Национальный исследовательский университет информационных технологий,
механики и оптики.
Кафедра вычислительной техники.
Методы и средства защиты компьютерной информации.

Лабораторная работа №6

Аддитивные шифры.

11 вариант

Работу выполнил студент группы P3415
Халанский Дмитрий

2017

1. Цель работы

- Расшифровать криптограмму, зашифрованную аддитивным шифром на базе сдвигового регистра.

2. Исходный текст

ВЗАИМОЗАМЕНЯЕМЫЙ

3. Гамма

1101010000111111
1011101101111010
0010110010111110
0010000001100110
1100011100111010
1110000100110000
0101010110100100
1010011110010001

4. Протокол криптоанализа

Мы составили программный комплекс, который обнаруживает для заданных биграмм и шифротекста те позиции, в которых может находиться каждая биграмма, методом поиска обратных матриц.

```
биграмма 1      позиция 5-6     отводы 1000011  05 блоков назад
биграмма 1      позиция 8-9     отводы 1100011  08 блоков назад
биграмма 1      позиция 12-13   отводы 1110001  12 блоков назад
биграмма 1      позиция 14-15   отводы 0000011  14 блоков назад
биграмма 2      позиция 2-3     отводы 0001011  02 блоков назад
биграмма 2      позиция 3-4     отводы 0000011  03 блоков назад
биграмма 2      позиция 6-7     отводы 0101011  06 блоков назад
биграмма 2      позиция 8-9     отводы 1000010  08 блоков назад
биграмма 2      позиция 10-11   отводы 0000111  10 блоков назад
биграмма 2      позиция 11-12   отводы 0011111  11 блоков назад
биграмма 2      позиция 12-13   отводы 1101111  12 блоков назад
биграмма 3      позиция 3-4     отводы 0111001  03 блоков назад
биграмма 3      позиция 10-11   отводы 0010100  10 блоков назад
биграмма 3      позиция 13-14   отводы 0110101  13 блоков назад
биграмма 4      позиция 3-4     отводы 0110101  03 блоков назад
биграмма 4      позиция 11-12   отводы 0100011  11 блоков назад
```

```
биграмма 4      позиция 13-14   отводы 1100000  13 блоков назад
биграмма 5      позиция 8-9     отводы 1100110  08 блоков назад
биграмма 5      позиция 11-12   отводы 0000001  11 блоков назад
биграмма 6      позиция 2-3     отводы 1101111  02 блоков назад
биграмма 6      позиция 6-7     отводы 0000110  06 блоков назад
биграмма 6      позиция 9-10    отводы 1111011  09 блоков назад
биграмма 6      позиция 10-11   отводы 1001001  10 блоков назад
биграмма 6      позиция 12-13   отводы 0100001  12 блоков назад
биграмма 7      позиция 2-3     отводы 1000100  02 блоков назад
биграмма 7      позиция 3-4     отводы 1110000  03 блоков назад
биграмма 8      позиция 10-11   отводы 0011011  10 блоков назад
биграмма 8      позиция 12-13   отводы 1110010  12 блоков назад
```

После определения возможнх положений биграмм мы начали перебор и обнаружили, что третье предположение приводит к читаемому тексту.

Протокол работы программы выглядит так:

```
***************
Загружен вариант №11.
Шифрограмма:
0001011011111000
0111101110110010
1110000001110000
1110011110100110
0000101111111111
0010110011101111
1001000001101000
0111110001011000
-----------
Выбрана вероятная биграмма ЕН
-----------
Открытый текст ВЗАИМОЗАМЕНЯЕМЫЙ получен предполагая, что:
-вероятная биграмма находится на позиции 12-13
-вероятная часть ключа 0101010110100101
-для шифрования использовался регистр с положением отводов: 1110001
-начальное заполнение при шифровании: 0101011
**********ВЫХОД
```

5. Проверка алгоритмом Берликэмпа-Месси

Мы ожидаем увидеть отвод, задаваемый формулой $h(x) = x^7 + x^6 + x^5 + x^4 + 1$, что соответствует формуле $C(D) = D^7 + D^3 + D^2 + D + 1$.

g_N	D	$T(D)$	$C(D)$	L	m	$B(D)$	N
-	-	-	1	0	-1	1	0
0	0	-	1	0	-1	1	1
1	1	1	$1+D^2$	2	1	1	2
0	0	1	$1+D^2$	2	1	1	3
1	0	1	$1+D^2$	2	1	1	4
0	0	1	$1+D^2$	2	1	1	5
1	0	1	$1+D^2$	2	1	1	6
0	0	1	$1+D^2$	2	1	1	7
1	0	1	$1+D^2$	2	1	1	8
1	1	$1+D^2$	$1+D^2+D^7$	7	8	$1+D^2$	9
0	1	$1+D^2+D^7$	$1+D+D^2+D^3+D^7$	7	8	$1+D^2$	10
1	0	$1+D^2+D^7$	$1+D+D^2+D^3+D^7$	7	8	$1+D^2$	11
0	0	$1+D^2+D^7$	$1+D+D^2+D^3+D^7$	7	8	$1+D^2$	12
0	0	$1+D^2+D^7$	$1+D+D^2+D^3+D^7$	7	8	$1+D^2$	13
1	0	$1+D^2+D^7$	$1+D+D^2+D^3+D^7$	7	8	$1+D^2$	14

Результат совпал с нашими ожиданиями.