Постольський О.С.
студент;
Захарченко М.В.
доктор технічних наук, професор,
Одеська національна Академія зв'язку імені О.С. Попова

ДИСПЕРСІЙНА ОЦІНКА ЯКОСТІ ШИФРУВАННЯ

Криптографічне кодування переслідує декілька цілей. Найбільш очевидні з них – необхідність гарантувати, що кодована інформація зберігається в секреті від усіх одержувачів, окрім тих кому вона призначена. Однак оскільки взаємодіючі в мережі зв'язку партнери можуть бути фізично розділені, то існують і інші вимоги до захисту, вони повинні включати в себе гарантії того, що протилежна сторона є саме тим, ким вона себе об'являє. Тому другою вимогою криптографічного кодування є гарантія того, що зв'язуючі сторони не шахраюють.

В данній роботі проведений аналіз відкритого та зашифрованого тексту, та визначенні статистичні параметри відкритого тексту та шифрограми:

1) значення математичного очікування частоти появи кожного символа M(x_i) на *вході та виході шифратора* $M_{\text{вх}}(x_i) * M_{\text{вых}}(x_i)$

2) значення дисперсії відхилень D(x_i) частот появи кожного символа $M_{\text{вх}}(x_i) * M_{\text{вых}}(x_i)$

Статистичні параметри відкритого тексту приведені в таблиці 1

Таблиця 1

Статистичні параметри відкритого тексту

Букви	А	Б	В	Г	Д	Е	Ж	З
1	18	2	18	2	9	37	3	9
2	0,048	0,005	0,048	0,005	0,024	0,099	0,008	0,024
3	0,868	0,01	0,868	0,01	0,217	3,67	0,024	0,217
4	70,157	594,189	70,157	594,157	301,925	112,869	546,437	301,925
5	8,376	24,376	8,376	24,376	17,176	10,624	23,376	17,376

Букви	И	К	Л	М	Н	О	П	Р
1	52	8	8	17	30	43	11	17
2	0,139	0,021	0,021	0,045	0,08	0,115	0,029	0,045
3	7,249	0,171	0,171	0,774	2,413	4,957	0,324	0,774
4	56,589	337,677	337,677	87,909	13,133	276,357	236,421	87,909
5	25,624	18,376	18,376	9,376	3,624	16,624	15,376	9,376

Букви	С	Т	У	Ф	Х	Ц	Ч
1	27	21	4	2	7	5	4
2	0,072	0,056	0,01	0,005	0,018	0,013	0,01
3	1,954	1,182	0,043	0,01	0,131	0,067	0,043
4	0,389	28,901	500,685	594,189	375,429	456,933	500,685
5	0,623	5,376	22,376	24,376	19,376	21,376	22,376

Букви	Ш	Щ	Э	Ю	Я	Ь	Ъ	∑
1	1	2	2	3	8	2	1	373
2	0,002	0,005	0,005	0,008	0,021	0,005	0,002	1,009
3	0,002	0,01	0,01	0,024	0,171	0,01	0,002	26,376
4	643,941	594,189	594,189	546,437	337,667	594,189	643,941	11037
5	25,376	24,376	24,376	23,376	18,376	24,376	25,376	105

Джерело: розробка автора

В таблиці 1 представлений аналіз відкритого тексту.
Статистичні параметри шифрограми представлені у вигляді таблиці 2.

Таблиця 2

Статистичні параметри шифрограми

Букви	А	Б	В	Г	Д	Е	Ж	З
1	12	5	13	7	13	21	13	10
2	0,032	0,013	0,034	0,018	0,034	0,056	0,034	0,026
3	0,386	0,067	0,453	0,131	0,453	1,181	0,453	0,268
4	17,413	124,835	10,067	84,143	10,067	23,299	10,067	38,105
5	4,173	11,173	3,173	9,173	3,173	4,826	3,173	6,173

Букви	И	К	Л	М	Н	О	П	Р
1	23	18	7	20	17	25	14	24
2	0,061	0,048	0,018	0,053	0,045	0,067	0,037	0,064
3	1,418	0,868	0,131	1,072	0,774	1,675	0,525	1,544
4	46,607	3,337	84,143	14,645	0,683	77,915	4,721	61,261
5	6,862	1,826	9,173	3,826	0,826	8,826	2,173	7,826

Букви	С	Т	У	Ф	Х	Ц	Ч
1	22	19	8	13	13	18	9
2	0,058	0,05	0,021	0,034	0,034	0,048	0,024
3	1,297	0,967	0,171	0,453	0,453	0,868	0,217
4	33,953	7,991	66,797	10,067	10,067	3,337	51,451
5	5,826	2,826	8,173	3,173	3,173	1,826	7,173

Букви	Ш	Щ	Э	Ю	Я	Ь	Ъ	СУМА
1	6	5	5	3	4	2	4	373
2	0,016	0,013	0,013	0,008	0,01	0,005	0,01	0,984
3	0,096	0,067	0,067	0,024	0,042	0,01	0,042	16,173
4	103,489	124,835	124,835	173,527	148,181	200,873	148,181	1818,892
5	10,173	11,173	11,173	13,173	12,173	14,173	12,173	42,64

Джерело: розробка автора

В таблиці 2 представлений аналіз зашифрованого тексту, шифром Віженера з ключем довжиною 4 символи.

В першому стовбці цифрами 1-5 позначені:

1) кількість кожної літери в зашифрованому тексті;
2) частота появи літер в зашифрованому тексті;
*3)*відхилення від математичного очікування появи літер в тексті

$$M(X) = \sum_{i=1}^{n} x_i * p_i ;$$

4) квадрати відхилень

$$D(X) = (M(x) - x_i)^2 ;$$

5) середнєквадратичне відхилення

$$\sigma(x) = \sqrt{(M(x) - x_i)^2} ;$$

Список використаних джерел:

1. Анин Б. О шифровании и дешифровании. Журнал Конфидент. 1997. № 1.
2. Петраков А.В. Защита и охрана личности, собственности и информации. – М.: Радио и связь. 1997. 320 с.
3. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров.
4. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. 2009. 38 с.