Зміст (І)

- Основні алгоритми симетричного блокового шифрування, що використовуються в Україні станом на 2015 р., та їхні властивості
- Заміни ГОСТ 28147-89 у країнах СНД
- Основні компоненти національного стандарту України ДСТУ 7624:2014
- Блоковий шифр «Калина»: вимоги, конструкція, огляд властивостей компонентів
- Криптографічна стійкість алгоритму «Калина»
- Порівняння швидкодії блокового шифра “Калина” із іншими алгоритмами

24. Калина (ДСТУ 7624-2014)

Національний стандарт України ДСТУ 7624:2014

- симетричний блоковий шифр “Калина” (декілька варіантів розміру блоку і довжини ключа)
- режими роботи блокового шифру
- додаток: нелінійні таблиці заміни (S-блоки)
- додаток: алгоритм доповнення повідомлення для режимів роботи, що вимагають довжину, кратну розміру блоку
- додаток: приклади для перевірки, включаючи повідомлення із довжиною, не кратною розміру блоку і байту
- додаток: вимоги до реалізації

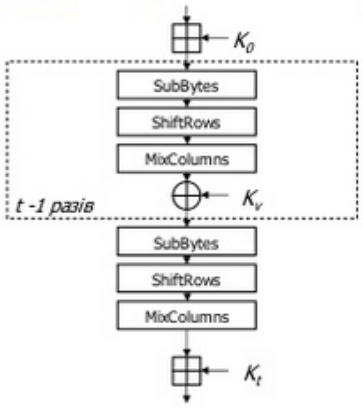
Вимоги до блокового шифру «Калина»

- високий рівень криптографічної стійкості із достатнім запасом на випадок появи нових атак протягом тривалого часу
- висока швидкодія програмної реалізації на сучасних та перспективних платформах
- компактність програмної і програмно-апаратної реалізації, можливість ефективної інтеграції декількох алгоритмів в одному засобі криптографічного захисту
- прозорість проектування, консервативний підхід щодо забезпечення стійкості
- вища (або порівняна) ефективність щодо найкращих світових рішень

Комбінації довжини ключа і розміру блоку шифру „Калина”

Розмір блоку	Довжина ключа
128	128, 256
256	256, 512
512	512

“Калина”: функція зашифрування



$$T_{l,k}^{(K)} = \eta_l^{(K_t)} \circ \psi_l \circ \tau_l \circ \pi_l' \circ$$
$$\circ \left(\prod_{r=1}^{t-1} \left(\kappa_l^{(K_r)} \circ \psi_l \circ \tau_l \circ \pi_l' \right) \right) \circ \eta_l^{(K_0)}$$

Ефективна програмна реалізація перетворення використовує один таблиць передобчислень (AES потребує два набору), виконавши оптимізацію для зашифрування, що дозволяє досягти вищої швидкодії як при зашифруванні, так і розшифруванні для більшості режимів (CTR, CFB, CMAC, OFB, GCM, GMAC, CCM).

“Калина”: кількість циклів шифрування

Блок \ Ключ	128 ($N_k = 2$)	256 ($N_k = 4$)	512 ($N_k = 8$)
128 ($N_b = 2$)	10	14	–
256 ($N_b = 4$)	–	14	18
512 ($N_b = 8$)	–	–	18

Блоковий шифр “Калина”: циклове перетворення

- чотири різних S-блоки із різних класів еквівалентності, із алгебраїчними властивостями, кращими ніж у AES, та нелінійністю вищою, ніж у СТБ 34.101.31-2011 та “Стрибог”/”Кузнечик” (**найкраще відоме у світі співвідношення** для захисту від різних атак)
  - можливість використання у якості довгосторокового ключа для спеціальних застосувань блокового перетворення
- один набір таблиць передобчислень, оптимізований для швидкодіючої реалізації як зашифрування, так і формування циклових ключів (для зашифрування і розшифрування більшість режимів роботи алгоритму вимагають виключно зашифрування режиму простої заміни, ECB)
- ефективність реалізації систем криптографічного захисту: основні елементи спільні для національних стандартів ґешування і шифрування (блокового перетворення)

Функція зашифрування алгоритму “Калина”

- прозора конструкція, консервативний підхід до проектування, використання відомої стратегії “широкого сліду” (wide trail design strategy), посилення попереднім та прикінцевим модульним (2^{64}) забілюванням
- наявність запасу стійкості на випадок появи нових атак протягом тривалого часу
- новий набір S блоків, які не можуть бути описані перевизначеною системою 2 го степеня (додатковий захист від алгебраїчних атак)
- орієнтація на 64 бітові платформи (додавання за модулем 2^{64}, МДВ матриця розміром 8x8)
- у більшості режимів роботи як для зашифрування, так і розшифрування повідомлень використовується лише пряме перетворення
- ефективна програмна і програмно апаратна реалізація

Вимоги до схеми формування циклових ключів алгоритму “Калина”

- нелінійна залежність кожного біта кожного циклового ключа від кожного біта ключа шифрування
- циклові ключі суттєво відрізняються і мають складну нелінійну залежність
- захист від відомих криптоаналітичних атак, що орієнтовані на схему розгортання ключів
- відсутність слабких ключів, при яких погіршуються криптографічні властивості або знижується стійкість перетворення
- висока обчислювальна складність відновлення ключа шифрування по одному або декільком цикловим ключам, що є доступними для криптоаналитика (додатковий захист від атак на реалізацію)
- обчислювальна складність формування всіх циклових ключів не перевищує складності зашифрування 2,5 блоків
- можливість формування циклових ключів у довільному порядку (однакова обчислювальна і просторова складність для зашифрування і розшифрування)
- простота програмної і програмно-апаратної реалізації

Криптографічна стійкість блокового шифру “Калина”, блок 128 бітів

Метод криптоаналізу	Найменша кількість циклів, для якої шифр є стійким	Показники атак		
		Макс. кілкість циклів	Обчисл. складність, екв. оп. шифрув.	Пам’ять, байтів
Диференційний	5	4	2^{55}	
Лінійний	5	3	$2^{52,8}$	
Усіч. диференц.	4	3		
Інтегральний	6	5	2^{97}	2^{33+4}
Нездійсн. дифер.	6	5	2^{62}	2^{66}
Бумеранг	5	4	2^{120}	

Криптографічна стійкість блокового шифру “Калина”, блок 256 бітів

Метод криптоаналізу	Найменша кількість циклів, для якої шифр є стійким	Показники атак		
		Макс. кілкість циклів	Обчисл. складність, екв. оп. шифрув.	Пам’ять, байтів
Диференційний	7	6	2^{230}	
Лінійний	7	5	$2^{220,8}$	
Усіч. диференц.	4	3		
Інтегральний	7	6	2^{145}	2^{64+5}
Нездійсн. дифер.	6	5	2^{61}	2^{66}
Бумеранг	6	5	2^{220}	

Криптографічна стійкість блокового шифру “Калина”, блок 512 бітів

Метод криптоаналізу	Найменша кількість циклів, для якої шифр є стійким	Показники атак		
		Макс. кілкість циклів	Обчисл. складність, екв. оп. шифрув.	Пам’ять, байтів
Диференційний	9	8	2^{490}	
Лінійний	9	7	$2^{470,4}$	
Усіч. диференц.	4	3		
Інтегральний	7	6	2^{137}	2^{64+5}
Нездійсн. дифер.	6	5	2^{260}	2^{66}
Бумеранг	7	6	2^{340}	

Криптографічна стійкість блокового шифру “Калина”

Стійкість забезпечується (наявність запасу):

- 128-битовий блок: 6 раундів (із 10 або 14, залежно від довжини ключа)
- 256-битовий блок: 7 раундів (із 14 або 18, залежно від довжини ключа)
- 512-битовий блок: 9 раундів (із 18)

Новий національний стандарт симетричного блокового перетворення забезпечує

- високий і надвисокий рівень стійкості із запасом на випадок появи нових атак та вдосконалення криптоаналітичних комплексів протягом тривалого часу
- високу швидкодію програмної реалізації на сучасних та перспективних платформах
- вищу або порівняну ефективність щодо найкращих світових рішень
- наявність режимів роботи, необхідних для ефективної реалізації сучасних засобів криптографічного захисту
- можливість ефективної інтеграції двох національних алгоритмів в одному засобі криптографічного захисту
- зручність реалізації для розробників засобів криптографічного захисту