E1E57512CD38E6A
51D0C2B04F0D6A50E0CB43358B8C4E8B
A361331436C6FFD38D77BBBBF5FEC56A
234108A6CC8CB298360943E849E5BD64

PLAINTEXT [0]:

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

PLAINTEXT:

808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0

В.11 Захист ключових даних

В.11.1 Перетворення Калина-128/128-KW та Калина-128/128- KW-p

В.11.1.1 Зашифрування без доповнення

KEY:

000102030405060708090A0B0C0D0E0F

PLAINTEXT (N = 128):

101112131415161718191A1B1C1D1E1F

padded:

1011121314151617 18191A1B1C1D1E1F
0000000000000000 0000000000000000

V:

18

B [0]:

1011121314151617

b [0,2]:

18191A1B1C1D1E1F

b [0,3]:

0000000000000000

b [0,4]:

0000000000000000

B [1]:

E0C9EA39B4D2AD06

b [1,4]:

81BF1C7D779BAC20

b [1,2]:

0000000000000000

b [1,3]:

0000000000000000

B [2]:

9616FF2161DC1C80

b [2,4]:
 846CB27DF9E5EA62
 b [2,2]:
 0000000000000000
 b [2,3]:
 81BF1C7D779BAC20
 B [3]:
 16D4D8040BAB9770
 b [3,4]:
 E8FADC96C0164FC7
 b [3,2]:
 81BF1C7D779BAC20
 b [3,3]:
 846CB27DF9E5EA62
 B [4]:
 2FA7BABA8BEF881E
 b [4,4]:
 97641AE1751E3668
 b [4,2]:
 846CB27DF9E5EA62
 b [4,3]:
 E8FADC96C0164FC7
 B [5]:
 46287D9B32DB6EED
 b [5,4]:
 E39D6755CA9909FA
 b [5,2]:
 E8FADC96C0164FC7
 b [5,3]:
 97641AE1751E3668
 B [6]:
 36C7CBAA83163361
 b [6,4]:
 8C3D01910930FE9D
 b [6,2]:
 97641AE1751E3668
 b [6,3]:
 E39D6755CA9909FA
 B [7]:
 30B3F2DA71B0794A
 b [7,4]:
 2F548F690FAACF71
 b [7,2]:
 E39D6755CA9909FA
 b [7,3]:
 8C3D01910930FE9D
 B [8]:
 6683C7C62F4C11D9
 b [8,4]:
 94C3DD624FDC7F14
 b [8,2]:
 8C3D01910930FE9D
 b [8,3]:
 2F548F690FAACF71
 B [9]:
 2C70C839E442B4F4
 b [9,4]:
 8BC00C8CE891058E
 b [9,2]:
 2F548F690FAACF71
 b [9,3]:
 94C3DD624FDC7F14
 B [10]:
 38F627141D055364
 b [10,4]:

02A65B3741515391
 b [10,2]:
 94C3DD624FDC7F14
 b [10,3]:
 8BC00C8CE891058E
 B [11]:
 55FB3C5537D958A5
 b [11,4]:
 96A46AED96B9B634
 b [11,2]:
 8BC00C8CE891058E
 b [11,3]:
 02A65B3741515391
 B [12]:
 D0B8BCDBE47B86B2
 b [12,4]:
 7D1555B543A661ED
 b [12,2]:
 02A65B3741515391
 b [12,3]:
 96A46AED96B9B634
 B [13]:
 37F77355E52DEC1
 b [13,4]:
 8C547E14C1F348D4
 b [13,2]:
 96A46AED96B9B634
 b [13,3]:
 7D1555B543A661ED
 B [14]:
 A356546DE6BE1DA9
 b [14,4]:
 6AE0EBC1ED2B33E4
 b [14,2]:
 7D1555B543A661ED
 b [14,3]:
 8C547E14C1F348D4
 B [15]:
 413E178CFBED9493
 b [15,4]:
 92EBD515D48E1BDB
 b [15,2]:
 8C547E14C1F348D4
 b [15,3]:
 6AE0EBC1ED2B33E4
 B [16]:
 E96F98BF552828A3
 b [16,4]:
 DBED25ADDA95A1B6
 b [16,2]:
 6AE0EBC1ED2B33E4
 b [16,3]:
 92EBD515D48E1BDB
 B [17]:
 871D4C7C47E05D4C
 b [17,4]:
 AD3E15056E489738
 b [17,2]:
 92EBD515D48E1BDB
 b [17,3]:
 DBED25ADDA95A1B6
 B [18]:
 1DC91DC6E52575F6
 b [18,4]:
 972C199FB9EE2913

b [18,2]:
 DBED25ADDA95A1B6
 b [18,3]:
 AD3E15056E489738
 CIPHERTEXT [1]:
 1DC91DC6E52575F6 DBED25ADDA95A1B6

 CIPHERTEXT [2]:
 AD3E15056E489738 972C199FB9EE2913

 CIPHERTEXT:
 1DC91DC6E52575F6DBED25ADDA95A1B6
 AD3E15056E489738972C199FB9EE2913

В.11.1.2 Розшифрування без доповнення

KEY:
 000102030405060708090A0B0C0D0E0F

 CIPHERTEXT (N = 128):
 1DC91DC6E52575F6DBED25ADDA95A1B6
 AD3E15056E489738972C199FB9EE2913

V:
 18

B [18]:
 1DC91DC6E52575F6
 b [18,2]:
 DBED25ADDA95A1B6
 b [18,3]:
 AD3E15056E489738
 b [18,4]:
 972C199FB9EE2913
 B [18]:
 1DC91DC6E52575F6
 b [18,4]:
 972C199FB9EE2913
 b [18,2]:
 DBED25ADDA95A1B6
 b [18,3]:
 AD3E15056E489738
 B [17]:
 871D4C7C47E05D4C
 b [17,4]:
 AD3E15056E489738
 b [17,2]:
 92EBD515D48E1BDB
 b [17,3]:
 DBED25ADDA95A1B6
 B [16]:
 E96F98BF552828A3
 b [16,4]:
 DBED25ADDA95A1B6
 b [16,2]:
 6AE0EBC1ED2B33E4
 b [16,3]:
 92EBD515D48E1BDB
 B [15]:
 413E178CFBED9493
 b [15,4]:
 92EBD515D48E1BDB
 b [15,2]:
 8C547E14C1F348D4
 b [15,3]:

6AE0EBC1ED2B33E4
 B [14]:
 A356546DE6BE1DA9
 b [14,4]:
 6AE0EBC1ED2B33E4
 b [14,2]:
 7D1555B543A661ED
 b [14,3]:
 8C547E14C1F348D4
 B [13]:
 37F77355E52DECF1
 b [13,4]:
 8C547E14C1F348D4
 b [13,2]:
 96A46AED96B9B634
 b [13,3]:
 7D1555B543A661ED
 B [12]:
 D0B8BCDBE47B86B2
 b [12,4]:
 7D1555B543A661ED
 b [12,2]:
 02A65B3741515391
 b [12,3]:
 96A46AED96B9B634
 B [11]:
 55FB3C5537D958A5
 b [11,4]:
 96A46AED96B9B634
 b [11,2]:
 8BC00C8CE891058E
 b [11,3]:
 02A65B3741515391
 B [10]:
 38F627141D055364
 b [10,4]:
 02A65B3741515391
 b [10,2]:
 94C3DD624FDC7F14
 b [10,3]:
 8BC00C8CE891058E
 B [9]:
 2C70C839E442B4F4
 b [9,4]:
 8BC00C8CE891058E
 b [9,2]:
 2F548F690FAACF71
 b [9,3]:
 94C3DD624FDC7F14
 B [8]:
 6683C7C62F4C11D9
 b [8,4]:
 94C3DD624FDC7F14
 b [8,2]:
 8C3D01910930FE9D
 b [8,3]:
 2F548F690FAACF71
 B [7]:
 30B3F2DA71B0794A
 b [7,4]:
 2F548F690FAACF71
 b [7,2]:
 E39D6755CA9909FA
 b [7,3]:
 8C3D01910930FE9D

```

B [6]:
  36C7CBAA83163361
b [6,4]:
  8C3D01910930FE9D
b [6,2]:
  97641AE1751E3668
b [6,3]:
  E39D6755CA9909FA
B [5]:
  46287D9B32DB6EED
b [5,4]:
  E39D6755CA9909FA
b [5,2]:
  E8FADC96C0164FC7
b [5,3]:
  97641AE1751E3668
B [4]:
  2FA7BABA8BEF881E
b [4,4]:
  97641AE1751E3668
b [4,2]:
  846CB27DF9E5EA62
b [4,3]:
  E8FADC96C0164FC7
B [3]:
  16D4D8040BAB9770
b [3,4]:
  E8FADC96C0164FC7
b [3,2]:
  81BF1C7D779BAC20
b [3,3]:
  846CB27DF9E5EA62
B [2]:
  9616FF2161DC1C80
b [2,4]:
  846CB27DF9E5EA62
b [2,2]:
  0000000000000000
b [2,3]:
  81BF1C7D779BAC20
B [1]:
  E0C9EA39B4D2AD06
b [1,4]:
  81BF1C7D779BAC20
b [1,2]:
  0000000000000000
b [1,3]:
  0000000000000000
PLAINTEXT [1]:
  1011121314151617 18191A1B1C1D1E1F

PLAINTEXT [2]:
  0000000000000000 0000000000000000

PLAINTEXT:
  101112131415161718191A1B1C1D1E1F

```

В.11.1.3 Зашифрування із доповненням

```

KEY:
  000102030405060708090A0B0C0D0E0F

PLAINTEXT (N = 144):

```

```
101112131415161718191A1B1C1D1E1F
2021
padded:
1011121314151617 18191A1B1C1D1E1F
2021900000000000 0000800000000000
0000000000000000 0000000000000000

CIPHERTEXT:
0EA983D6CE48484D51462C32CC616722
10FCC44196ABE635BAF878FDB83E1A63
114128585D49DB355C5819FD38039169
```

В.11.1.4 Розшифрування із доповненням

```
KEY:
000102030405060708090A0B0C0D0E0F

CIPHERTEXT (N = 144):
0EA983D6CE48484D51462C32CC616722
10FCC44196ABE635BAF878FDB83E1A63
114128585D49DB355C5819FD38039169

PLAINTEXT:
101112131415161718191A1B1C1D1E1F
20219000000000000000800000000000

unpadded:
101112131415161718191A1B1C1D1E1F
20219000000000000000

PLAINTEXT:
101112131415161718191A1B1C1D1E1F
2021
```

В.11.2 Перетворення Калина-128/256-KW та Калина-128/256-KW-p

В.11.2.1 Зашифрування без доповнення

```
KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

PLAINTEXT (N = 384):
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F

padded:
2021222324252627 28292A2B2C2D2E2F
3031323334353637 38393A3B3C3D3E3F
4041424344454647 48494A4B4C4D4E4F
0000000000000000 0000000000000000

V:
42

B [0]:
2021222324252627
b [0,2]:
28292A2B2C2D2E2F
b [0,3]:
```

```

3031323334353637
...
b [42,5]:
E05992B0B24B39E0
b [42,6]:
2EA496368E0841CC
b [42,7]:
1E3FA44556A3048C
CIPHERTEXT [1]:
2D09A7C18E6A5A08 16331EC27CEA5969

CIPHERTEXT [2]:
03F77EC8D63F3BDB 73299DE7FD9F4558

CIPHERTEXT [3]:
E05992B0B24B39E0 2EA496368E0841CC

CIPHERTEXT [4]:
1E3FA44556A3048C 5A6E9E335717D17D

CIPHERTEXT:
2D09A7C18E6A5A0816331EC27CEA5969
03F77EC8D63F3BDB73299DE7FD9F4558
E05992B0B24B39E02EA496368E0841CC
1E3FA44556A3048C5A6E9E335717D17D

```

В.11.2.2 Розшифрування без доповнення

```

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

CIPHERTEXT (N = 384):
2D09A7C18E6A5A0816331EC27CEA5969
03F77EC8D63F3BDB73299DE7FD9F4558
E05992B0B24B39E02EA496368E0841CC
1E3FA44556A3048C5A6E9E335717D17D

V:
42

B [42]:
2D09A7C18E6A5A08
b [42,2]:
16331EC27CEA5969
b [42,3]:
03F77EC8D63F3BDB
...
b [1,5]:
48494A4B4C4D4E4F
b [1,6]:
0000000000000000
b [1,7]:
0000000000000000
PLAINTEXT [1]:
2021222324252627 28292A2B2C2D2E2F

PLAINTEXT [2]:
3031323334353637 38393A3B3C3D3E3F

PLAINTEXT [3]:
4041424344454647 48494A4B4C4D4E4F

PLAINTEXT [4]:
0000000000000000 0000000000000000

```

PLAINTEXT:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F

В.11.2.3 Зашифрування із доповненням

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

PLAINTEXT (N = 314):

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464

padding:

2021222324252627 28292A2B2C2D2E2F
3031323334353637 38393A3B3C3D3E3F
404142434445464E 8040000000000020
0000000000000000 0000000000000000

CIPHERTEXT:

37E3EECB91150C6FA04CFD19D6FC57B7
168C9FA5C5ED18601C68EE4AFD7301F8
C8C51D7A0A5CD34F6FAB0D8AF11845CC
1E4B16E0489FDA1D76BA4EFCFD161F76

В.11.2.4 Розшифрування із доповненням

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

CIPHERTEXT (N = 314):

37E3EECB91150C6FA04CFD19D6FC57B7
168C9FA5C5ED18601C68EE4AFD7301F8
C8C51D7A0A5CD34F6FAB0D8AF11845CC
1E4B16E0489FDA1D76BA4EFCFD161F76

PLAINTEXT:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464E8040000000000020

unpadding:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464E8040000000000000

PLAINTEXT:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464

В.11.3 Перетворення Калина-256/256-KW та Калина-256/256-KW-p

В.11.3.1 Зашифрування без доповнення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

PLAINTEXT (N = 768):

202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F
 404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F

padded:

202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F
 404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F
 00000000000000000000000000000000
 00000000000000000000000000000000

V:

42

B [0]:

2021222324252627 28292A2B2C2D2E2F

b [0,2]:

303132333435363738393A3B3C3D3E3F

b [0,3]:

404142434445464748494A4B4C4D4E4F

...

b [42,5]:

199CA4F878E4723B 7171DD4D1E8DF59C

b [42,6]:

0F25FA0C20946BA6 4F9037D724BB1D50

b [42,7]:

B6C2BD9788B2AF83 EF6163087CD2D448

CIPHERTEXT [1]:

BE59D3C3C31B2685 A8FA57CD000727F1
 6AF303F0D87BC2D7 ABD80DC2796BBC4C

CIPHERTEXT [2]:

DBC4E0408943AF4D AF7DE9084DC81BFE
 F15FDCDD0DF39998 3DF69BF730D7AE2A

CIPHERTEXT [3]:

199CA4F878E4723B 7171DD4D1E8DF59C
 0F25FA0C20946BA6 4F9037D724BB1D50

CIPHERTEXT [4]:

B6C2BD9788B2AF83 EF6163087CD2D448
 8BC19F3A858D813E 3A8947A529B6D65D

CIPHERTEXT:

BE59D3C3C31B2685A8FA57CD000727F1
 6AF303F0D87BC2D7ABD80DC2796BBC4C
 DBC4E0408943AF4DAF7DE9084DC81BFE

F15FDCDD0DF399983DF69BF730D7AE2A
 199CA4F878E4723B7171DD4D1E8DF59C
 0F25FA0C20946BA64F9037D724BB1D50
 B6C2BD9788B2AF83EF6163087CD2D448
 8BC19F3A858D813E3A8947A529B6D65D

В.11.3.2 Розшифрування без доповнення

KEY:

000102030405060708090A0B0C0D0E0F
 101112131415161718191A1B1C1D1E1F

CIPHERTEXT (N = 768):

BE59D3C3C31B2685A8FA57CD000727F1
 6AF303F0D87BC2D7ABD80DC2796BBC4C
 DBC4E0408943AF4DAF7DE9084DC81BFE
 F15FDCDD0DF399983DF69BF730D7AE2A
 199CA4F878E4723B7171DD4D1E8DF59C
 0F25FA0C20946BA64F9037D724BB1D50
 B6C2BD9788B2AF83EF6163087CD2D448
 8BC19F3A858D813E3A8947A529B6D65D

V:

42

B [42]:

BE59D3C3C31B2685 A8FA57CD000727F1

b [42, 2]:

6AF303F0D87BC2D7ABD80DC2796BBC4C

b [42, 3]:

DBC4E0408943AF4DAF7DE9084DC81BFE

b [1, 5]:

7071727374757677 78797A7B7C7D7E7F

b [1, 6]:

0000000000000000 0000000000000000

b [1, 7]:

0000000000000000 0000000000000000

PLAINTEXT [1]:

2021222324252627 28292A2B2C2D2E2F
 3031323334353637 38393A3B3C3D3E3F

PLAINTEXT [2]:

4041424344454647 48494A4B4C4D4E4F
 5051525354555657 58595A5B5C5D5E5F

PLAINTEXT [3]:

6061626364656667 68696A6B6C6D6E6F
 7071727374757677 78797A7B7C7D7E7F

PLAINTEXT [4]:

0000000000000000 0000000000000000
 0000000000000000 0000000000000000

PLAINTEXT:

202122232425262728292A2B2C2D2E2F
 303132333435363738393A3B3C3D3E3F
 404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F

707172737475767778797A7B7C7D7E7F

В.11.3.3 Зашифрування із доповненням

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

PLAINTEXT (N = 648):

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
70

padded:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
708802000000000000000000000000
008000000000000000000000000000
000000000000000000000000000000
000000000000000000000000000000
000000000000000000000000000000
000000000000000000000000000000

CIPHERTEXT:

CC41D643B08592F509432E3C6F4B7315
6907A53B9FFB99B157DEC708F917AEA1
E41D76475EDFB138A8B0220A152B673E
9713DE7A2791E3573FE257C3FF3C0DAA
9AD13477E52770F54CBF94D1603AED7C
A876FB7913BC359D2B89562299FA92D3
2A9C17DBE4CC21CCE097089B9FBC2455
80D6DB59F8731D864B604E654397E5F5
E7A79A6A777C75856039C8C86140D0CB
359CA3923D902D08269F8D48E7F0F085

В.11.3.4 Розшифрування із доповненням

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F

CIPHERTEXT (N = 648):

CC41D643B08592F509432E3C6F4B7315
6907A53B9FFB99B157DEC708F917AEA1
E41D76475EDFB138A8B0220A152B673E
9713DE7A2791E3573FE257C3FF3C0DAA
9AD13477E52770F54CBF94D1603AED7C
A876FB7913BC359D2B89562299FA92D3
2A9C17DBE4CC21CCE097089B9FBC2455
80D6DB59F8731D864B604E654397E5F5
E7A79A6A777C75856039C8C86140D0CB
359CA3923D902D08269F8D48E7F0F085

PLAINTEXT:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
708802000000000000000000000000

00800000000000000000000000000000
00000000000000000000000000000000

unpadded:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
70880200000000000000000000000000
00

PLAINTEXT:

202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
70

В.11.4 Перетворення Калина-256/512-KW та Калина-256/512-KW-p

В.11.4.1 Зашифрування без доповнення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 768):

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

padded:

404142434445464748494A4B4C4D4E4F

505152535455565758595A5B5C5D5E5F

606162636465666768696A6B6C6D6E6F

707172737475767778797A7B7C7D7E7F

808182838485868788898A8B8C8D8E8F

909192939495969798999A9B9C9D9E9F

00000000000000000000000000000000

00000000000000000000000000000000

V:

42

B [0]:

4041424344454647 48494A4B4C4D4E4F

b [0,2]:

505152535455565758595A5B5C5D5E5F

b [0,3]:

606162636465666768696A6B6C6D6E6F

...

b [42,5]:
BF4F18FA9303B288 741ABD71013CF208

b [42,6]:
F31B4C76FBE342F8 9B1ABFD97E830457

b [42,7]:
555651B74D3CCDBF 94CC5E5EEC228215

CIPHERTEXT [1]:
599217EB2B5270EC EF0BB716D70E2512
34A2451CE04FCFBA EEA92022C581F19B

CIPHERTEXT [2]:
7C9386BB7476B4AD 721D40778F49062C
3605F1E8FAC9F3F3 AC04E46E89E1844D

CIPHERTEXT [3]:
BF4F18FA9303B288 741ABD71013CF208
F31B4C76FBE342F8 9B1ABFD97E830457

CIPHERTEXT [4]:
555651B74D3CCDBF 94CC5E5EEC228215
36A96F44C8BC4346 B0271303E67FD313

CIPHERTEXT:
599217EB2B5270ECEFE0BB716D70E2512
34A2451CE04FCFBAEEA92022C581F19B
7C9386BB7476B4AD721D40778F49062C
3605F1E8FAC9F3F3AC04E46E89E1844D
BF4F18FA9303B288741ABD71013CF208
F31B4C76FBE342F89B1ABFD97E830457
555651B74D3CCDBF94CC5E5EEC228215
36A96F44C8BC4346B0271303E67FD313

В.11.4.2 Розшифрування без доповнення

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

CIPHERTEXT (N = 768):
599217EB2B5270ECEFE0BB716D70E2512
34A2451CE04FCFBAEEA92022C581F19B
7C9386BB7476B4AD721D40778F49062C
3605F1E8FAC9F3F3AC04E46E89E1844D
BF4F18FA9303B288741ABD71013CF208
F31B4C76FBE342F89B1ABFD97E830457
555651B74D3CCDBF94CC5E5EEC228215
36A96F44C8BC4346B0271303E67FD313

V:
42

B [42]:
599217EB2B5270EC EF0BB716D70E2512

b [42,2]:
34A2451CE04FCFBAEEA92022C581F19B

b [42,3]:

```

7C9386BB7476B4AD721D40778F49062C
...
b [1,5]:
9091929394959697 98999A9B9C9D9E9F

b [1,6]:
0000000000000000 0000000000000000

b [1,7]:
0000000000000000 0000000000000000

PLAINTEXT [1]:
4041424344454647 48494A4B4C4D4E4F
5051525354555657 58595A5B5C5D5E5F

PLAINTEXT [2]:
6061626364656667 68696A6B6C6D6E6F
7071727374757677 78797A7B7C7D7E7F

PLAINTEXT [3]:
8081828384858687 88898A8B8C8D8E8F
9091929394959697 98999A9B9C9D9E9F

PLAINTEXT [4]:
0000000000000000 0000000000000000
0000000000000000 0000000000000000

PLAINTEXT:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F

```

В.11.4.3 Зашифрування із доповненням

```

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 648):
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
90
padded:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
90880200000000000000000000000000
00800000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000

CIPHERTEXT:
B92E58F53C38F7D23F1068FA98B921AC

```

```
800AD0D1947BD620700D0B6088F87D03
D6A516F54198154D0C71169C2BCF520F
3DF3DF527FC23E800E9A65158D45BB25
3A3BD0493E4822DF0DB5A366BC2F4755
1C5D477DDDE724A0B869F562223CEDB9
D4AA36C750FA864ADF938273FBC859F7
D4930F6B70C6474304AB670BA32CB0C4
1023769338A29EA1555F526CDFEB75C7
2212CD2D29F4BA49C2A62ACBE4F3272B
```

В.11.4.4 Розшифрування із доповненням

KEY:

```
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F
```

CIPHERTEXT (N = 648):

```
B92E58F53C38F7D23F1068FA98B921AC
800AD0D1947BD620700D0B6088F87D03
D6A516F54198154D0C71169C2BCF520F
3DF3DF527FC23E800E9A65158D45BB25
3A3BD0493E4822DF0DB5A366BC2F4755
1C5D477DDDE724A0B869F562223CEDB9
D4AA36C750FA864ADF938273FBC859F7
D4930F6B70C6474304AB670BA32CB0C4
1023769338A29EA1555F526CDFEB75C7
2212CD2D29F4BA49C2A62ACBE4F3272B
```

PLAINTEXT:

```
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
90880200000000000000000000000000
00800000000000000000000000000000
000000000000000000000000000000
```

unpadded:

```
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
90880200000000000000000000000000
00
```

PLAINTEXT:

```
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
90
```

В.11.5 Перетворення Калина-512/512-KW та Калина-512/512-KW-p

В.11.5.1 Зашифрування без доповнення

KEY:

```
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
```

303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 1024):

404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F
 606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F
 808182838485868788898A8B8C8D8E8F
 909192939495969798999A9B9C9D9E9F
 A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
 B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

padding:

404142434445464748494A4B4C4D4E4F
 505152535455565758595A5B5C5D5E5F

 606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F

 808182838485868788898A8B8C8D8E8F
 909192939495969798999A9B9C9D9E9F

 A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
 B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

 00000000000000000000000000000000
 00000000000000000000000000000000

 00000000000000000000000000000000
 00000000000000000000000000000000

V:

30

B [0]:

4041424344454647 48494A4B4C4D4E4F
 5051525354555657 58595A5B5C5D5E5F

b [0,2]:

606162636465666768696A6B6C6D6E6F
 707172737475767778797A7B7C7D7E7F

b [0,3]:

808182838485868788898A8B8C8D8E8F
 909192939495969798999A9B9C9D9E9F

...

b [30,2]:

6270832039FF045B CF7878E7DA9C3B4C
 F89326CA8B4D29DB 8680EEAE1B5A1846

b [30,3]:

3284713A323A69AE BF33CFC4B11283C7
 C8041FFC97668EDF 727823411C955981

b [30,4]:

6C108C11EC401643 765527860D8DA0ED
 7254792C21DB775D EB1D6971C924CC83

b [30,5]:

EB626173D8946949 43B1828ABDE8F949
 5BCEBA9AC3A4A035 92C085AA29CC9A0C

CIPHERTEXT [1]:

9618AE6065069D50 54464040F17337D5
 8EB51AE92391D74 0BDF7ABB239709C4

6270832039FF045B CF7878E7DA9C3B4C
F89326CA8B4D29DB 8680EEAE1B5A1846

CIPHERTEXT [2]:

3284713A323A69AE BF33CFC4B11283C7
C8041FFC97668EDF 727823411C955981
6C108C11EC401643 765527860D8DA0ED
7254792C21DB775D EB1D6971C924CC83

CIPHERTEXT [3]:

EB626173D8946949 43B1828ABDE8F949
5BCEBA9AC3A4A035 92C085AA29CC9A0C
65786E631A702D58 9B819C89E79EEFF2
9C4EC312C8860BB6 8F02272EA770FB8D

CIPHERTEXT:

9618AE6065069D5054464040F17337D5
8BEB51AE92391D740BDF7ABB239709C4
6270832039FF045BCF7878E7DA9C3B4C
F89326CA8B4D29DB8680EEAE1B5A1846
3284713A323A69AEBF33CFC4B11283C7
C8041FFC97668EDF727823411C955981
6C108C11EC401643765527860D8DA0ED
7254792C21DB775DEB1D6971C924CC83
EB626173D894694943B1828ABDE8F949
5BCEBA9AC3A4A03592C085AA29CC9A0C
65786E631A702D589B819C89E79EEFF2
9C4EC312C8860BB68F02272EA770FB8D

В.11.5.2 Розшифрування без доповнення

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

CIPHERTEXT (N = 1024):

9618AE6065069D5054464040F17337D5
8BEB51AE92391D740BDF7ABB239709C4
6270832039FF045BCF7878E7DA9C3B4C
F89326CA8B4D29DB8680EEAE1B5A1846
3284713A323A69AEBF33CFC4B11283C7
C8041FFC97668EDF727823411C955981
6C108C11EC401643765527860D8DA0ED
7254792C21DB775DEB1D6971C924CC83
EB626173D894694943B1828ABDE8F949
5BCEBA9AC3A4A03592C085AA29CC9A0C
65786E631A702D589B819C89E79EEFF2
9C4EC312C8860BB68F02272EA770FB8D

V:

30

B [30]:

9618AE6065069D50 54464040F17337D5
8BEB51AE92391D74 0BDF7ABB239709C4

b [30,2]:

6270832039FF045BCF7878E7DA9C3B4C
F89326CA8B4D29DB8680EEAE1B5A1846

b [30,3]:

3284713A323A69AEBF33CFC4B11283C7
C8041FFC97668EDF727823411C955981

...
b [1,3]:
A0A1A2A3A4A5A6A7 A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7 B8B9BABBBBCBDBEBF

b [1,4]:
0000000000000000 0000000000000000
0000000000000000 0000000000000000

b [1,5]:
0000000000000000 0000000000000000
0000000000000000 0000000000000000

PLAINTEXT [1]:
4041424344454647 48494A4B4C4D4E4F
5051525354555657 58595A5B5C5D5E5F
6061626364656667 68696A6B6C6D6E6F
7071727374757677 78797A7B7C7D7E7F

PLAINTEXT [2]:
8081828384858687 88898A8B8C8D8E8F
9091929394959697 98999A9B9C9D9E9F
A0A1A2A3A4A5A6A7 A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7 B8B9BABBBBCBDBEBF

PLAINTEXT [3]:
0000000000000000 0000000000000000
0000000000000000 0000000000000000
0000000000000000 0000000000000000
0000000000000000 0000000000000000

PLAINTEXT:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF

В.11.5.3 Зашифрування із доповненням

KEY:
000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

PLAINTEXT (N = 1288):
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
B0B1B2B3B4B5B6B7B8B9BABBBBCBDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0

padded:
404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F

[illegible]

CIPHERTEXT:

3A05BB41513555F171E9234D4834EDAD
16C0BAA6136197650138219C5DA406A7
03C39259E9DCCF6F2691EC691CE7414B
5D3CDA006DE6D6C62142FAAA742C5F8A
F64FCE95BE7ABA7FE5E06C3C33EE67BA
EAB196E3A71132CAE78CD605A22E34D5
3CD159217E7B692CC79FAC66BF5E08DB
C4FE274299474E176DDDF9F462AC63F4
872E9B7F16B98AA56707FEE5F2F94616C
FC6A9548ADB7DCB73664C3312139645
93F712ECCDFA7A94E3ABA7995176EA4B
7E77096A3A3FF4E4087F430B62D5DEE6
4999F235FA9EAC79896A1C2258BF1DFC
8A6AD0E5E7E06EAEA0CC2DEF62F67E
CE8D12EFF432277C40A7BF1A23440B35
33AF1E2F7AE1BBC076D12628BB4BC7B2
E4D4B4353BCEAF9A67276B3FA23CADCA
80062B95EBB2D51510FA16F97249DF9
8E7B845C9A410F24B3C8B3FE838E58D22
BC2D14F46190FC1BFBDB60C9691404F99

В.11.5.4 Розшифрування із доповненням

KEY:

000102030405060708090A0B0C0D0E0F
101112131415161718191A1B1C1D1E1F
202122232425262728292A2B2C2D2E2F
303132333435363738393A3B3C3D3E3F

CIPHERTEXT (N = 1288):

3A05BB41513555F171E9234D4834EDAD
16C0BAA6136197650138219C5DA406A7
03C39259E9DCCF6F2691EC691CE7414B
5D3CDA006DE6D6C62142FAAA742C5F8A
F64FCE95BE7ABA7FE5E06C3C33EE67BA
EAB196E3A71132CAE78CD605A22E34D5
3CD159217E7B692CC79FAC66BF5E08DB
C4FE274299474E176DDDF9F462AC63F4
872E9B7F16B98AA56707EE5F2F94616C
FC6A9548ABD7DCB73664C3312139645
93F712ECCDFA7A94E3ABA7995176EA4B
7E77096A3A3FF4E4087F430B25D5EE6
4999F235FA9EAC79896A1C2258BF1DFC
8A6AD05E7E06EAEAA0CC2DEF62F67E
C8ED12EFF432277C40A7BF1A23440B35

33AF1E2F7AE1BBC076D12628BB4BC7B2
E4D4B4353BCEAF9A67276B3FA23CADCA
80062B95EBB2D51510AFA16F97249DF9
8E7B845C9A410F24B3C8B3E838E58D22
BC2D14F46190FC1BFDB60C9691404F99

PLAINTEXT:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0080500000000000000000000000000
00000000000000000000000000000000
00800000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000

unpadded:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0080500000000000000000000000000
00000000000000000000000000000000
00

PLAINTEXT:

404142434445464748494A4B4C4D4E4F
505152535455565758595A5B5C5D5E5F
606162636465666768696A6B6C6D6E6F
707172737475767778797A7B7C7D7E7F
808182838485868788898A8B8C8D8E8F
909192939495969798999A9B9C9D9E9F
A0A1A2A3A4A5A6A7A8A9AAABACADAFAF
B0B1B2B3B4B5B6B7B8B9BABBBBCDBEBF
C0C1C2C3C4C5C6C7C8C9CACBCCCDCECF
D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF
E0

Додаток Г (довідковий)

Вимоги до реалізації алгоритму симетричного блокового перетворення

Г.1 Загальні вимоги щодо захисту від витоку побічними каналами

Ключ шифрування і ключ автентифікації криптографічного алгоритму, визначеного у цьому стандарті, всі проміжні значення, що формуються при обробці, час обробки (якщо він залежить від змісту повідомлення або значення ключа) повинні бути захищеними від загрози розголошення недовіреній стороні.

У випадку, коли довжина повідомлення (в тому числі при попередньому застосуванні алгоритмів стиснення інформації) або кількість повідомлень за одиницю часу є пов'язаною із змістом інформації, що міститься у самому повідомленні, розробник засобу криптографічного захисту інформації повинен передбачити додаткові заходи.

Пристрій, який виконує криптографічні перетворення, має бути захищений від зовнішнього впливу, що може викликати появу помилок при обробці.

Г.2 Обмеження на сумарну довжину повідомлень, що захищаються з використанням одного ключа

Загальна сумарна довжина повідомлень, які захищаються з використанням одного ключа, має обмеження в залежності від розміру блоку базового перетворення. Відповідно до умови використання рекомендованих параметрів режимів роботи, ці обмеження наведені у табл. Г.1.

У разі, коли сумарна довжина повідомлень при практичній експлуатації засобів криптографічного захисту інформації для довжини блоку $l = 128$ бітів потенційно може перевищити вказані обмеження, застосовується більший розмір блоку ($l = 256$ або $l = 512$).

Таблиця Г.1

Обмеження на кількість блоків, що захищаються на одному ключі			
Позначення режиму	Розмір блоку (l)		
	128	256	512
<i>CTR, CFB, CBC, OFB, XTS</i>	2^{60} (16 млн ТБ)	2^{124}	2^{251}
<i>CMAC, CCM, GCM, GMAC, KW</i>	2^{46} (64 ТБ)	2^{109}	2^{237}

Г.3 Вимоги щодо синхропосилки

При застосуванні режимів, що вимагають синхропосилку, повинні бути забезпечені її унікальні (неповторні) значення для всіх повідомлень, що захищені на одному ключі.

Якщо деякий режим накладає додаткові вимоги до синхропосилки, вони наведені в описі відповідного режиму.

Вимоги щодо конфіденційності синхропосилки не висуваються.

Режим захисту ключових даних (KW) не використовує синхропосилку. Розробник криптографічного засобу захисту інформації повинен передбачити механізм зміни ключа шифрування кожен раз, коли те ж саме повідомлення повинне бути захищене повторно.

Г.4 Захист від повторного прийому повідомлення

Режими, які забезпечують цілісність повідомлення, не виконують аналізу щодо того, чи є перевірка цілісності повторною для того ж самого повідомлення. У разі, коли кожне повідомлення, чия цілісність забезпечується алгоритмом симетричного блокового перетворення, повинне бути прийняте системою як цілісне лише один раз, розробник криптографічного засобу захисту інформації зобов'язаний застосувати додаткові механізми безпеки.

Код УКНД 35.040.
класифікація угруповання (згідно з ДК 004)

Ключові слова: інформаційна технологія, криптографічний захист інформації, алгоритм симетричного блокового перетворення, блоковий шифр, режим роботи блокового шифра, шифрування, конфіденційність, цілісність, код автентифікації повідомлення, імітовставка, імітозахист.

Генеральний директор приватного
акціонерного товариства „Інститут
інформаційних технологій”

(підпис)

С.Ю. Сінаюк

Головний конструктор приватного
акціонерного товариства „Інститут
інформаційних технологій”

(підпис)

І.Д. Горбенко

Начальник відділу наукових
досліджень приватного
акціонерного товариства „Інститут
інформаційних технологій”

(підпис)

Р.В. Олійников