ЗАВДАННЯ ДО РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ З ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»

1. Базові операції шифрування: підстановки та перестановки.

1.1. Зашифрувати повідомлення[1] шифром Цезаря із заданим ключем.

№ варіанту	відкритий текст	ключ шифрування
1.	interface	3
2.	procedure	5
3.	function	7
4.	program	9
5.	network	11
6.	substitution	13
7.	permutation	15
8.	cipher	17
9.	solution	2
10.	encryption	4
11.	decryption	6
12.	evolution	8
13.	protocol	10
14.	message	12
15.	project	14
16.	signature	16
17.	website	18
18.	mathematics	1
19.	tester	19
20.	digital	20
21.	software	5
22.	developer	7
23.	statistics	9
24.	library	11
25.	hardware	4

1.2. Згідно з ключовим словом зашифрувати шифром Віженера фразу "In God we trust the rest we test".

№ варіанту	ключове слово
1.	interface
2.	procedure
3.	function
4.	program
5.	network
6.	substitution
7.	permutation
8.	cipher

[1] У всіх завданнях відкритий текст записувати малими літерами без пробілів, а шифрований – великими літерами без пробілів.

9.	solution
10.	encryption
11.	decryption
12.	evolution
13.	protocol
14.	message
15.	project
16.	signature
17.	website
18.	mathematics
19.	tester
20.	digital
21.	software
22.	developer
23.	statistics
24.	library
25.	hardware

1.3. Згідно з ключем зашифрувати методом перестановок фразу "In God we trust the rest we test".

№ варіанту	ключ
1.	54321
2.	45321
3.	53421
4.	35421
5.	54231
6.	52431
7.	25431
8.	54312
9.	54132
10.	51432
11.	15432
12.	14325
13.	41325
14.	13425
15.	31425
16.	13245
17.	13254
18.	13452
19.	52341
20.	25341
21.	52314
22.	51342
23.	51423
24.	13524
25.	15243

Довідковий матеріал.

Таблиця Віженера.

	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**
a	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
b	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	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

2. Блокові шифри. Алгоритм "спрощений DES".

2.1. Згідно варіанту обчислити шифрований алгоритмом S-DES[2] текст C від відкритого тексту M та ключа K – $C_1 = E_K(M)$. У звіті подати проміжні результати виконання кожної операції. Провести операцію дешифрування і переконатись в коректності роботи алгоритму.

2.2. Обчислити шифрований текст від інвертованого вхідного тексту – $C_2 = E_K(\overline{M})$.

2.3. Обчислити шифрований текст від інвертованого вхідного тексту та інвертованого ключа – $C_3 = E_{\overline{K}}(\overline{M})$.

2.4. Зробити висновки з отриманих результатів.

№ варіанту	відкритий текст	ключ шифрування
1.	11110111	1010000010
2.	10011001	1010101010
3.	11111111	1111111111
4.	00000000	1111100000
5.	00001111	1111100000
6.	10100101	1111111111
7.	10100011	1111111111
8.	10010110	1000110001
9.	01011011	1111111111
10.	10010110	1011010010
11.	00000000	0000000000
12.	11101010	0111111101
13.	00010011	0111111101
14.	11001100	0111111101
15.	00110011	1100110001
16.	00100011	1100110001
17.	00110011	1100110011
18.	10000001	1000000001
19.	11011011	1011010010
20.	00110000	1011010010
21.	01010100	1011010010
22.	01000110	1101110100
23.	00011101	1101110100
24.	10101001	1101110100
25.	10010000	0111111111

[2] Детальний опис алгоритму S-DES можна знайти, наприклад, за посиланням https://www.c-sharpcorner.com/article/s-des-or-simplified-data-encryption-standard/ або https://intuit.ru/studies/courses/553/409/lecture/17872

3. Криптографія з відкритим ключем. Алгоритм RSA.

3.1. Дано два простих числа p та q. Згідно варіанту обчислити шифрований публічним ключем текст C від відкритого тексту M за алгоритмом RSA. В якості параметра e обрати мінімальне значення. У звіті подати проміжні результати виконання кожної операції. Провести операцію дешифрування і переконатись в коректності роботи алгоритму.

№ варіанту	M	p	q
1.	22	2	19
2.	63	3	23
3.	81	5	17
4.	14	7	11
5.	101	11	13
6.	57	13	7
7.	117	17	13
8.	33	19	3
9.	39	23	2
10.	47	2	29
11.	21	3	17
12.	98	5	29
13.	105	7	19
14.	30	11	3
15.	61	13	5
16.	157	17	11
17.	93	19	5
18.	77	23	5
19.	19	2	17
20.	78	3	29
21.	44	5	11
22.	116	7	23
23.	109	11	19
24.	189	13	19
25.	91	17	7

4. Обмін ключами шифрування. Схема Діффі–Хеллмана.

4.1. Дано просте число q, його первісний корінь α, та секретні значення користувачів *A* і *B* – X_A та X_B відповідно. Обчислити секретні ключі шифрування користувачів *A* та *B*.

№ варіанту	q	α	X_A	X_B
1.	19	10	8	17
2.	19	2	3	11
3.	19	3	7	15
4.	19	13	13	4
5.	19	14	9	13
6.	19	15	11	6
7.	17	3	13	7
8.	17	5	5	14
9.	17	6	7	12
10.	17	7	16	4
11.	23	5	19	3
12.	23	7	17	5
13.	23	10	13	4
14.	23	11	15	8
15.	23	14	11	9
16.	23	15	21	4
17.	23	17	10	12
18.	23	19	12	18
19.	13	2	3	7
20.	13	6	4	8
21.	13	7	5	9
22.	13	11	6	10
23.	11	6	3	10
24.	11	7	5	9
25.	11	8	7	8

5. Розрахунок дайджесту повідомлення за допомогою простих хеш-функцій.

5.1. Згідно варіанту обчислити дайджест повідомлення[3] ***Криптографія*** з використанням однієї з простих хеш-функцій. Результати подати у шістнадцятковому форматі. Змінити першу літеру повідомлення на малу та порахувати дайджест. Порівняти отримані результати.

№ варіанту	Функція	Напрям зсуву	Розрядність зсуву	Довжина хешу, біт
1.	XOR	–	–	8
2.	XOR	–	–	16
3.	XOR	–	–	32
4.	XOR	–	–	64
5.	RXOR	L	1	8
6.	RXOR	L	1	16
7.	RXOR	L	1	32
8.	RXOR	L	1	64
9.	RXOR	L	2	8
10.	RXOR	L	2	16
11.	RXOR	L	2	32
12.	RXOR	L	2	64
13.	RXOR	R	1	8
14.	RXOR	R	1	16
15.	RXOR	R	1	32
16.	RXOR	R	1	64
17.	RXOR	R	2	8
18.	RXOR	R	2	16
19.	RXOR	R	2	32
20.	RXOR	R	2	64
21.	RXOR	L	3	16
22.	RXOR	L	3	32
23.	RXOR	L	3	64
24.	RXOR	R	3	16
25.	RXOR	R	3	32

[3] При виконанні завдання вважати, що текст кодується 16-бітними символами Unicode.

Довідковий матеріал.

Таблиця символів Unicode (фрагмент).

Код	Символ	Код	Символ
0×0410	А	0×0430	а
0×0411	Б	0×0431	б
0×0412	В	0×0432	в
0×0413	Г	0×0433	г
0×0414	Д	0×0434	д
0×0415	Е	0×0435	е
0×0401	Ё	0×0451	ё
0×0416	Ж	0×0436	ж
0×0417	З	0×0437	з
0×0418	И	0×0438	и
0×0419	Й	0×0439	й
0×041A	К	0×043A	к
0×041B	Л	0×043B	л
0×041C	М	0×043C	м
0×041D	Н	0×043D	н
0×041E	О	0×043E	о
0×041F	П	0×043F	п
0×0420	Р	0×0440	р
0×0421	С	0×0441	с
0×0422	Т	0×0442	т
0×0423	У	0×0443	у
0×0424	Ф	0×0444	ф
0×0425	Х	0×0445	х
0×0426	Ц	0×0446	ц
0×0427	Ч	0×0447	ч
0×0428	Ш	0×0448	ш
0×0429	Щ	0×0449	щ
0×042A	Ъ	0×044A	ъ
0×042B	Ы	0×044B	ы
0×042C	Ь	0×044C	ь
0×042D	Э	0×044D	э
0×042E	Ю	0×044E	ю
0×042F	Я	0×044F	я
0×0404	Є	0×0454	є
0×0406	І	0×0456	і
0×0407	Ї	0×0457	ї

Прості функції хешування.

Всі функції хешування побудовані на наступних загальних принципах. Введене значення (повідомлення, файл і т.д.) розглядається як послідовність n-бітових блоків. Введені дані обробляються послідовно блок за блоком, щоб у результаті отримати n-бітове значення функції хешування.

Однією з найпростіших функцій хешування є зв'язування всіх блоків операцією порозрядного «виключного АБО» (XOR). Це можна записати в наступному вигляді:

$$C_i = b_{i1} \oplus b_{i2} \dots \oplus b_{im}$$

де
C_i – i-й біт хеш-коду, $1 \leq i \leq n$,
m – кількість n-бітових вхідних блоків,
b_{ij} – i-й біт в j-ому блоці,
$\oplus$ – операція XOR.

Найпростіше удосконалення такої схеми полягає у виконанні однобітового циклічного зсуву значення функції хешування після завершення обробки кожного чергового блоку.

Така процедура складається з наступних етапів:

1) Початкова ініціалізація n-бітового значення функції хешування нульовим значенням.
2) Послідовна обробка n-бітових блоків даних за наступним правилом:
    a. Виконання циклічного зсуву поточного значення функції хешування вліво (або вправо) на один біт.
    b. Додавання значення поточного блоку до значення функції хешування за допомогою операції XOR.