Лабораторна робота *№8*

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ШИФРУВАННЯ ТЕКСТОВОЇ ІНФОРМАЦІЇ ІЗ ВИКОРИСТАННЯМ КРИПТОГРАФІЧНОГО ШИФРУ ГАМУВАННЯ

Мета – дослідження процесів шифрування текстової інформації із використанням криптографічного шифру гамування

ТЕОРЕТИЧНІ ВІДОМОСТІ

Перетворення відкритого тексту часто виконується за допомогою обчислень, що здійснюються над літерами алфавіту, яким попередньо присвоєні деякі числові значення. Наприклад, літери алфавіту нумеруються з нуля, а їх числові значення збігаються з цими номерами. Для латинського алфавіту літері A можна приписати значення 0, літері B – значення 1, літері C – значення 2 і так далі до літери Z, якій приписується значення, що рівне 25. Для того, щоб скласти літери B і D складемо їх числові значення: 1 + 3 = 4. Розглянемо суму як числове значення деякої літери латинського алфавіту. Легко бачити, що такою літерою є літера E. Вважаємо тому: $B + D = E$. При додаванні літери Z з літерою C числове значення дорівнює 27 і, мабуть, не відповідає жодній літері алфавіту. В таких випадках вважають, що в алфавіті за літерою Z йде літера A, потім B і т. д. У другому алфавіті літері A приписане числове значення рівне 26, літері B – 27 і так до літери Z. Потім йде третій алфавіт, четвертий алфавіт і так далі необхідну кількість разів. Таким чином, можна додавати кілька букв в одному виразі, виконувати множення букв або множити літери на константи. В даному випадку: $Z + C = B$. Зазначені дії над числовими значеннями букв відповідають операціям, виконуваним над числами за модулем m, де модуль дорівнює кількості знаків в алфавіті.

Часто величину m називають модулем алфавіту. Під час виконання модульних операцій однаковим літерам, які знаходяться в різних, послідовно записаних алфавітах повинні відповідати однакові числові значення. Наприклад, значення 1, 27, 53 задають ту саму букву B і вони, у цьому розумінні, еквівалентні. Неважко бачити, що ці числа відрізняються на величину, кратну m, тобто мають один і той же залишок під час ділення на модуль алфавіту. Такі числа називаються порівняними за модулем m, що записується у вигляді так званих порівнянь: $a = b(\mathrm{mod}\ m)$, тобто $1 = 27(\mathrm{mod}\ 26)$, або $1 = 27(26)$. При переході до порівнянь, числові значення і модуль алфавіту маються на увазі, а самі порівняння часто записуються як рівності: $Z + C = B$, замість $Z + C = B(\mathrm{mod}\ 26)$.

Для отримання шифрованого тексту S існує три способи накладання гами Г на відкритий текст O: додавання гами і тексту $S = Г + O$, віднімання гами з тексту $S = O — Г$ і віднімання тексту з гами $S = Г — O$. Під операціями додавання і віднімання розуміються як звичайні операції за модулем m, так і застосування замість них відповідних таблиць. Процедура розшифрування, очевидно, будується природним чином, використовуючи обернені перетворення $O = S — Г$, $O = S + Г$, $O = Г — S$ або обернені таблиці, відповідно.

Створення ключа

Для шифрування методом гамування необхідно визначити алфавіт, на основі якого будуть створюватись повідомлення та ключ. Також кожному символу треба надати послідовний номер (код), який буде використовуватись при гамування.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

У якості основи гами (ключ) зручно обрати слово-гасло. Нехай це буде «amusement». Сама гама має довжину відкритого повідомлення і складається із повторення гасла.

Шифрування

Необхідно зашифрувати наступний відкритий текст: «Unix is user-friendly. It's just very selective about who its friends are». Приводимо даний текст до канонічного вигляду, тобто відкидаємо усі символи, що відсутні в означеному алфавіті. Отримуємо:

unixisuserfriendlyitsjustveryselectiveaboutwhoitsfriendsare

Складаємо таблицю із трьох рядків. Перший ряд О містить відкрите повідомлення, другий Г — гаму, третій S — шифрований текст.

За умовою завдання гамування необхідно здійснити за формулою S = Г — О(mod 26). Це означає, що для отримання поточного символу шифротексту треба від коду відповідного символу гами відняти код відповідного символу відкритого тексту. Таким чином перший символ гами «a», що має код 0, відняти по модулю 26 перший символ відкритого тексту «u» із кодом 20 дає у результаті код 6, тобто символ «g» шифротексту. В результаті виконання усього процесу гамування отримуємо таблицю:

О	u	n	i	x	i	s	u	s	e	r	f	r	i	e	n	d	l	y	i	t	s	j	u	s	t	v	e	r	y	s
Г	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u
S	g	z	m	v	w	u	k	v	p	j	h	d	k	a	z	b	c	v	s	t	c	j	k	u	l	s	p	j	o	c
О	e	l	e	c	t	i	v	e	a	b	o	u	t	w	h	o	i	t	s	f	r	i	e	n	d	s	a	r	e	
Г	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	
S	o	t	i	c	u	l	f	i	u	r	q	s	l	r	m	m	e	b	a	z	v	w	j	g	x	u	u	b	a	

Зашифроване повідомлення має такий вигляд:

gzmvwukvpjhdkazbcvstcjkulspjocoticulfiurqslrmmebazvwjgxuuba

Дешифрування

Дешифрування відбувається у зворотньому порядку за формулою О = Г — S(mod 26). Так перший символ гами «a» (0) відняти по модулю 26 перший символ шифротексту «g» (6) буде 20, тобто «u».

S	g	z	m	v	w	u	k	v	p	j	h	d	k	a	z	b	c	v	s	t	c	j	k	u	l	s	p	j	o	c
Г	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u
О	u	n	i	x	i	s	u	s	e	r	f	r	i	e	n	d	l	y	i	t	s	j	u	s	t	v	e	r	y	s
S	o	t	i	c	u	l	f	i	u	r	q	s	l	r	m	m	e	b	a	z	v	w	j	g	x	u	u	b	a	
Г	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	
О	e	l	e	c	t	i	v	e	a	b	o	u	t	w	h	o	i	t	s	f	r	i	e	n	d	s	a	r	e	

Після розшифрування отримуємо:

unixisuserfriendlyitsjustveryselectiveaboutwhoitsfriendsare

Розшифроване повідомлення еквівалентне вихідному відкритому повідомленню. Це свідчить про правильність виконання процесів шифрування та дешифрування.

Формули для шифрування:

1. S = (О + Г)modN

Наприклад 1. N=26, О=14, Г=20. S = (14 + 20)mod26 = 34mod26 = 8

2. N=26, О=14, Г=10. S = (14 + 10)mod26 = 24mod26 = 24

2. S = (О - Г)

Наприклад 1. N=26, О=14, Г=20. Якщо О< Г тоді S = (О+N)-Г = (14+26)-20 = 20

2. N=26, О=14, Г=10. S = (14 - 10) = 4

3. S = (Г - О) Аналогічно як в 2.

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Варіант	Формула	Текст для шифрування
1.	S = (О + Г)modN	Вимоги безпеки до технологічного обладнання та процесів
2.	S = (О - Г)	Для створення шифрованого тексту на вихідний накладається гама.
3.	S = (Г - О)	Атака, що має на меті змусити сервер не відповідати на запити
4.	S = (О + Г)modN	Безліч людей розмовляють в масштабі реального часу шляхом набору повідомлень на клавіатурі
5.	S = (О - Г)	Сьогодні є чимало каналів просочування інформації з організації
6.	S = (Г - О)	У першій частині розглядаються загальні проблеми безпеки інформаційних систем
7.	S = (О + Г)modN	У другій частині увага приділяється методам та засобам можливого вирішення цих проблем
8.	S = (О - Г)	Роль інформації в сучасному світі та необхідність її захисту
9.	S = (Г - О)	Разом з поняттям інформація, важливе значення має поняття дані
10.	S = (О + Г)modN	Від інформації дані відділяються конкретною формою подань.
11.	S = (О - Г)	Інформація на стадії даних характеризується певною формою подання й додатковою характеристикою
12.	S = (Г - О)	Нематеріальність інформації полягає у тому, що не можна виміряти параметри відомими фізичними методами
13.	S = (О + Г)modN	Таким чином, інформація зберігається і передається на матеріальних носіях
14.	S = (О - Г)	Все що є матеріальним об’єктом, інформацією бути не може
15.	S = (Г - О)	Інформація не може існувати сама по собі, у відриві від матеріального носія
16.	S = (О + Г)modN	Матерія ж не може не нести інформації, оскільки завжди перебуває в певному стані
17.	S = (О - Г)	Матеріальними носіями інформації можуть бути мозок людини, звукові та електромагнітні хвилі
18.	S = (Г - О)	Інформація, якщо вона міститься на матеріальному носієві, доступна людині.

19.	S = (О + Г)modN	Цінність інформації визначається мірою її корисності для власника
20.	S = (О - Г)	Якщо доступ до інформації обмежується, то така інформація є конфіденційною
21.	S = (Г - О)	Для позначення цінності конфіденційної комерційної інформації використовується категорія конфіденційно
22.	S = (О + Г)modN	Інформацію правочинно розглядати як товар, що має певну цінність
23.	S = (О - Г)	Кількість інформації тим більша, чим нижча ймовірність події
24.	S = (Г - О)	Підхід ентропії широко використовується при визначенні кількості інформації, переданої по каналах зв'язку
25.	S = (О + Г)modN	Тезарусний підхід заснований на розумінні інформації як знань
26.	S = (О - Г)	У результаті копіювання без зміни інформаційних параметрів носія кількість інформації не змінюється, а ціна зменшується
27.	S = (Г - О)	Проблеми захисту інформації непокоїли людство з давніх-давен

ЗАВДАННЯ НА САМОСТІЙНУ ПІДГОТОВКУ

Реалізувати програмно варіант завдання. Продемонструвати викладачу робочу програму та отримати додатково 3 бали в рейтинг-лист.

КОНТРОЛЬНІ ПИТАННЯ

1. Які недоліки притаманні моноалфавітним криптографічним алгоритмам?
2. У чому складність використання такого роду криптографічних алгоритмів?