УДК 681.322

Білан С.М., Шварц І.М., Щербакова І.О., Желєзняк А.Л.

ЗАСТОСУВАННЯ МОДИФІКОВАНОГО МЕТОДУ КРИПТОАНАЛІЗУ АНДЕЛЬМАНА І РІДСА ДО ПЕРЕВІРКИ НА СТІЙКІСТЬ АЛГОРИТМУ ШИФРУВАННЯ BLOWFISH

Методи захисту інформації постійно вдосконалюються з урахуванням попереднього досвіду і з використанням позитивних властивостей відомих алгоритмів. Оскільки одночасно із вдосконаленням захисту проводиться робота щодо пошуку ефективних методів злому, то всі відомі методи захисту постійно змінюються з метою підвищення надійності [1]. Саме тому перед застосуванням всі розроблені методи захисту повинні бути перевірені на стійкість до злому.

Для перевірки на стійкість застосуємо метод Андельмана і Рідса. Головна ідея методу полягає в тому, що ймовірність появи в бітових розрядах ключа "0" або "1" складає в середньому 0,5. А розподіл "0" і "1" в розрядах ключа здійснюється за законом нормального розподілу, оскільки користувач при створенні ключа, як правило, не приділяє уваги розподілу бітів "0" та "1" в розрядах ключа, тому що це – громіздка операція [2].

Тому на відміну від методів простого і ймовірнісного перебору варіантів ключів пропонується перевірка лише тих ключів, які мають однакову або майже однакову "0" і "1" в розрядах ключа. Тобто генеруватись ключі можуть методами простого чи ймовірнісного перебору варіантів ключів, а перевірятися будуть лише ті, які відповідають умові

$$\frac{|k_0 - k_1|}{k_0 + k_1} \le \Delta,$$

де k_0 – кількість "0" в розрядах ключа; k_1 – кількість "1" в розрядах ключа; Δ - процентне відхилення від паритетного (50% на 50%) співвідношення "0" і "1" в розрядах ключа.

Для тестового прикладу складено програму в середовищі Delphi, що реалізує модифікований метод криптоаналізу Андельмана і Рідса.

Програма дозволяє вводити довжину ключа і отримувати знайдений ключ, кількість перебраних варіантів, час та швидкість підбору ключів.

Розрахунки проводились за допомогою персонального комп'ютера з процесором Celeron 466 для довжини ключів від 1 до 3 символів, оскільки відкриття ключів з більшою довжиною потребує дуже великого періоду часу.

Для зручності аналізу значення трудомісткості, часу та швидкості "відкриття" ключів довжиною від 1 до 3 символів зведемо до табл. 1. На основі результатів, зведених до табл. 1, побудуємо графік залежності трудомісткості E від довжини ключа m для довжини ключа від 1 до 3 символів (рис. 1) в логарифмічній системі координат по осі ординат, який показує, що трудомісткість суттєво нелінійно залежить від довжини ключа.

Таблиця 1.

Значення трудомісткості "відкриття" ключів з довжиною від 1 до 3 символів

m, символів	m, біт	Трудомісткість E	t, с	v, вар/с	Ключ	Бітне представлення ключа
1	8	264	0,16	1650	Г	11000011
2	16	39787	14	2753	ГС	11000011 11010001
3	24	21009758	6060	3467	ГСб	11000011 11010001 11100001

Для визначення трудомісткості E для ключів довжиною m>3 символів проведемо регресійний аналіз залежності трудомісткості E від довжини ключа m. Для цього скористаємося програмним забезпеченням Microsoft Excel, яке дозволяє будувати лінії тренду та отримувати рівняння регресії. За характером кривої, зображеної на рис. 1, переконуємося в доцільності апроксимації експоненціальною функцією виду $y = ae^{bx}$, де a,

b – коефіцієнти регресії. Рівняння регресії і коефіцієнт кореляції наведені на вільному полі графіка.

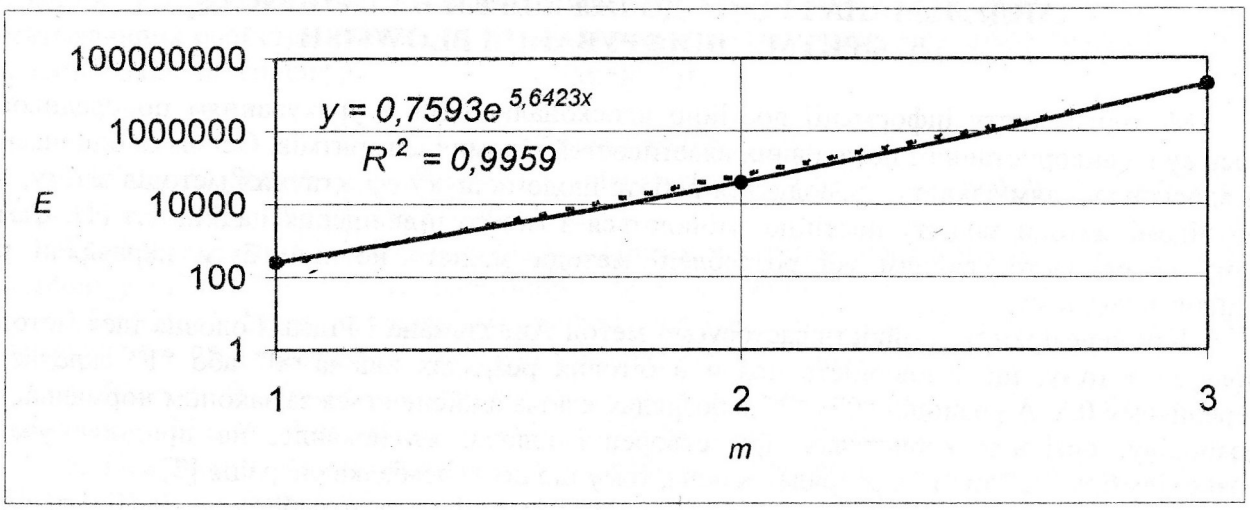

Рис. 1. Графік залежності трудомісткості E від довжини ключа m для довжини ключа від 1 до 3символів

На основі отриманого експоненціального рівняння регресії залежності трудомісткості E від довжини ключа m можна розрахувати теоретичне (прогнозоване) значення трудомісткості для значень довжини ключа m=4–56 символів (56 – максимальне значення довжини ключа для алгоритму шифрування BlowFish) [3].

Отримані значення зведемо до табл. 2.

Таблиця 2.

Значення трудомісткості "відкриття" ключів з довжиною від 1 до 56 символів

m, символів	m, біт	Трудомісткість E	m, символів	m,біт	Трудомісткість E	m, символів	m, біт	Трудомісткість E
1	8	264	20	160	7,7412E+48	39	312	2,7976E+95
2	16	39787	21	168	2,1839E+51	40	320	7,8923E+97
3	24	21009758	22	176	6,161E+53	41	328	2,227E+100
4	32	4809416853	23	184	1,7381E+56	42	336	6,281E+102
5	40	1,3568E+12	24	192	4,9033E+58	43	344	1,772E+105
6	48	3,8276E+14	25	200	1,3833E+61	44	352	4,999E+107
7	56	1,0798E+17	26	208	3,9024E+63	45	360	1,41E+110
8	64	3,0463E+19	27	216	1,1009E+66	46	368	3,979E+112
9	72	8,5939E+21	28	224	3,1058E+68	47	376	1,122E+115
10	80	2,4244E+24	29	232	8,7617E+70	48	384	3,166E+117
11	88	6,8396E+26	30	240	2,4718E+73	49	392	8,933E+119
12	96	1,9295E+29	31	248	6,9731E+75	50	400	2,52E+122
13	104	5,4434E+31	32	256	1,9672E+78	51	408	7,109E+124
14	112	1,5356E+34	33	264	5,5496E+80	52	416	2,006E+127
15	120	4,3322E+36	34	272	1,5656E+83	53	424	5,658E+129
16	128	1,2222E+39	35	280	4,4168E+85	54	432	1,596E+132
17	136	3,4479E+41	36	288	1,246E+88	55	440	4,503E+134
18	144	9,7268E+43	37	296	3,5152E+90	56	448	1,27E+137
19	152	2,744E+46	38	304	9,9166E+92			

На основі результатів табл. 2 побудуємо графік залежності трудомісткість – довжина ключа для довжини ключа 1...56 символів (рис. 2).

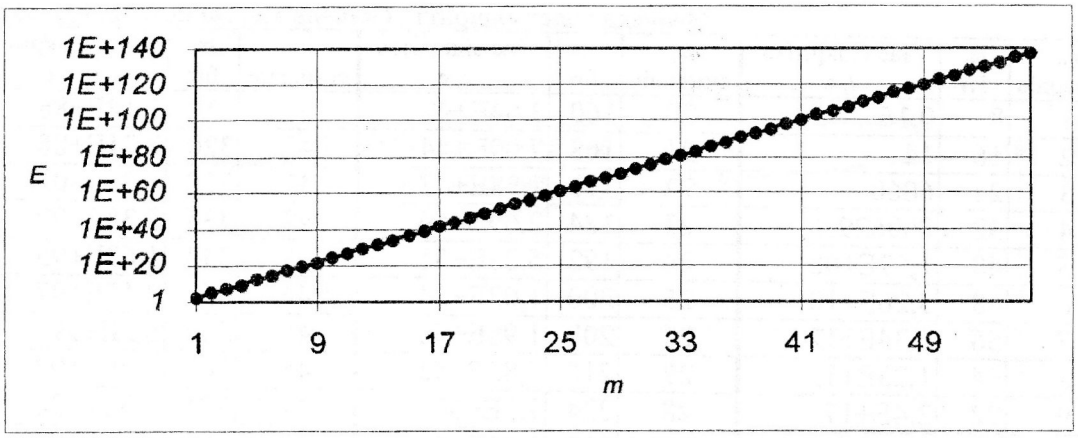

Рис. 2. Графік залежності трудомісткості *E* від довжини ключа *m* для довжини ключа від 1 до 56 символів

Наведені табл. 2 і рис. 2, отримані на основі регресійного аналізу, дозволяють визначити трудомісткість "відкриття" *E* ключа при будь-якій допустимій довжині ключа *m*. Значення квадрату коефіцієнта кореляції R^2 свідчить про високу достовірність отриманих результатів.

Використовуючи результати, наведені в табл. 1, побудуємо графік залежності часу відкриття *t* від довжини ключа *m* для довжини ключа від 1 до 3 символів (рис. 3) в логарифмічній системі координат по осі ординат, який показує, що час відкриття ключа суттєво нелінійно залежить від довжини ключа.

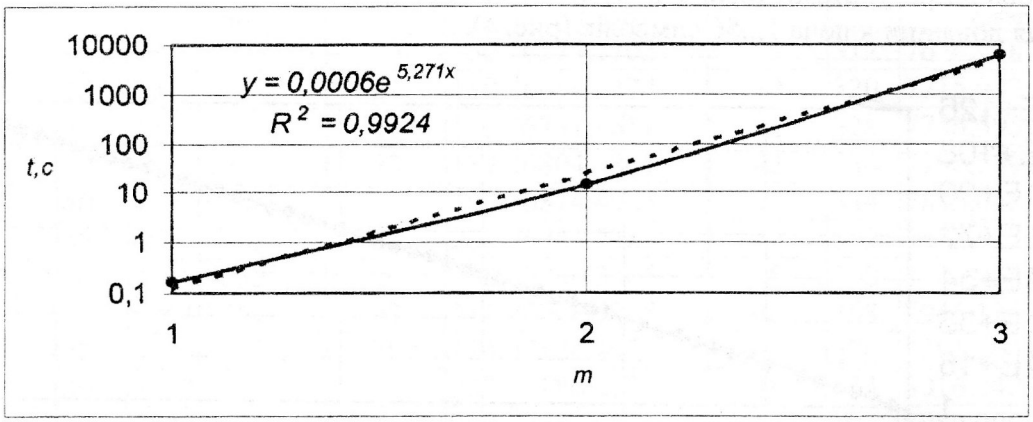

Рис. 3. Графік залежності часу відкриття *t* від довжини ключа *m* для довжини ключа від 1 до 3 символів

З метою визначення часу відкриття *t* для ключів довжиною *m*>3 символів проведемо регресійний аналіз залежності часу відкриття *t* від довжини ключа *m*. За характером кривої, зображеної на рис. 3, переконуємося в доцільності апроксимації експоненціальною функцією виду $y = ae^{bx}$, де *a*, *b* – коефіцієнти регресії. Рівняння регресії і коефіцієнт кореляції наведені на вільному полі графіка.

На основі отриманого експоненціального рівняння регресії залежності часу відкриття *t* від довжини ключа *m* можна розрахувати теоретичне (прогнозоване) часу відкриття *t* для значень довжини ключа *m*=4-56 символів (56 – максимальне значення довжини ключа для алгоритму шифрування BlowFish).

Отримані значення зведемо до табл. 3.

Таблиця 3.

Значення часу відкриття *t* ключів з довжиною від 1 до 56 символів

m, символів	*m*, біт	Час відкриття *t*, с	*m*, символів	*m*, біт	Час відкриття *t*, с	*m*, символів	*m*, біт	Час відкриття *t*, с
1	8	0,16	20	160	3,64E+42	39	312	1,14E+86
2	16	14	21	168	7,09E+44	40	320	2,21E+88
3	24	6060	22	176	1,38E+47	41	328	4,3E+90
4	32	860629,3	23	184	2,69E+49	42	336	8,38E+92
5	40	1,67E+08	24	192	5,23E+51	43	344	1,63E+95
6	48	3,26E+10	25	200	1,02E+54	44	352	3,17E+97
7	56	6,34E+12	26	208	1,98E+56	45	360	6,2E+99
8	64	1,23E+15	27	216	3,85E+58	46	368	1,2E+102
9	72	2,4E+17	28	224	7,5E+60	47	376	2,3E+104
10	80	4,68E+19	29	232	1,46E+63	48	384	4,6E+106
11	88	9,1E+21	30	240	2,84E+65	49	392	8,9E+108
12	96	1,77E+24	31	248	5,52E+67	50	400	1,7E+111
13	104	3,45E+26	32	256	1,08E+70	51	408	3,4E+113
14	112	6,71E+28	33	264	2,09E+72	52	416	6,5E+115
15	120	1,31E+31	34	272	4,07E+74	53	424	1,3E+118
16	128	2,54E+33	35	280	7,92E+76	54	432	2,5E+120
17	136	4,94E+35	36	288	1,54E+79	55	440	4,8E+122
18	144	9,62E+37	37	296	3E+81	56	448	9,4E+124
19	152	1,87E+40	38	304	5,84E+83			

На основі результатів табл. 3 побудуємо графік залежності часу відкриття *t* – довжина ключа для довжини ключа 1...56 символів (рис. 4).

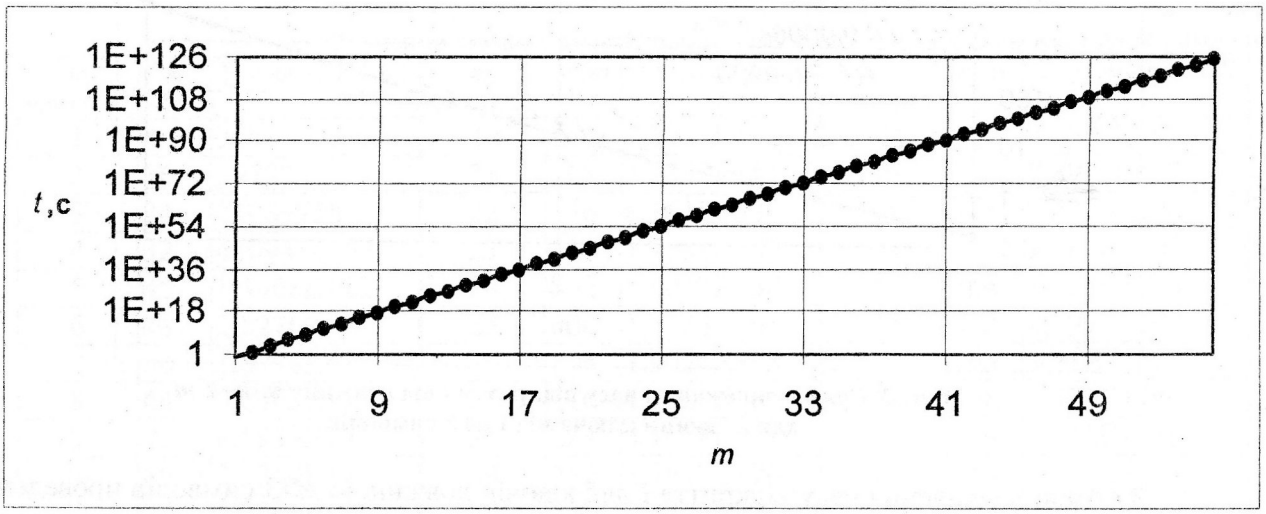

Рис. 4. Графік залежності часу відкриття *t* від довжини ключа *m* для довжини ключа від 1 до 56 символів

Наведені табл. 3 і рис. 4, отримані на основі регресійного аналізу, дозволяють визначити час відкриття *t* ключа при будь-якій допустимій довжині ключа *m*. Значення квадрату коефіцієнта кореляції R^2 свідчить про високу достовірність отриманих результатів.

Користуючись результатами (табл. 1), побудуємо графік залежності швидкості відкриття v від довжини ключа *m* для довжини ключа від 1 до 3 символів (рис. 5), який показує, що швидкість відкриття ключа нелінійно залежить від довжини ключа.

З метою визначення швидкості відкриття v для ключів довжиною $m>3$ символів проведемо регресійний аналіз залежності швидкості відкриття v від довжини ключа *m*. За характером кривої, зображеної на рис. 3, переконуємося в доцільності апроксимації

логарифмічною функцією виду $y = a \ln x + b$, де a, b – коефіцієнти регресії. Рівняння регресії і коефіцієнт кореляції наведені на вільному полі графіка.

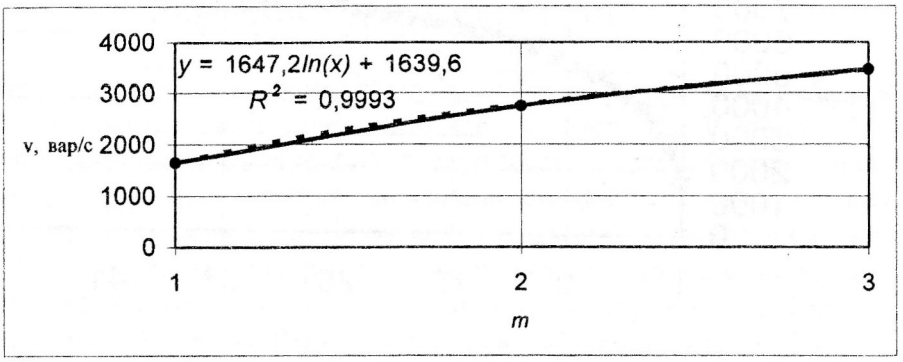

Рис. 5. Графік залежності швидкості відкриття v від довжини ключа *m* для довжини ключа від 1 до 3 символів

На основі отриманого логарифмічного рівняння регресії залежності швидкості відкриття v від довжини ключа m можна розрахувати теоретичне (прогнозоване) значення швидкості відкриття v для значень довжини ключа m=4–56 символів (56 – максимальне значення довжини ключа для алгоритму шифрування BlowFish).

Отримані значення зведемо до табл. 4.

Таблиця 4.

Значення швидкості відкриття v ключів з довжиною від 1 до 56 символів

m, символів	*m*, біт	Швидкість відкриття v, вар/с	*m*, символів	*m*, біт	Швидкість відкриття v, вар/с	*m*, символів	*m*, біт	Швидкість відкриття v, вар/с
1	8	1650	20	160	6574,1702	39	312	7674,2187
2	16	2753	21	168	6654,5374	40	320	7715,9222
3	24	3467	22	176	6731,1651	41	328	7756,5959
4	32	3923,1041	23	184	6804,3861	42	336	7796,2894
5	40	4290,6661	24	192	6874,4903	43	344	7835,0488
6	48	4590,9862	25	200	6941,7323	44	352	7872,9172
7	56	4844,9032	26	208	7006,3366	45	360	7909,9345
8	64	5064,8561	27	216	7068,5025	46	368	7946,1381
9	72	5258,8683	28	224	7128,4073	47	376	7981,5631
10	80	5432,4182	29	232	7186,2097	48	384	8016,2423
11	88	5589,4131	30	240	7242,0523	49	392	8050,2064
12	96	5732,7382	31	248	7296,0637	50	400	8083,4843
13	104	5864,5846	32	256	7348,3602	51	408	8116,1032
14	112	5986,6552	33	264	7399,0473	52	416	8148,0887
15	120	6100,3003	34	272	7448,2211	53	424	8179,4648
16	128	6206,6081	35	280	7495,9693	54	432	8210,2545
17	136	6306,469	36	288	7542,3724	55	440	8240,4792
18	144	6400,6204	37	296	7587,504	56	448	8270,1593
19	152	6489,6799	38	304	7631,4319			

На основі результатів табл. 4 побудуємо графік залежності швидкості відкриття v – довжина ключа для довжини ключа 1–56 символів (рис. 6).

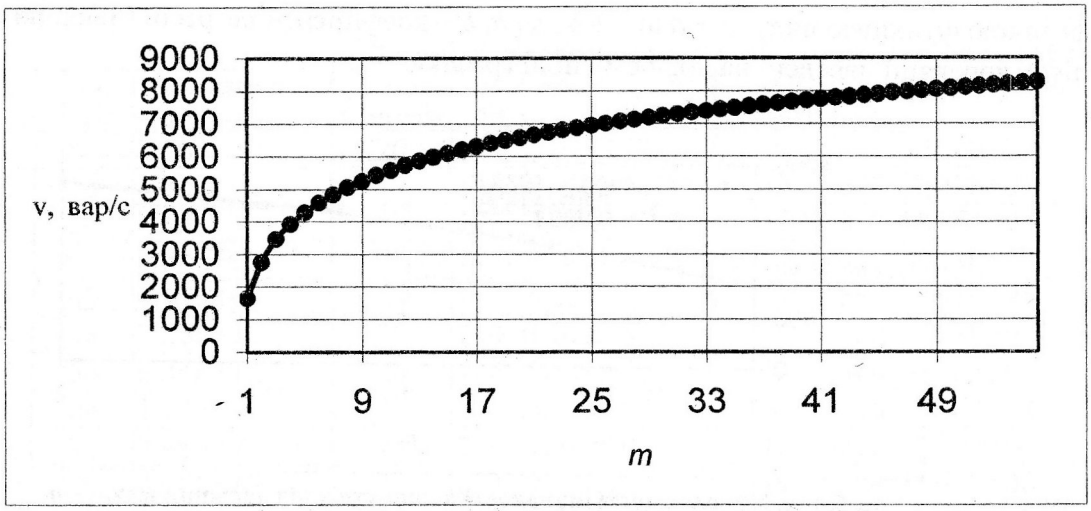

Рис. 6. Графік залежності швидкості відкриття v від довжини ключа *m* для довжини ключа від 1 до 56 символів

Наведені табл. 4 і рис. 6, отримані на основі регресійного аналізу, дозволяють визначити швидкість відкриття v ключа при будь-якій допустимій довжині ключа *m*. Значення квадрату коефіцієнта кореляції R^2 свідчить про високу достовірність отриманих результатів.

Таким чином, результати регресійного аналізу, наведені у табл. 2–4 і на рис. 2, 4, 6, дозволяють визначити трудомісткість, час та швидкість "відкриття" ключа модифікованим методом криптоаналізу Андельмана і Рідса при будь-якій допустимій довжині ключа *m*. Одержано рівняння регресії: для трудомісткості і часу відкриття ключа у вигляді експоненціальної функції і для швидкості відкриття у вигляді логарифмічної функції. Значення квадратів коефіцієнтів кореляції R^2 свідчить про високу достовірність отриманих результатів.

Порівнюючи час відкриття ключа BlowFish модифікованим методом криптоаналізу Андельмана і Рідса з методами простого і ймовірнісного перебору варіантів ключів можна прийти до висновку, що використання модифікованого методу криптоаналізу Андельмана і Рідса дозволяє підвищити швидкість перевірки ключів порівняно з методами простого і ймовірнісного перебору варіантів ключів.

З точки зору криптостійкості стійкими до модифікованого методу криптоаналізу Андельмана і Рідса є ключі BlowFish довжиною $m \geq 6$ символів для документів з терміном секретності 50 років ($1{,}58 \cdot 10^9$ с). Використання динамічного ключа BlowFish [3] дозволить суттєво зменшити мінімально стійку довжину ключа, що дозволить зробити шифр BlowFish абсолютно стійким до криптоаналізу модифікованим методом Андельмана і Рідса.

Список літератури

1. *Жельников В.* Криптография от папируса до компьютера. - М.: ABF, 1997. –335 с.

2. *Andelman D., Reeds J.* On the cryptanalysis of rotor machines and substitu tion-permutation networks // IEEE transactions on information theory, v. IT-28, 1982, pp. 578-584.

3. *Шварц І.М., Білан С.М.* Авторське свідоцтво № 13572 «Комп'ютерна програма для програмування ПЛІС з використанням» вдосконаленого алгоритму Blowfish.

Надійшла 26.04.2006