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

СИНТЕЗ ШИФРОГРАМИ З РІВНОІМОВІРНИМИ КОДОВИМИ СЛОВАМИ

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 при шифруванні переданого тексту один і той же символ передається різними кодовими конструкціями, число яких дорівнює найближчому цілому значенні вірогідності появи данного символа. Для такої передачі необхідно що б на передавальній стороні були банки різних кодових слів в кількості рівній найближчим цілим числам вірогідності появи відповідного символа. В таблиці 1 приведені ці значення. В цьому випадку ентропія використаних кодових слів буде максимальна. Всього різних кодових слів $N_{\text{к.с}} = 116$. Але передаватися в канал зв'язку буде одна кодова комбінація із банка данного символа.

Вірогідність появи окремих символів російського алфавіту представлена у вигляді таблиці 1.

Також для повноти дослідження, в таблиці 2 представимо вірогідність появи літер в зашифрованому тексті, де загальна кількість кодових комбінацій буде дорівнювати N_(к.с)=111,

де:

1) кількість літер в тексті;
2) частота появи літер в тексті;
3) відсоток появи літер в тексті;
4) кількість кодових комбінацій;

Таким чином, кількість символів в таблиці 1 визначається вірогідністю появи символів, які приведені в рядку 4 різними кодовими конструкціями, забезпечує вірогідність появи кожного кодового слова в каналі і буде близьке до вірогідності P_(к.с)≈1%.

Для цього на передавальній стороні існують банки окремих символів x_i з пам'ятью про кількість кодових слів різних конструкцій на кожен символ x_i. При появі в передавальному тексті символа x_i з банка пам'яті передається наступне кодове слово з кодових слів відповідних данному символу.

Таблиця 1

Вірогідність появи окремих символів російського алфавіту

№	Символ	$P(x_i)$,%	Кількість кодових комбінацій	№	Символ	$P(x_i)$,%	Кількість кодових комбінацій
1	–	17,5	18	17	Я	1,8	2
2	О	9	9	18	Ы	1,6	2
3	Е, Ё	7,2	8	19	З	1,6	2
4	А	6,2	7	20	Ь, Ъ	1,4	2
5	И	6,2	7	21	Б	1,4	2
6	Т	5,3	6	22	Г	1,3	2
7	Н	5,3	6	23	Ч	1,2	2
8	С	4,5	5	24	Й	1	1
9	Р	4	4	25	Х	0,9	1
10	В	3,8	4	26	Ж	0,7	1
11	Л	3,5	4	27	Ю	0,6	1
12	К	2,8	3	28	Ш	0,6	1
13	М	2,6	3	29	Ц	0,4	1
14	Д	2,5	3	30	Щ	0,3	1
15	П	2,3	3	31	Э	0,3	1
16	У	2,1	3	32	Ф	0,2	1
Загальна кількість кодових комбінацій $N_{к.с} = 116$							

Розробка автора, по джерелу [4]

Таблиця 2

Вірогідність появи літер в зашифрованому тексті

Букви	А	Б	В	Г	Д	Е	Ж	З
1	9	9	9	7	10	14	4	15
2	0,024	0,024	0,024	0,018	0,026	0,037	0,01	0,04
3	2,4	2,4	2,4	1,8	2,6	3,7	1	4
4	3	3	3	2	3	4	1	4

Букви	И	К	Л	М	Н	О	П	Р
1	38	4	5	13	19	9	7	13
2	0,101	0,01	0,013	0,034	0,05	0,024	0,018	0,034
3	10,1	1	1,3	3,4	5	2,4	1,8	3,4
4	11	1	2	4	5	3	2	4

Букви	С	Т	У	Ф	Х	Ц	Ч
1	26	8	6	8	18	17	15
2	0,069	0,021	0,016	0,021	0,048	0,045	0,04
3	6,9	2,1	1,6	2,1	4,8	4,5	4
4	7	3	2	3	5	5	4

Букви	Ш	Щ	Э	Ю	Я	Ь	Ъ	СУМА
1	10	11	17	17	16	11	8	373
2	0,026	0,029	0,045	0,045	0,042	0,029	0,021	0,984
3	2,6	2,9	4,5	4,5	4,2	2,9	2,1	98,4
4	3	3	5	5	2	3	3	111

Джерело: розробка автора

Враховуючи приведене, середня вірогідність появи кодових слів в каналі, буде прагнути до рівноймовірної що не перевищує 1%.

Загальна кількість збережених різних кодових слів $N_{\text{к.с}}$ для всіх символів x_i,в зашифрованному тексті, дорівнює:

$$N_{\text{к.с}} = E^{+}\left[\frac{1}{P(x_1)}\right] + E^{+}\left[\frac{1}{P(x_2)}\right] + \cdots + E^{+}\left[\frac{1}{P(x_{32})}\right] = \sum_{i=1}^{n} E^{+}\left[\frac{1}{P(x_i)}\right] = 111$$

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. Г. Корн и Т. Корн. 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. 326 с.

Стайкуца С.В.
кандидат філософських наук, доцент;
Колівошко Р.М., Чернявський С.С.
студенти,
Одеська національна Академія зв'язку імені О.С. Попова

ЩОДО ПАРАМЕТРІВ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ З ФУНКЦІЄЮ ВІДЕОАНАЛІТИКИ

Системи відеоспостереження, як один з елементів технічних засобів охорони, широко використовуються для підвищення рівня безпеки об'єктів. Розуміння оптимальних параметрів систем відеоспостереження – запорука її ефективної роботи і підтримання «життєвого циклу» систем. Сьогодні при