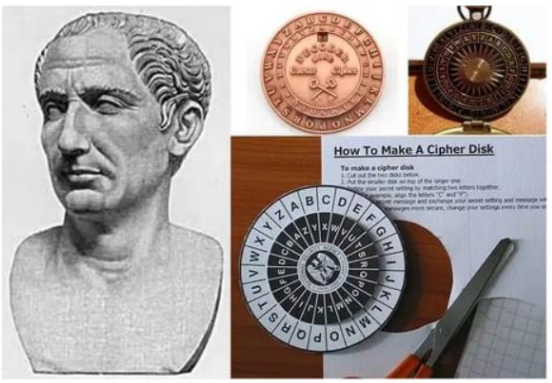
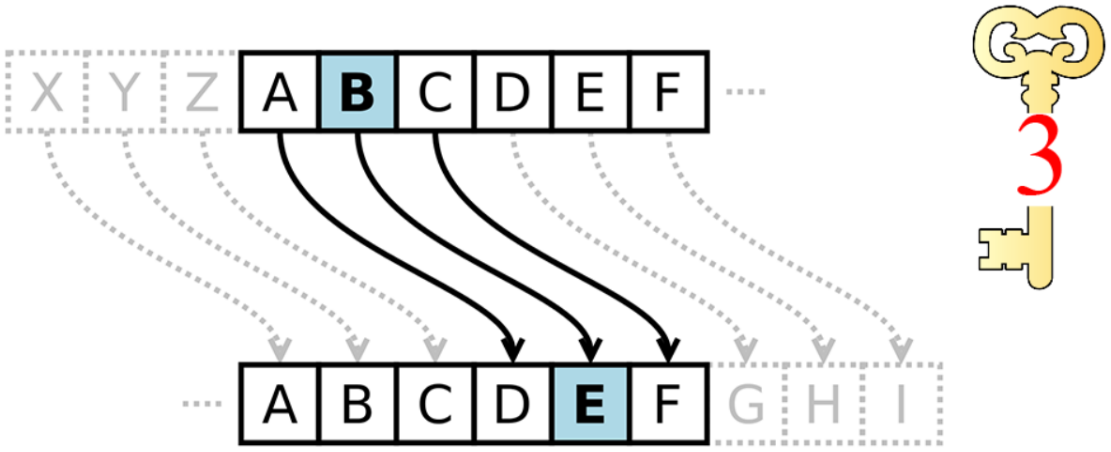
Уроки 24 і 25. Шифр Цезаря

Вивчення нового матеріалу

Слайд № 1	Сьогодні ми перетворимося на справжніх секретних агентів. І створимо проект для шифрування повідомлень. Зараз одним із найпростіших вважається шифр Цезаря, однак за часів Давнього Риму цей шифр не міг розшифрувати ніхто і ним користувався навіть імператор Юлій Цезар для приватного листування. 
Слайд № 2	Зашифрувати повідомлення – це все одно, як замкнути його в скрині: прочитати його зможе лише той, хто має ключ   Ключем називають невеликий обсяг інформації, за допомогою якого шифрують та розшифровують повідомлення.

Слайд № 3

Принцип шифрування за допомогою шифру Цезаря: кожну літеру тексту замінити на ту, яка в алфавіті від неї на k літер далі. k – це ключ.



Тут ключ = 3

Слайд № 4

Ми запрограмуємо такий варіант шифру Цезаря:

під час шифрування кожна літера замінюється іншою, що розташована від неї на відстані k в таблиці символів Unicode.

Величина k – це і є ключ.

літера	а	б	в	г	д	е	ж	з	и	й
код	1072	1073	1074	1075	1076	1077	1078	1079	1080	1081
літера	к	л	м	н	о	п	р	с	т	у
код	1082	1083	1084	1085	1086	1087	1088	1089	1090	1091
літера	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
код	1092	1093	1094	1095	1096	1097	1098	1099	1100	1101
літера	ю	я	è	ё	ђ	ѓ	є	ѕ	і	ї
код	1102	1103	1104	1105	1106	1107	1108	1109	1110	1111
літера	ј	љ	њ	ћ	ќ	ѝ	ў	џ	Ѡ	ѡ
код	1112	1113	1114	1115	1116	1117	1118	1119	1120	1121
літера	Ѣ	ѣ	Ѥ	ѥ	Ѧ	ѧ	Ѩ	ѩ	Ѫ	ѫ
код	1122	1123	1124	1125	1126	1127	1128	1129	1130	1131
літера	Ѭ	ѭ	Ѯ	ѯ	Ѱ	ѱ	Ѳ	ѳ	Ѵ	ѵ
код	1132	1133	1134	1135	1136	1137	1138	1139	1140	1141

Слайд № 5

Наприклад, зашифруємо у такий спосіб слово “шифрування”

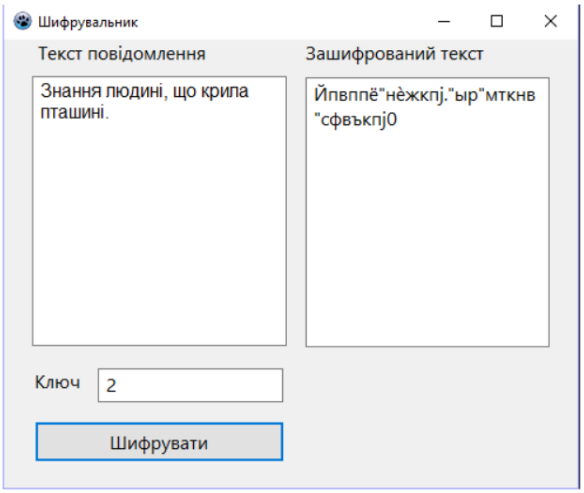
Ключ шифру k = 2.

літера	а	б	в	г	д	е	ж	з	и	й
шифр	в	г	д	е	ж	з	и	й	к	л
літера	к	л	м	н	о	п	р	с	т	у
шифр	м	н	о	п	р	с	т	у	ф	х
літера	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
шифр	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
літера	ю	я	è	ë	ђ	ѓ	є	ѕ	і	ї
шифр	è	ë	ђ	ѓ	є	ѕ	і	ї	ј	љ
літера	ј	љ	њ	ћ	ќ	ѝ	ў	џ	Ѡ	ѡ
шифр	њ	ћ	ќ	ѝ	ў	џ	Ѡ	ѡ	Ѣ	ѣ
літера	Ѣ	ѣ	Ѥ	ѥ	Ѧ	ѧ	Ѩ	ѩ	Ѫ	ѫ
шифр	Ѥ	ѥ	Ѧ	ѧ	Ѩ	ѩ	Ѫ	ѫ	Ѭ	ѭ
літера	Ѭ	ѭ	Ѯ	ѯ	Ѱ	ѱ	Ѳ	ѳ	Ѵ	ѵ
шифр	Ѯ	ѯ	Ѱ	ѱ	Ѳ	ѳ	Ѵ	ѵ	←	на 2

Відповідь: ъкцтхдвппё

Слайд № 6

Загальний вигляд форми проекту буде таким:

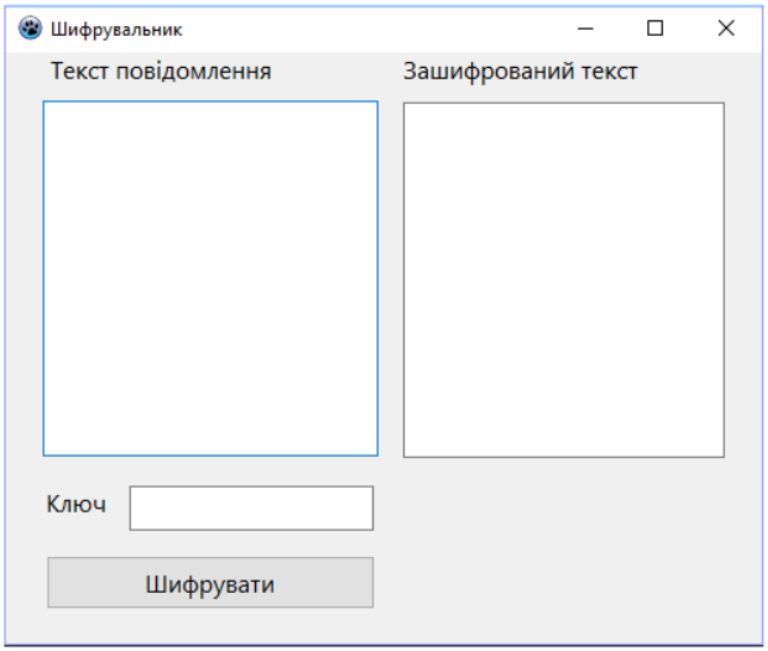


Вправа

Вправа № 1

Вправа 1 у Lazarus

Створіть форму згідно зразка



Вивчення нового матеріалу

Слайд № 7

Отже, ми визначили, що для шифрування рядка s1 необхідно для кожного символу виконати такі два кроки:

1) визначити код символу та додати до нього ключ;
2) одержати значеннння символу за його кодом та дописати його до шифрованого тексту.

Для визначення коду символу використовується функція ord(x), де x – символ

Для визначення символу Unicode за його кодом – widechar(y), де y – код символу

Наприклад,
ord('a')=97
widechar(97)='a'

Вправа № 2

Вправа 2 у Lazarus

Оголосіть змінні проекту:

s1, s2 – текст, який містять поля Memo1 та Memo2;

key – ключ шифру;

i – лічильник циклу;

n – кількість символів рядка s1;

kod – значення коду символу.

Підказка до вправи № 2

Підказка до вправи 2

Оголошення змінних виконайте після службового слова Var

Вправа № 3

Вправа 3 у Lazarus

Запишіть код обробника події натискання кнопки Шифрувати та перевірте правильність його виконання.

Алгоритм:

1. Присвоїти змінній key значення ключа, що міститься в полі Edit1.
2. Присвоїти змінній s1 текст, який містить поле Memo1.
3. Присвоїти змінній n довжину рядка s1.
4. Присвоїти змінній s2 порожній рядок.
5. Записати код шифрування кожного символу і присвоєння зашифрованого тексту змінній s2.
6. Вивести рядок s2 до поля Memo2.

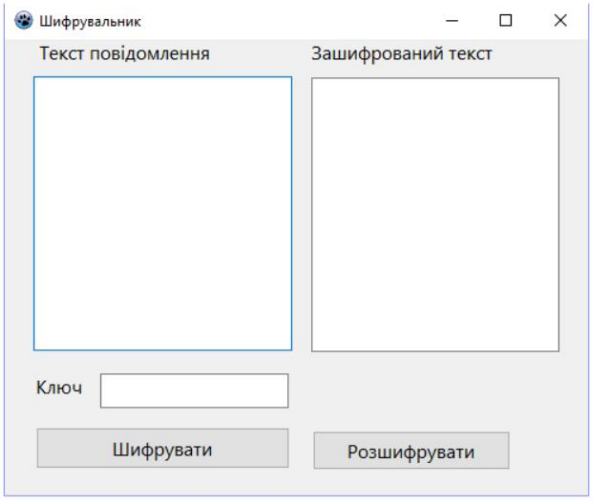
Підказка до вправи № 3

Підказка до вправи 3

Код шифрування i-го символу рядка s1 та дописування його до рядка в змінній s2:

```
kod:=ord(s1[i])+key;
s2:=s2+widechar(kod);
```

Вивчення нового матеріалу

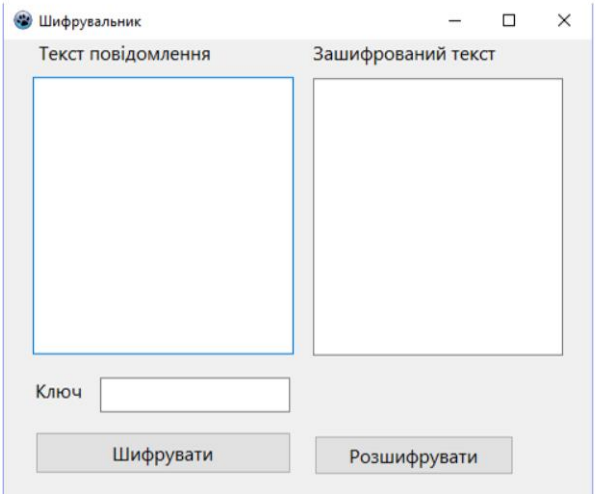
Слайд № 8	Удосконалимо створений проект. Додамо можливість не тільки зашифровувати текст, але і розшифровувати. 
Слайд № 9	Код буде аналогічним зашифруванню за винятком того, що: 1) ключ key не додається, а віднімається; 2) вхідний текст – у Memo2, а вихідний – у Memo1 (під час зашифрування – навпаки).

Вправа

Вправа № 4

Вправа 4 у Lazarus

1. Додайте до форми проекту кнопку Розшифрувати.
2. Уведіть програмний код обробника події кнопки Розшифрувати.
3. Запустіть проект та перевірте правильність його виконання.



Підказка до вправи № 4

Підказка до вправи 4

Скопіюйте код з обробника події кнопки «Зашифрувати» і внесіть деякі зміни:

1) ключ key не додається, а віднімається;
2) вхідний текст – у Memo2, а вихідний – у Memo1 (під час зашифрування – навпаки).

Вивчення нового матеріалу

Слайд № 10

Коли для зашифрованого повідомлення є ключ, то розшифрувати його не становить труднощів.

Але ж що робити, коли ключ невідомий?

Слайд № 11

У цьому випадку звертаються до так званого частотного криптоаналізу.
Його принцип полягає у визначенні частоти появи кожної літери у тексті.

Найкращий спосіб розшифрувати шифр Цезаря – це визначити, який символ у ньому зустрічається найчастіше. Найвірогідніше йому відповідатиме пробіл у початковому тексті, оскільки саме пробіл між словами в українському тексті трапляється частіше за всі інші символи.

Слайд № 12

Проте пробіл не завжди є найбільш уживаним символом в тексті, це може бути і деяка літера.

У таблиці нижче оранжевим виділено літери, які найчастіше зустрічаються у текстах української мови.

а	0,072	ї	0,006	у	0,04
б	0,017	й	0,008	ф	0,001
в	0,052	к	0,035	х	0,012
г	0,016	л	0,036	ц	0,006
д	0,035	м	0,031	ч	0,018
е	0,017	н	0,065	ш	0,012
є	0,008	о	0,094	щ	0,001
ж	0,009	п	0,029	ь	0,029
з	0,023	р	0,047	ю	0,004
и	0,061	с	0,041	я	0,029
і	0,057	т	0,055	пробіл	0,17

Практична робота

Практична робота

Практична робота

1. Напишіть або знайдіть в Інтернеті якесь повідомлення (не менше 7 слів), виберіть ключ (число від 1 до 30), зашифруйте повідомлення та надішліть однокласнику (сусіду, що сидить ліворуч).
2. Отримавши повідомлення від сусіда праворуч, спробуйте його розшифрувати, підібравши ключ.
3. Для цього можете скористатися програмою визначення частот символів у тексті, яку ми створювали на минулому уроці. Дізнавшись, які літери у повідомленні зустрічаються частіше, а які рідше, буде легше здогадатися, яким літерам в незашифрованому тексті вони відповідають і таким чином підібрати ключ.