ПРАКТИЧНЕ ЗАНЯТТЯ №2. ЗНАЙОМСТВО З ШИФРОМ «ОДНОРАЗОВИЙ БЛОКНОТ»

1.1 Мета заняття

Ознайомити студентів з шифром «одноразовий блокнот», відпрацювати навички використовування цього шифру для кодування та декодування тексту.

1.2 Теоретичні відомості

Для шифрування відкритого тексту використовуються шифроблокноти, на кожному аркуші яких написана послідовність випадкових чисел. Як у відправника, так і у одержувача повинні бути два заздалегідь складених однакових шифроблокнота.

Спочатку треба перетворити ваш текст в цифри. Для цього використовується таблиця стиснення (straddling checkerboard). В якомусь сенсі це аналог алгоритмів, що лежать в основі zip, rar тощо, тільки таблиця стиснення у нас фіксована. Ні, ви звичайно можете і просто зіставити буквам цифри за принципом А = 1, Б = 2 і т.д, але через надмірність мови ви будете змушені потім шифрувати десь на третину більше. Просидівши кілька годин з олівцем за тупою арифметикою, ви швидко оціните переваги таблиці стиснення...

Для створення таблиці стиснення запам'ятовуємо: А И ТЕСНО. Тут задіяно сім найчастіших букв в російській мові. Для англійської беремо скажімо AT ONE SIR (в англійській мові менше букв і можна обійтися тільки двома додатковими рядками) і т.п. Складаємо таблицю, в першому рядку якої йдуть символи, що часто зустрічаються, а в інших залишки алфавіту. Зверніть увагу, що в першому рядку не задіяні цифри 8, 9 і 0, і вони ж позначають, що буква (рідше зустрічається) кодується не однією цифрою, а двома. Отже, для кодування літери шукаємо її, якщо вона знаходиться в першому рядку, то ми вибираємо номер її колонки (наприклад Т = 3), якщо вона в інших колонках, то ми спочатку вибираємо номер її рядка, а потім номер колонки, наприклад Б = 81, а Я = 04:

	1	2	3	4	5	6	7	8	9	0
	А	И	Т	Е	С	Н	О			
8	Б	В	Г	Д	Ж	З	К	Л	М	П
9	Р	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
0	Ь	Э	Ю	Я						пробел

Однак після завершення перекладу в цифровий вираз текст все ще не є шифром. Закодований вищенаведеним способом текст уже помітно складніше взяти в лоб простим частотним аналізом, але все одно на шифр воно ніяк не тягне. Тепер беремо ключ, якщо є необхідність, таким же чином переводимо його в цифрове представлення. В ідеальному випадку ключ збігається довжиною з зашифрованим текстом, але в нашому навчальному прикладі він коротше, і досить його повторити потрібну кількість разів. Якщо ключ виявиться довшим повідомлення просто додайте в кінці повідомлення відповідну кількість нулів.

При роботі з одноразовими блокнотами в ручному режимі зручніше використовувати додавання по модулю 10, що можна записати в вигляді таблиці (т.зв. циркулянт):

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Зворотна операція віднімання по модулю виглядає як (рядок мінус стовпець):

-	0	1	2	3	4	5	6	7	8	9
0	0	9	8	7	6	5	4	3	2	1
1	1	0	9	8	7	6	5	4	3	2
2	2	1	0	9	8	7	6	5	4	3
3	3	2	1	0	9	8	7	6	5	4
4	4	3	2	1	0	9	8	7	6	5
5	5	4	3	2	1	0	9	8	7	6
6	6	5	4	3	2	1	0	9	8	7
7	7	6	5	4	3	2	1	0	9	8
8	8	7	6	5	4	3	2	1	0	9
9	9	8	7	6	5	4	3	2	1	0

Приклад виконаного шифрування в десятковій системі:

відкритий текст	25665	04501	78922	25554	25335
ключ	85948	22026	98654	25651	75871

шифротекст	00503	26527	66576	40105	90106

При зворотної операції з шифротекста шляхом віднімання ключа по модулю десять виходить відкритий текст:

шифротекст	00503	26527	66576	40105	90106
ключ	85948	22026	98654	25651	75871
відкритий текст	25665	04501	78922	25554	25335

1.3 Завдання для виконання

Завдання 1. Розшифрувати повідомлення прикладеним ключем. Варіант вибирається за номером в журналі (таблиця 6.1).

Таблиця 7.1 – Варіанти для першого завдання

№	Повідомлення	Ключ
1	671988219686408586497927 5245	лес
2	365257646529192855012695 9788	сол
3	188639984753915232037213 7912	три
4	635618243925445847851206097561	два
5	405661687923232269865264 3582	нав
6	694288839621302805827150520788	пол
7	571178238688308777010661697418 47	одо
8	571578278682308177050665697818 41	ода
9	679988019666406586485732 2825	лис
10	637682601023464285754583240282	дэв

Завдання 2. Варіанти другого завдання вибирається з таблиці на підставі декодування попереднього (таблиця 7.2).

Таблиця 7.2 – Варіанти другого завдання

№	Текст завдання
1	Зашифровать свои ФИО и день рождения номером в журнале
2	Зашифровать любое шестизначное число сегодняшним днём недели
3	Зашифровать название и дату произвольного праздника вашим именем
4	Зашифровать произвольный текст длинной до 70 символов ключом длинной до 30 символов

Завдання 3. Обмінятися з колегою результатами і ключами з попереднього завдання і зробити декодування.

1.4 Захист практичного завдання

Захист практичного завдання проводиться індивідуально або бригадою у складі двох студентів. Викладачу надається звіт та студент відповідає на теоретичні запитання в особистій бесіді.

Звіт включає в себе:

- мета практичного заняття;
- індивідуальне завдання;
- хід його вирішення;
- результат виконання;
- висновки.

1.5 Контрольні питання

1. Що таке шифроблокнот?
2. Для чого потрібна таблиця стиснення?
3. Як створюється таблиця стиснення?
4. Чому переведений в цифровий вираз текст все ще не є шифром?
5. Що таке ключ?

Що таке циркулянт?