


# Національний стандарт України ДСТУ 7624:2014 (шифр «Калина»)

A series of horizontal lines of varying lengths and colors (teal, light blue, white) extending from the left edge of the slide towards the right, positioned below the title.

# Симетричні криптоалгоритми, що використовуються в Україні

- ДСТУ ГОСТ 28147:2009;
- AES (у складі операційних систем загального призначення);
- RC4 та ін. (іноземні реалізації засобів захисту Web-з'єднань відповідно до протоколів SSL/TLS);
- Triple DES (Національний банк України, іноземні реалізації засобів захисту мережевого трафіка IPsec).

# ДСТУ ГОСТ 28147:2009

- Переваги:

- відомий шифр, який добре досліджений міжнародною спільнотою більш ніж 20 років;
- прийнятний рівень швидкодій (32-бітові платформи), достатньо зручний для апаратної реалізації, в т.ч. для малоресурсної (lightweight) криптографії;
- вузли заміни (S-блоки) із гарними властивостями забезпечують практичну стійкість шифра;

# ДСТУ ГОСТ 28147:2009

- Недоліки:

- наявність теоретичних атак із складністю, значно меншою повного перебору ключів;
- великі класи слабких ключів;
- використання вузлів заміни спеціального виду дозволяє зменшити рівень стійкості до реалізації практичних атак (виключно на основі шифртекстів) з використанням одного персонального комп'ютера;
- швидкодія на сучасних системах суттєво нижча порівняно із іншими блоковими шифрами.

# Triple DES

- Переваги

- відомий шифр, який добре досліджений міжнародною спільнотою більш ніж 30 років;
- забезпечує припустиму практичну стійкість ( $2^{112}$ );
- поширений у банківських системах, що імпортовані або орієнтовані на застарілі стандарти.

- Недоліки

- практична стійкість значно нижче теоретичної;
- наявність класів слабких ключів;
- швидкодія на сучасних системах суттєво нижча навіть порівняно із ДСТУ ГОСТ 2814:2009 і іншими блоковими шифрами.

# Заміна ГОСТ 28147-89 в інших країнах

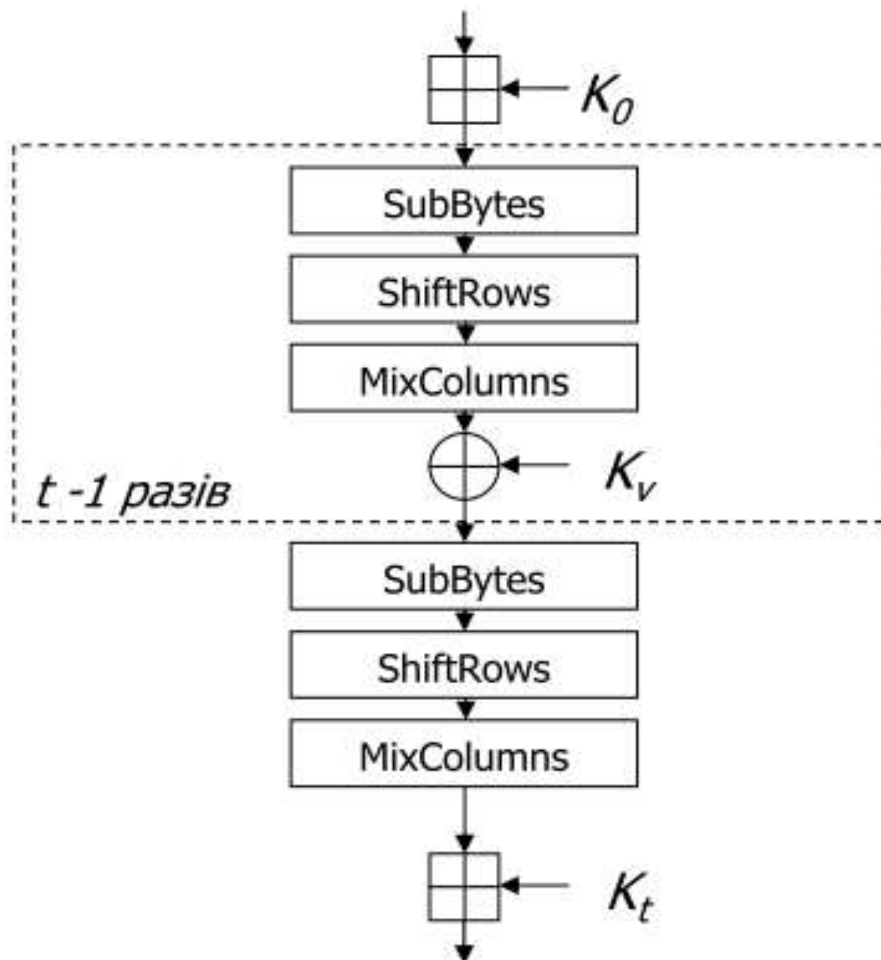
- СТБ 34.101.31-2011 (Білорусь)
  - блок 128 біт, ключ 128, 192 або 256 біт;
  - 8 циклів, які складаються з комбінації ланцюга Фейстеля та схеми Лая-Мессі;
  - один S-блок (8-біт-в-8) із гарними властивостями;
  - відсутність схеми розгортання ключів;
  - невідомі практичні атаки, ефективніші повного перебору;
  - швидший ніж ГОСТ 28147-89, але повільніший, ніж AES.
- “Кузнечик” (“Коник”, РФ)
  - блок 128 біт, ключ 256 біт;
  - 9 циклів AES-подібного перетворення;
  - один S-блок (8-біт-в-8), нециркулянтна матриця лінійного перетворення:  $16 \times 16$  над полем  $GF(2^8)$
  - схема розгортання ключів на базі циклового перетворення і ланцюга Фейстеля (конструкція CS-cipher);
  - однаковий S-блок із новою функцією ґешування “Стрибог” (ГОСТ Р 34.11-2012), але різні матриці лінійного перетворення (ускладнена реалізація систем криптографічного захисту);
  - великий розмір таблиць для оптимальної програмної реалізації ;
  - швидкодія нижча за AES.

# Основні параметри алгоритму

- Архітектура: Substitution-Permutation network (SP-мережа);
- Вхідний блок: 128/256/512 бітів; за цикл обробляється цілий блок;
- Довжина ключа: 128/256/512 бітів.
- К-сть раундів: 10/14/18 (залежить від довжин вхідного блоку та ключа):

$N_r$	$N_b = 2$ (128 бітів)	$N_b = 4$ (256 бітів)	$N_b = 8$ (512 бітів)
$N_k = 2$ (128 бітів)	10	14	-
$N_k = 4$ (256 бітів)	-	14	18
$N_k = 8$ (512 бітів)	-	-	18

# Блок-схема алгоритму



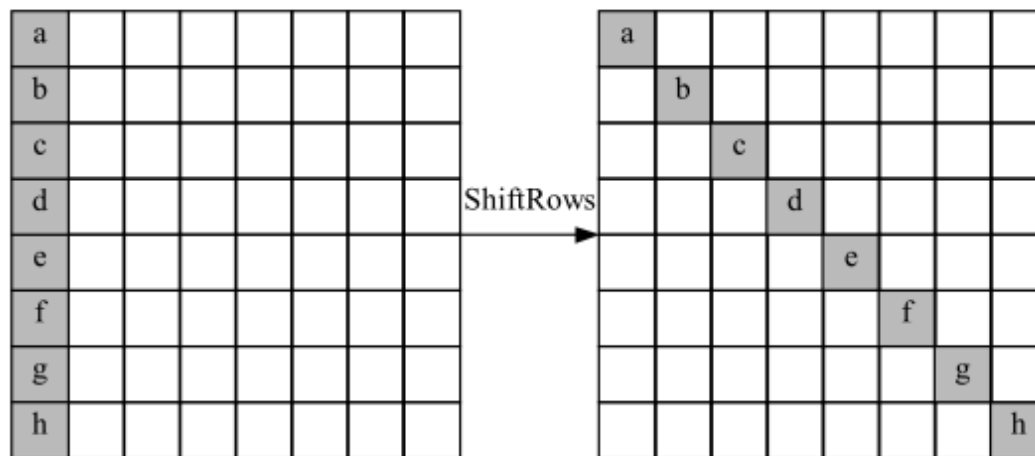
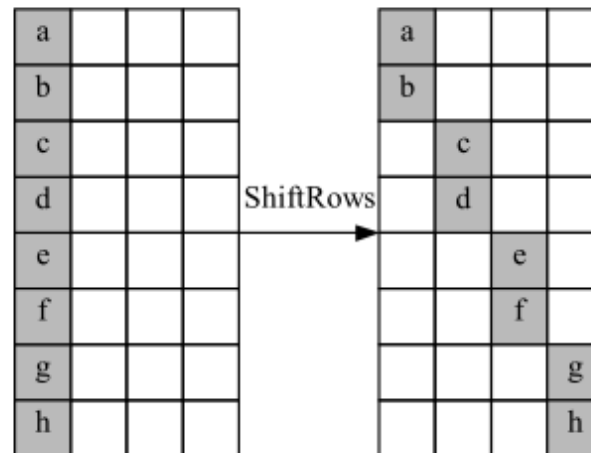
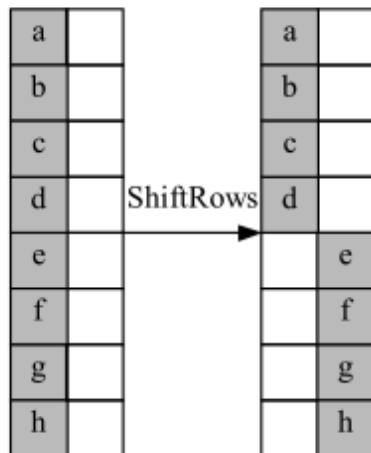
Всі операції виконуються над 64-бітовим станом.

Процедури відповідають таким в AES.

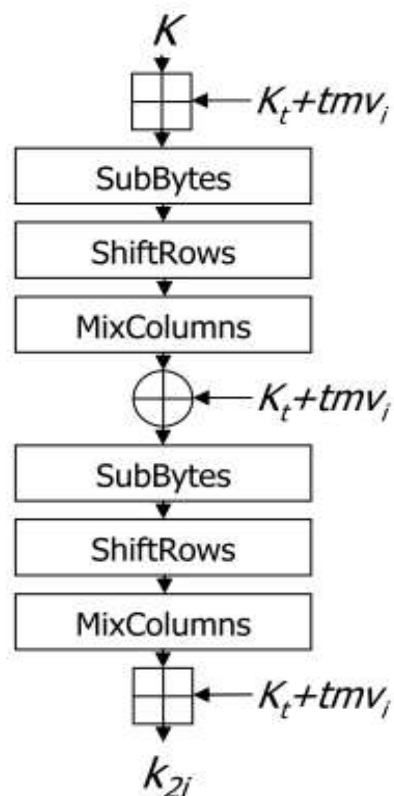
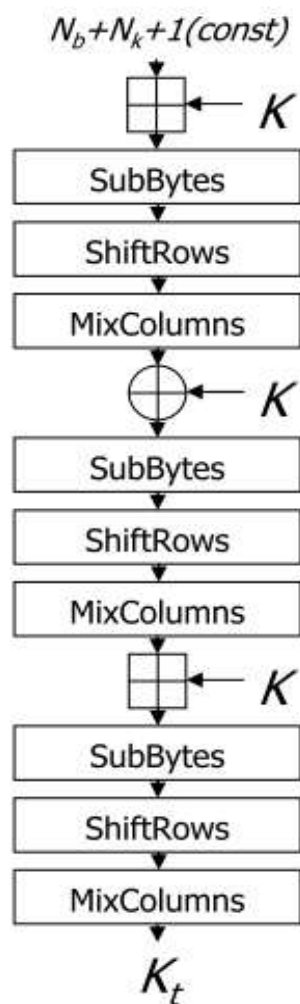
1. Процедура SubBytes використовує 8 таблиць заміни, побудованих випадковим чином.
2. Інший зсув рядків.
3. Використовується додавання за модулем 2 та за модулем  $2^{32}$ .
4. Процедура MixColumns використовує інші матриці для множення, побудовані на інших незвідних поліномах.
5. Інша процедура розгортання ключа.



# Зсув рядків



# Процедура розгортання ключа



$$k_{2i+1} = k_{2i} \lll (2 \cdot N_b + 3)$$

Ліворуч – операція розгортання ключів з непарними індексами;  
Праворуч – для ключів з парними індексами.  
Операції ті ж, що виконуються під час шифрування.

# Оцінка криптографічної стійкості (128-бітовий блок)

Метод криптоаналізу	Найменша кількість циклів, для якої шифр є стійким	Показники атак		
		Макс. кількість 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	$2^{120}$	

# Оцінка криптографічної стійкості (256-бітовий блок)

Метод криптоаналізу	Найменша кількість циклів, для якої шифр є стійким	Показники атак		
		Макс. кількість 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	$2^{220}$	

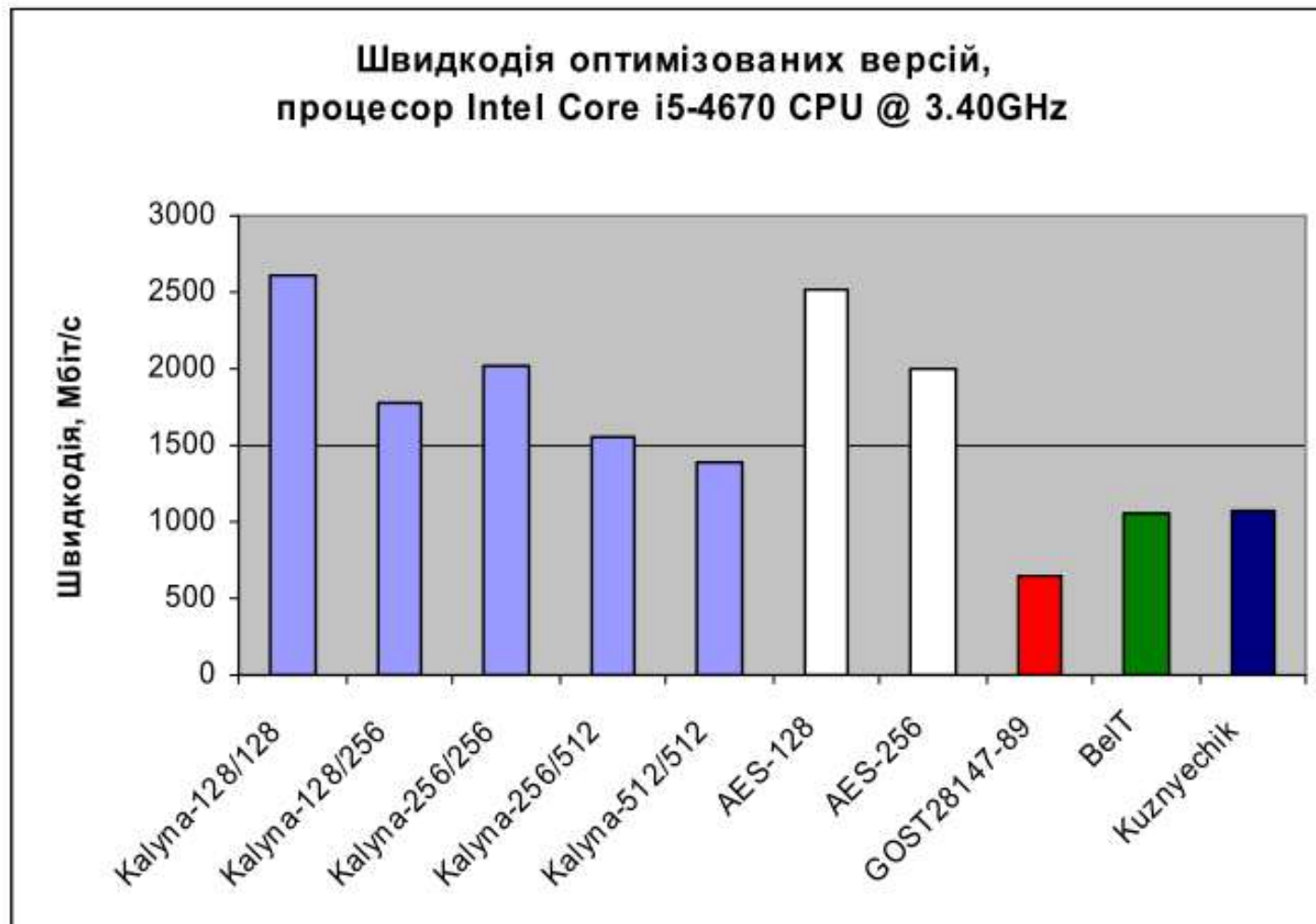
# Оцінка криптографічної стійкості (512-бітовий блок)

Метод криптоаналізу	Найменша кількість циклів, для якої шифр є стійким	Показники атак		
		Макс. кількість 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	$2^{60}$	$2^{66}$
Бумеранг	7	6	$2^{340}$	

# Запас криптостійкості

- 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).

# Порівняння швидкодії



# ВИСНОВКИ

Алгоритм «Калина» демонструє:

- 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 різних 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.



# Автори шифру «Калина»

- Р.В.Олійников; І.Д.Горбенко; О.В.Казимиров;
- В.І.Руженцев; О.О.Кузнєцов; Ю.І.Горбенко;
- В.І.Долгов; О.В.Дирда; А.І.Пушкарьов;
- Р.І.Мордвинов; Д.С.Кайдалов