

ЛЕКЦІЯ 6

Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)



План

1. Алгоритм шифрування «Калина»

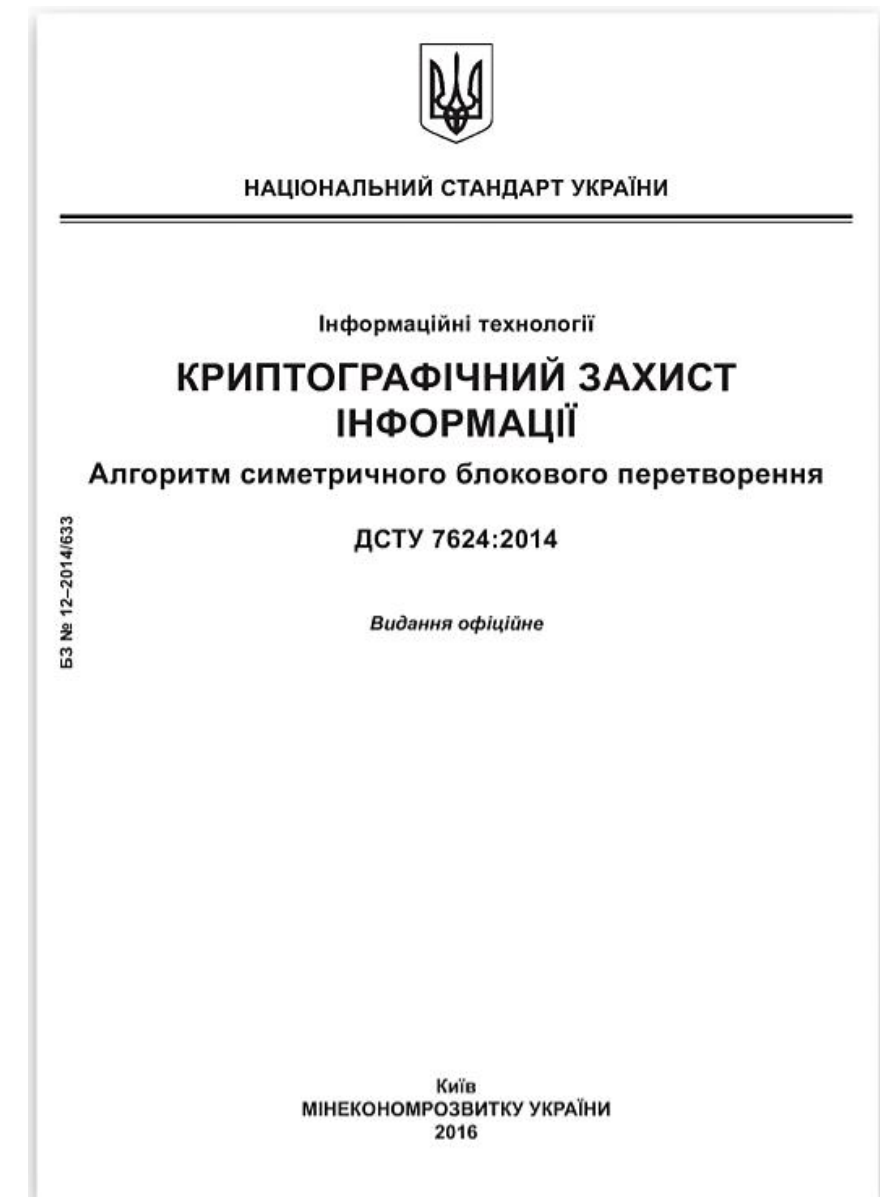
2. Режимы роботи «Калина»

3. «Калина» vs AES

1. Алгоритм шифрування «Калина»

«**Калина**» – блоковий симетричний шифр, описаний у національному стандарті України **ДСТУ 7624:2014** (введений в дію з 1 липня 2015 р.).

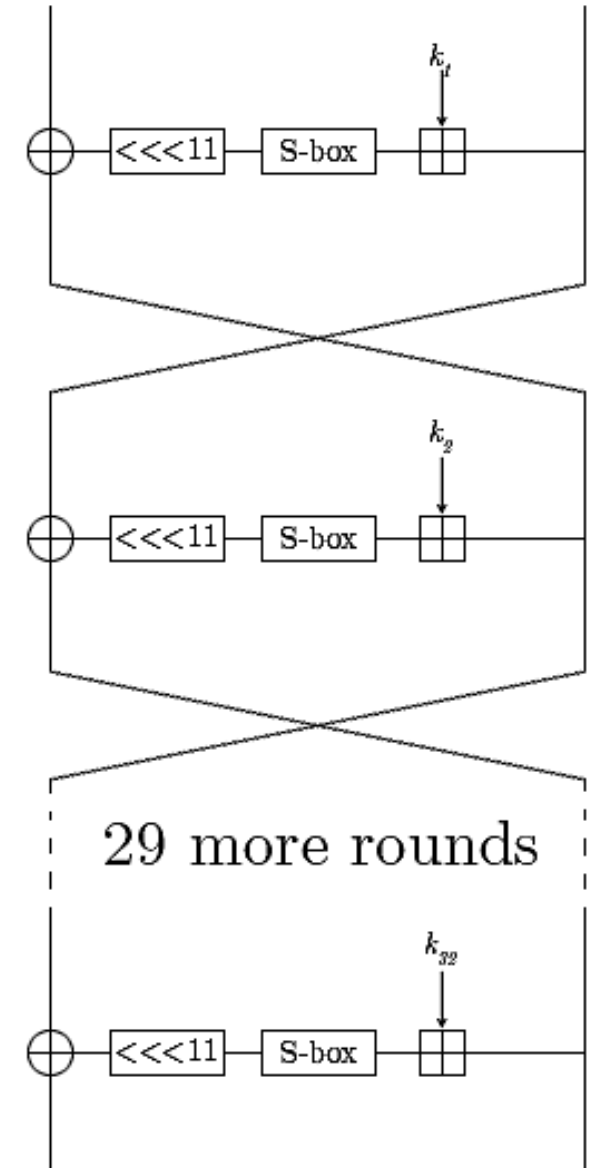
Стандарт розроблено у співпраці **Держспецзв'язку**, ПАТ «**Інститут інформаційних технологій**» та провідних українських науковців на чолі із Горбенком І. Д.



1. Алгоритм шифрування «Калина»

Раніше в Україні діяв **ДСТУ ГОСТ 28147:2009** (перевиданий ГОСТ 28147-89 – радянський і російський стандарт шифрування).

Цей стандарт вже також виведений із дії в Білорусі та видозмінений у РФ.



1. Алгоритм шифрування «Калина»

Основні характеристики

- 1) Спроектований на основі SP-мережі (AES);
- 2) Забезпечує захист від відомих методів криптоаналізу;
- 3) Має високу швидкодію на сучасних і перспективних програмних та програмно-апаратних платформах;
- 4) Визначає 10 режимів роботи.

1. Алгоритм шифрування «Калина»

Розмір блоку 128, 256 або
512 бітів

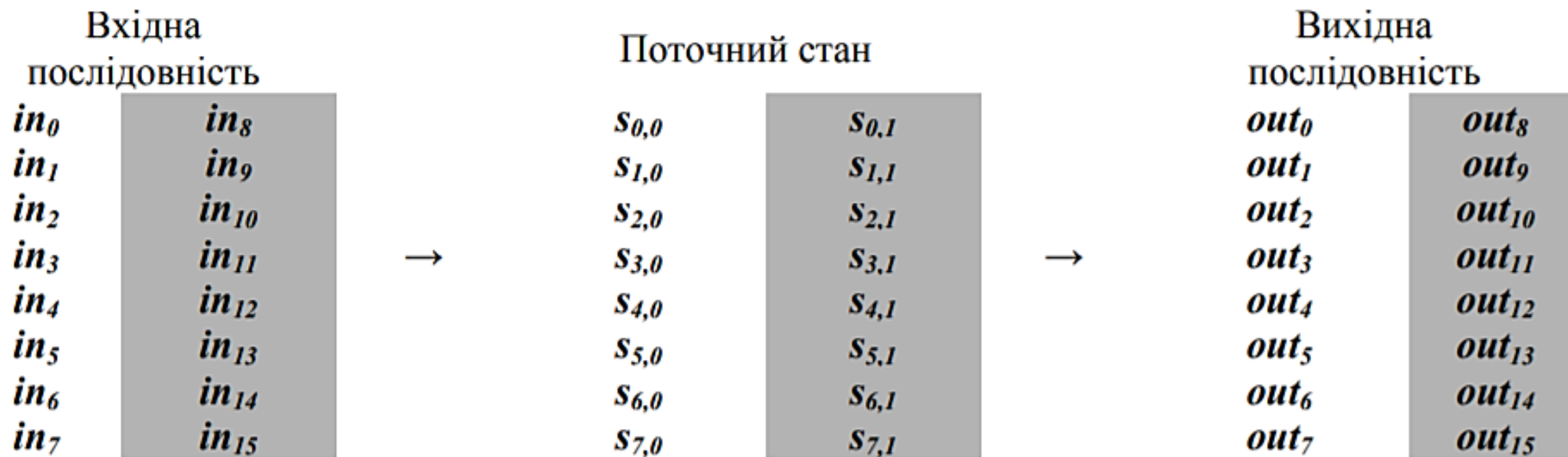
Матриця стану має 8 рядків
та Nb стовпців байтів ($64 \times$
 Nb біт), що являють собою
елементи поля $GF(2^8)$

Матриця стану при $Nb = 2$:

$$\begin{pmatrix} S_{0,0} & S_{0,1} \\ S_{1,0} & S_{1,1} \\ S_{2,0} & S_{2,1} \\ S_{3,0} & S_{3,1} \\ S_{4,0} & S_{4,1} \\ S_{5,0} & S_{5,1} \\ S_{6,0} & S_{6,1} \\ S_{7,0} & S_{7,1} \end{pmatrix}$$

1. Алгоритм шифрування «Калина»

Заповнення матриці стану (128 біт)



1. Алгоритм шифрування «Калина»

Довжина ключа може бути
128, 256 або 512 бітів

Ключ: матриця байтів, яка
має 8 рядків Nk стовпців

Розмір блока і довжина ключа
використовуються у
позначенні шифру як
параметр. Наприклад, Калина-
128/256

Матриця ключа при $Nk = 4$:

$$\begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \\ k_{4,0} & k_{4,1} & k_{4,2} & k_{4,3} \\ k_{5,0} & k_{5,1} & k_{5,2} & k_{5,3} \\ k_{6,0} & k_{6,1} & k_{6,2} & k_{6,3} \\ k_{7,0} & k_{7,1} & k_{7,2} & k_{7,3} \end{pmatrix}$$

1. Алгоритм шифрування «Калина»

Кількість раундів шифрування алгоритму «Калина»

Розмір блоку	Кількість раундів шифрування для різних довжин ключа		
	Довжина ключа 128 бітів ($Nk = 2$)	Довжина ключа 256 бітів ($Nk = 4$)	Довжина ключа 512 бітів ($Nk = 8$)
128 ($Nb = 2$)	10	14	–
256 ($Nb = 4$)	–	14	18
512 ($Nb = 8$)	–	–	18

Довжина ключа **збігається** з розміром блоку або **удвічі більша** за нього

1. Алгоритм шифрування «Калина»

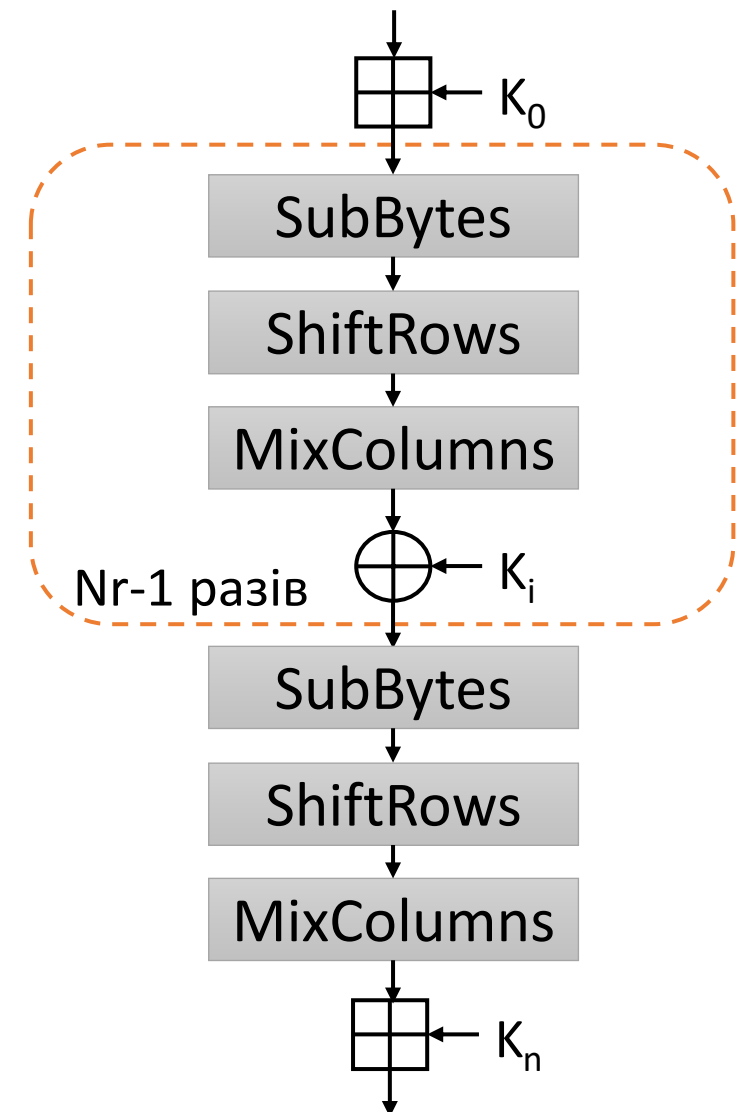
Зашифрування за алгоритмом «Калина»

I. Додавання з нульовим ключем по модулю 2^{64}

II. $Nr-1$ раундів, кожен з яких складається з чотирьох етапів:

1. Підстановка байтів;
2. Зсув рядків;
3. Перемішування стовпців;
4. Додавання раундового ключа по модулю 2

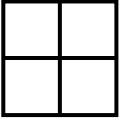
III. Завершальний раунд Nr , в якому замість \oplus виконується додавання по модулю 2^{64}



1. Алгоритм шифрування «Калина»

Додавання з нульовим підключем по модулю 2^{64}

Операція \boxplus забезпечує побітове **додавання** стовпців **раундового ключа** до відповідних стовпців матриці стану за модулем 2^{64} . При виконанні додавання менші значущі байти мають менші індекси, тобто використовується формат little endian.

$$\begin{pmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \\ S_{4,0} & S_{4,1} & S_{4,2} & S_{4,3} \\ S_{5,0} & S_{5,1} & S_{5,2} & S_{5,3} \\ S_{6,0} & S_{6,1} & S_{6,2} & S_{6,3} \\ S_{7,0} & S_{7,1} & S_{7,2} & S_{7,3} \end{pmatrix} \boxplus \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \\ k_{4,0} & k_{4,1} & k_{4,2} & k_{4,3} \\ k_{5,0} & k_{5,1} & k_{5,2} & k_{5,3} \\ k_{6,0} & k_{6,1} & k_{6,2} & k_{6,3} \\ k_{7,0} & k_{7,1} & k_{7,2} & k_{7,3} \end{pmatrix}$$


1. Алгоритм шифрування «Калина»

Приклад 1.1:

$$\begin{pmatrix} C3 & 5A \\ 1E & 21 \\ E8 & A4 \\ A8 & 35 \\ 7E & FD \\ 2C & B2 \\ ED & 5B \\ 24 & 92 \end{pmatrix} \boxplus \begin{pmatrix} 95 & B7 \\ CD & 26 \\ 56 & 53 \\ 60 & E1 \\ 91 & 71 \\ D3 & 80 \\ 27 & F3 \\ 65 & 81 \end{pmatrix} = \begin{pmatrix} 58 & 11 \\ EC & 48 \\ 3E & F7 \\ 09 & 16 \\ 10 & 6F \\ 00 & 33 \\ 15 & 4F \\ 8A & 14 \end{pmatrix}$$

$$(925BB2FD35A4215A + 81F38071E15326B7) \bmod 2^{64} = 144F336F16F74811$$

$$(24ED2C7EA8E81EC3 + 6527D3916056CD95) \bmod 2^{64} = 8A150010093EEC58$$

C31EE8A87E2CED245A21A435FDB25B92 (big endian)

925BB2FD35A4215A24ED2C7EA8E81EC3 (little endian)

95CD566091D32765B72653E17180F381 (big endian)

+

+

81F38071E15326B76527D3916056CD95 (little endian)

144F336F16F748118A150010093EEC58 (little endian)

58EC3E091000158A1148F7166F334F14 (big endian)

1. Алгоритм шифрування «Калина»

Підстановка байтів

Кожен байт матриці стану **замінюється** відповідно до заданої таблиці підстановки (загалом є **4 таблиці**)

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

1. Алгоритм шифрування «Калина»

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

Для перетворення може використовуватися й **інший** набір підстановок

1. Алгоритм шифрування «Калина»

До байтів **одного рядка** поточного стану застосовується **одна й та сама** підстановка.

$S_{0,i}$	0-рядок	π_0
$S_{1,i}$	1-рядок	π_1
$S_{2,i}$	2-рядок	π_2
$S_{3,i}$	3-рядок	π_3
$S_{4,i}$	4-рядок	π_0
$S_{5,i}$	5-рядок	π_1
$S_{6,i}$	6-рядок	π_2
$S_{7,i}$	7-рядок	π_3

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

Результат підстановки для значення **5A** – це число **66**, що знаходиться в таблиці на перетині 6-го рядка та 11 стовпця.

1. Алгоритм шифрування «Калина»


Зсув рядків

Рядки стану циклічно **зсувають праворуч** на різну кількість байтів, залежно від розміру блока

Номер рядка	Значення зсуву, байтів		
	Довжина блоку 128 бітів	Довжина блоку 256 бітів	Довжина блоку 512 бітів
0	0	0	0
1	0	0	1
2	0	1	2
3	0	1	3
4	1	2	4
5	1	2	5
6	1	3	6
7	1	3	7

1. Алгоритм шифрування «Калина»


a	
b	
c	
d	
e	
f	
g	
h	



a	
b	
c	
d	
	e
	f
	g
	h

Зсув рядків **128-**
бітового блоку


a			
b			
c			
d			
e			
f			
g			
h			



a			
b			
	c		
	d		
		e	
		f	
			g
			h

Зсув рядків **256-**
бітового блоку

a							
b							
c							
d							
e							
f							
g							
h							



a							
	b						
		c					
			d				
				e			
					f		
						g	
							h

Зсув рядків **512-**
бітового блоку

1. Алгоритм шифрування «Калина»

Перемішування стовпців

Стовпці стану розглядають як многочлен над полем $GF(2^8)$ та множать за модулем $x^8 + 1$ на фіксований многочлен $c(x)$:

$$c(x) = 01_{16} \cdot x^7 + 05_{16} \cdot x^6 + 01_{16} \cdot x^5 + 08_{16} \cdot x^4 + 06_{16} \cdot x^3 + 07_{16} \cdot x^2 + 04_{16} \cdot x + 01_{16}$$

Або у матричному вигляді:

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 01 & 01 & 05 & 01 & 08 & 06 & 07 & 04 \\ 04 & 01 & 01 & 05 & 01 & 08 & 06 & 07 \\ 07 & 04 & 01 & 01 & 05 & 01 & 08 & 06 \\ 06 & 07 & 04 & 01 & 01 & 05 & 01 & 08 \\ 08 & 06 & 07 & 04 & 01 & 01 & 05 & 01 \\ 01 & 08 & 06 & 07 & 04 & 01 & 01 & 05 \\ 05 & 01 & 08 & 06 & 07 & 04 & 01 & 01 \\ 01 & 05 & 01 & 08 & 06 & 07 & 04 & 01 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix}$$

1. Алгоритм шифрування «Калина»

Для **множення** у полі $GF(2^8)$ алгоритм «Калина» використовує нерозкладний многочлен

$$m(x) = x^8 + x^4 + x^3 + x^2 + 1$$

Наприклад, **результат множення** фіксованої матриці на один деякий стовпець матриці стану матиме вигляд:

$$\begin{pmatrix} 01 & 01 & 05 & 01 & 08 & 06 & 07 & 04 \\ 04 & 01 & 01 & 05 & 01 & 08 & 06 & 07 \\ 07 & 04 & 01 & 01 & 05 & 01 & 08 & 06 \\ 06 & 07 & 04 & 01 & 01 & 05 & 01 & 08 \\ 08 & 06 & 07 & 04 & 01 & 01 & 05 & 01 \\ 01 & 08 & 06 & 07 & 04 & 01 & 01 & 05 \\ 05 & 01 & 08 & 06 & 07 & 04 & 01 & 01 \\ 01 & 05 & 01 & 08 & 06 & 07 & 04 & 01 \end{pmatrix} \cdot \begin{pmatrix} A8 \\ 14 \\ C4 \\ 5E \\ B4 \\ 57 \\ BB \\ 1F \end{pmatrix} = \begin{pmatrix} 4D \\ A7 \\ 4F \\ 33 \\ C3 \\ 48 \\ 5F \\ 0C \end{pmatrix}$$

1. Алгоритм шифрування «Калина»

Додавання раундового ключа по модулю 2

Операція \oplus забезпечує побітове **додавання раундового ключа** до матриці стану за модулем 2.

$$\begin{pmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \\ S_{4,0} & S_{4,1} & S_{4,2} & S_{4,3} \\ S_{5,0} & S_{5,1} & S_{5,2} & S_{5,3} \\ S_{6,0} & S_{6,1} & S_{6,2} & S_{6,3} \\ S_{7,0} & S_{7,1} & S_{7,2} & S_{7,3} \end{pmatrix} \oplus \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \\ k_{4,0} & k_{4,1} & k_{4,2} & k_{4,3} \\ k_{5,0} & k_{5,1} & k_{5,2} & k_{5,3} \\ k_{6,0} & k_{6,1} & k_{6,2} & k_{6,3} \\ k_{7,0} & k_{7,1} & k_{7,2} & k_{7,3} \end{pmatrix}$$

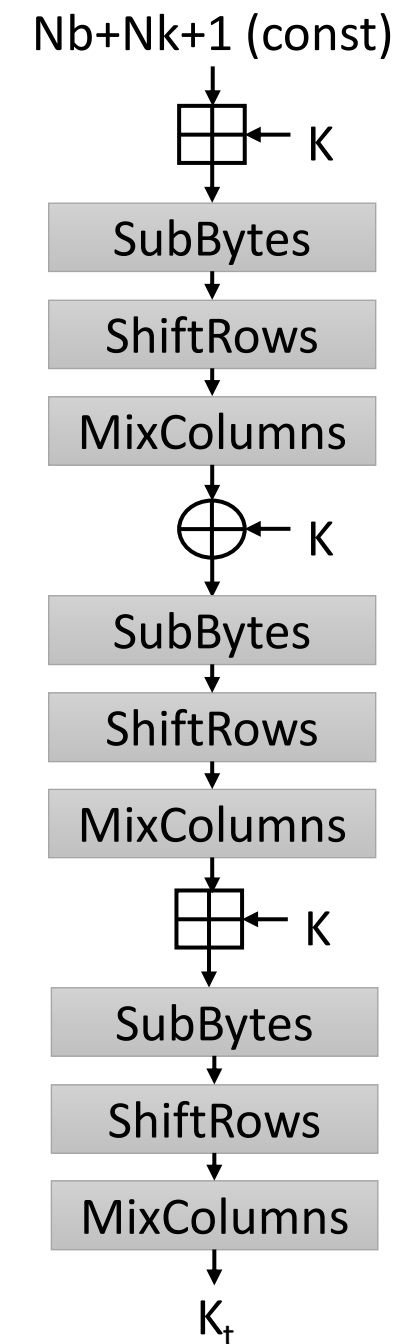
1. Алгоритм шифрування «Калина»

Розгортання ключів

1. З ключа шифрування K формується **допоміжний ключ** K_t з довжиною, що дорівнює розміру блока ($64 \times Nb$ біт) з використанням **трьох раундів зашифрування**.

Вхіднимим даними для перетворення є число $Nb + Nk + 1$ (у двійковому вигляді), інші байти заповнюються нулями.

У якості раундових ключів використовується **ключ шифрування** K (якщо ключ довше блоку, використовується його молодша і старша половини).

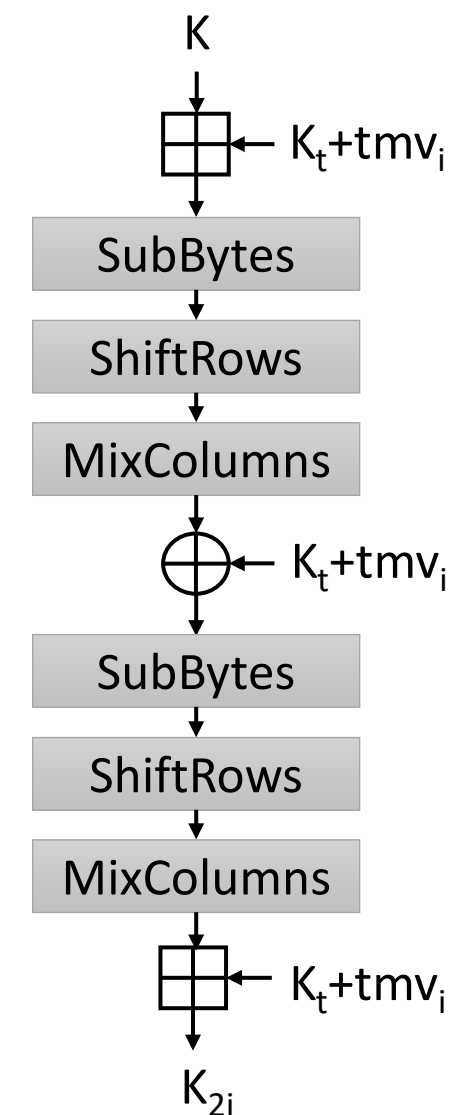


1. Алгоритм шифрування «Калина»

Розгортання ключів

2. На основі ключа K та допоміжного ключа K_t формуються **раундові ключі** K_{2i} (з **парними індексами**) довжиною, що дорівнює розміру блока ($64 \times Nb$ біт), з використанням **двох раундів зашифрування** для кожного раундового ключа.

У якості раундових ключів використовується результат додавання по модулю 2^{64} **допоміжного ключа** K_t та **змінної** tmv_i – двійкове значення, яке залежить від індексу раундового ключа, який формується.



$$tmv_0 = 0x01000100 \dots 0100$$

$$tmv_{i+2} = tmv_i \ll 1$$

1. Алгоритм шифрування «Калина»

Розгортання ключів

3. З раундових ключів K_{2i} з парними індексами формуються раундові ключі K_{2i+1} (з **непарними індексами**) шляхом **циклічного зсуву** попереднього ключа з парним індексом вліво на $2 \times Nb + 3$ байт.

<i>Розмір блоку, біт (байт)</i>	<i>Зсув вліво (байт)</i>
128(16)	7
256(32)	11
512(64)	19

Загалом використовується $Nr+1$ раундових ключів K_i ($i = 0, 1 \dots, Nr$), кожен довжиною $64 \times Nb$ біт.

1. Алгоритм шифрування «Калина»

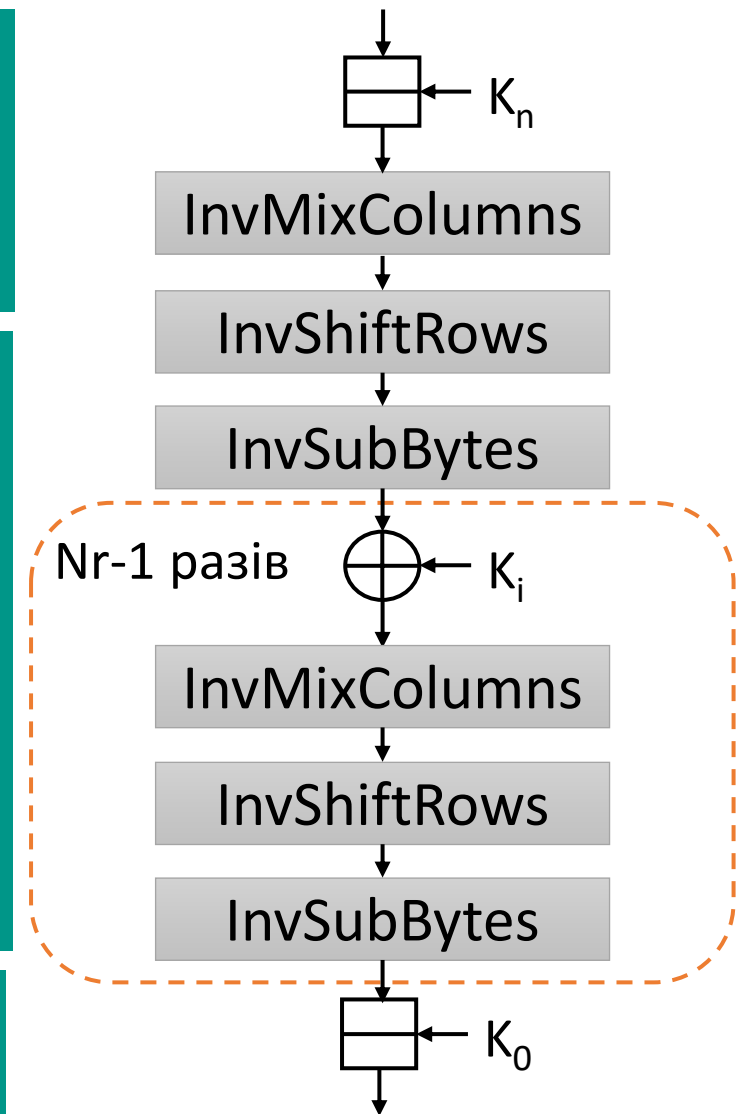
Дешифрування за алгоритмом «Калина»

I. Виконуються операції з п. II, але на початку замість \oplus виконується віднімання по модулю 2^{64} з ключем останнього раунду

II. $Nr-1$ раундів, кожен з яких складається з чотирьох етапів:

1. Додавання раундового ключа за модулем 2;
2. Зворотна операція до перемішування стовпців;
3. Зсув рядків в зворотному порядку;
4. Обернена операція до підстановки байтів.

III. Віднімання з ключем нульового раунду по модулю 2^{64}



1. Алгоритм шифрування «Калина»

Операція, зворотна операції перемішування стовпців

Стовпці стану множать на фіксований многочлен $c^{-1}(x)$ оберений до $c(x)$:

$$c^{-1}(x) = 95_{16} \cdot x^7 + 76_{16} \cdot x^6 + A8_{16} \cdot x^5 + 2F_{16} \cdot x^4 + 49_{16} \cdot x^3 + D7_{16} \cdot x^2 + CA_{16} \cdot x + AD_{16}$$

Або у матричному вигляді:

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} AD & 95 & 76 & A8 & 2F & 49 & D7 & CA \\ CA & AD & 95 & 76 & A8 & 2F & 49 & D7 \\ D7 & CA & AD & 95 & 76 & A8 & 2F & 49 \\ 49 & D7 & CA & AD & 95 & 76 & A8 & 2F \\ 2F & 49 & D7 & CA & AD & 95 & 76 & A8 \\ A8 & 2F & 49 & D7 & CA & AD & 95 & 76 \\ 76 & A8 & 2F & 49 & D7 & CA & AD & 95 \\ 95 & 76 & A8 & 2F & 49 & D7 & CA & AD \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix}$$

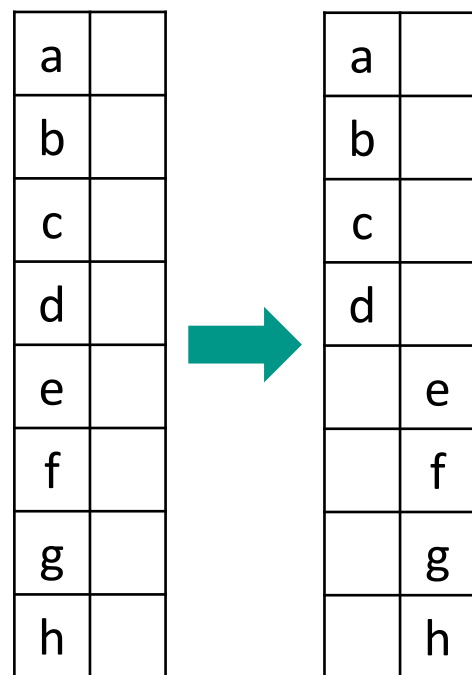
1. Алгоритм шифрування «Калина»

Зсув рядків в зворотному порядку

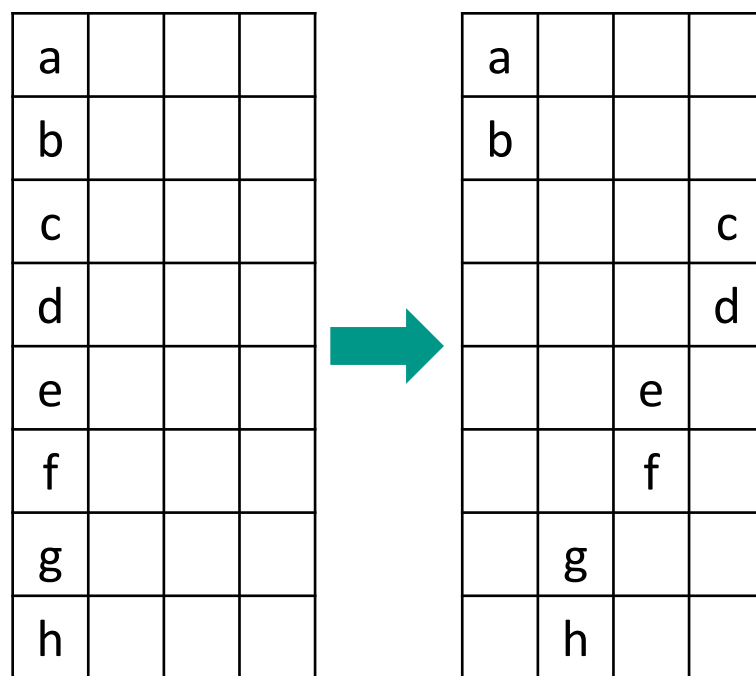
Рядки стану циклічно **зсувають ліворуч** на різну кількість байтів, залежно від розміру блока

Номер рядка	Значення зсуву, байтів		
	Довжина блоку 128 бітів	Довжина блоку 256 бітів	Довжина блоку 512 бітів
0	0	0	0
1	0	0	1
2	0	1	2
3	0	1	3
4	1	2	4
5	1	2	5
6	1	3	6
7	1	3	7

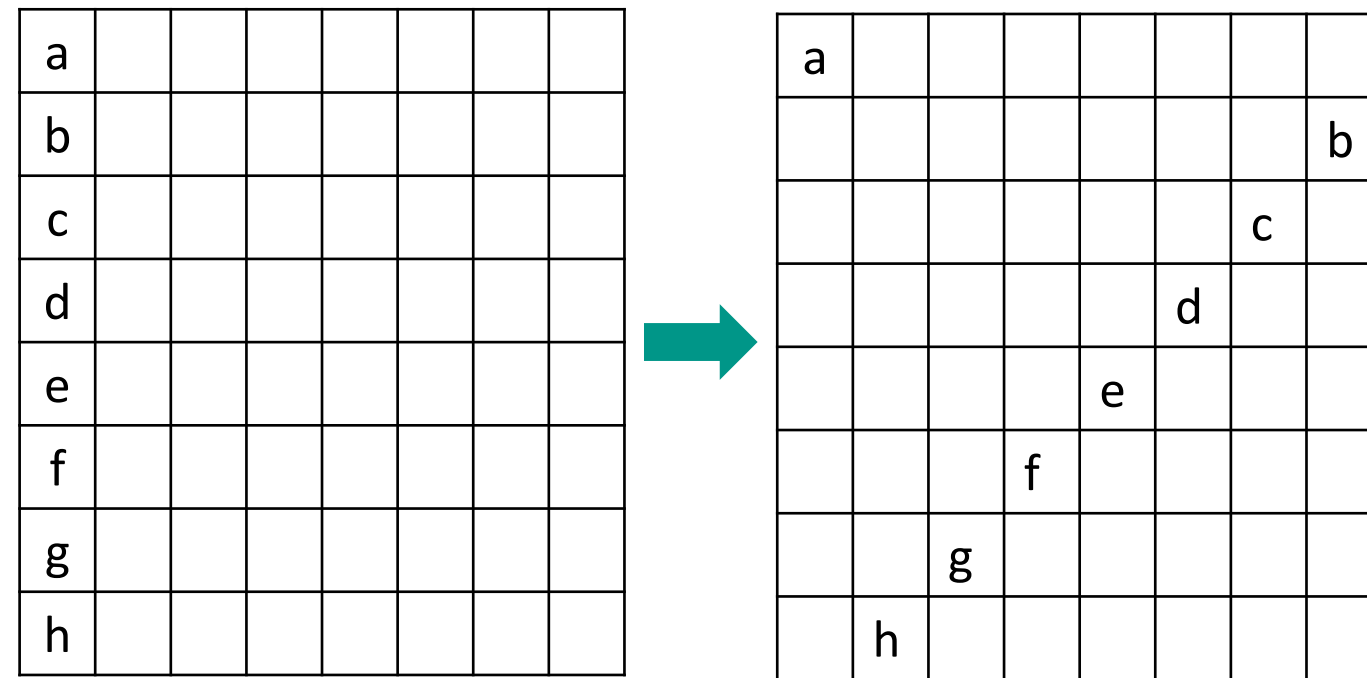
1. Алгоритм шифрування «Калина»



Зворотний зсув
рядків **128-**
бітового блоку



Зворотний зсув
рядків **256-**
бітового
блоку



Зворотний зсув
рядків **512-**
бітового
блоку

1. Алгоритм шифрування «Калина»

Обернена операція до операції підстановки байтів

Кожен байт матриці стану **замінюється** відповідно до заданої таблиці зворотної заміни

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

1. Алгоритм шифрування «Калина»

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

2. Режими роботи «Калина»

Стандарт ДСТУ 7624:2014 (Калина) визначає алгоритм симетричного блокового перетворення для забезпечення *конфіденційності* і (або) *цілісності* даних

<i>№ режиму</i>	<i>Назва режиму</i>	<i>Позначення</i>	<i>Послуга безпеки</i>
1	<i>Проста заміна (базове перетворення)</i>	ECB	Конфіденційність
2	<i>Гамування</i>	CTR	Конфіденційність
3	<i>Гамування зі зворотнім зв'язком за шифротекстом</i>	CFB	Конфіденційність
4	<i>Вироблення імітовставки</i>	CMAC	Цілісність
5	<i>Зчеплення шифроблоків</i>	CBC	Конфіденційність

2. Режими роботи «Калина»

№ режиму	Назва режиму	Позначення	Послуга безпеки
6	<i>Гамування зі зворотнім зв'язком за шифрогамою</i>	OFB	Конфіденційність
7	<i>Вибіркове гамування із прискореним виробленням імітовставки</i>	GCM, GMAC	Конфіденційність і цілісність (GCM), тільки цілісність (GMAC)
8	<i>Вироблення імітовставки і гамування</i>	CCM	Цілісність і конфіденційність
9	<i>Індексованої заміни</i>	XTS	Конфіденційність
10	<i>Захисту ключових даних</i>	KW	Конфіденційність і цілісність

3. «Калина» vs AES (заповнити самостійно)

	AES	«Калина»
Розмір ключа		
Розмір блока		
Кількість раундів		
Математичні операції		
Кількість таблиць підстановки		
Нерозкладний многочлен		
Генерація ключів (основні операції)		