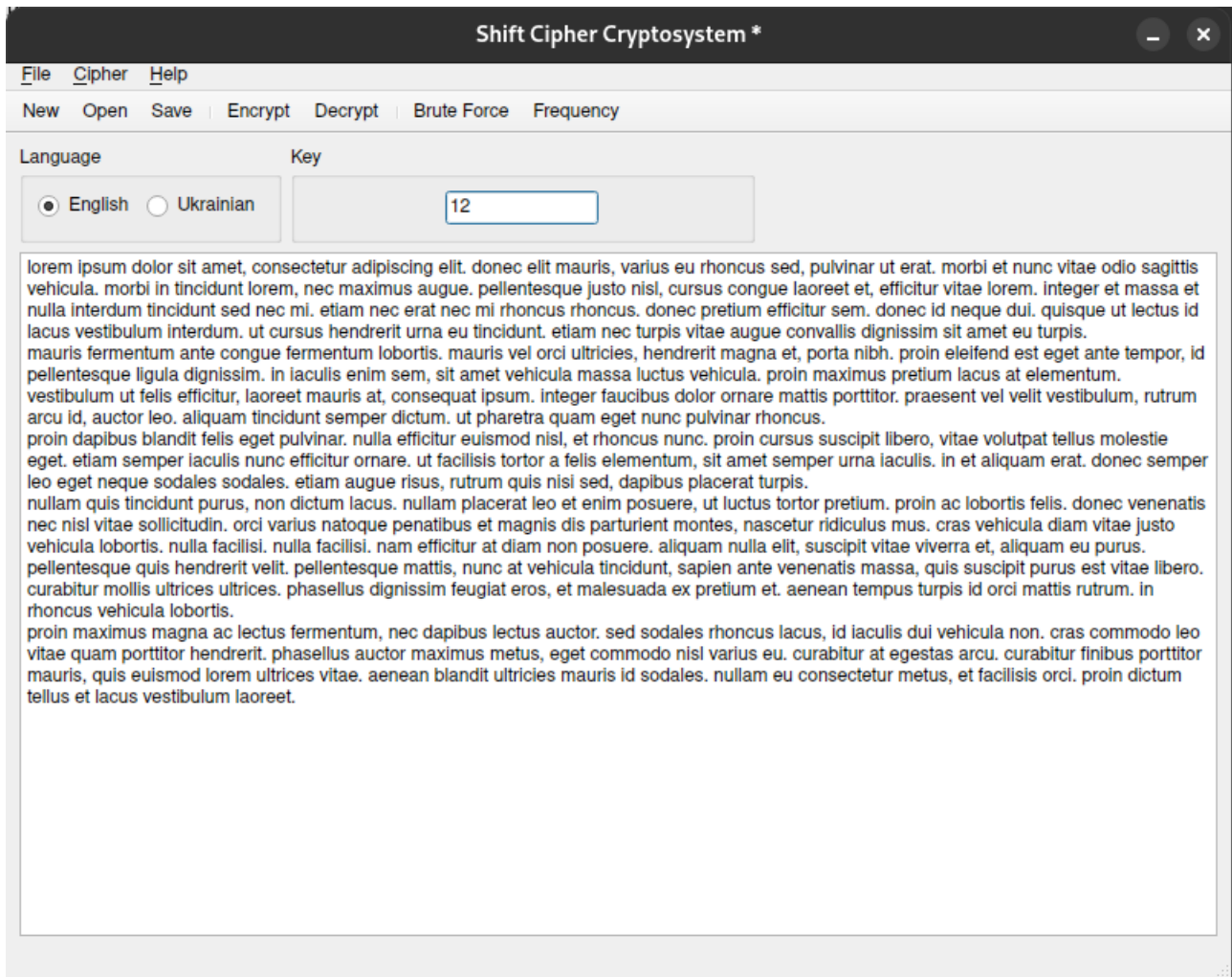


### Інтерфейс криптографічної системи

Головне вікно програми є основним інтерфейсом для взаємодії з користувачем. Воно розділене на кілька основних секцій, кожна з яких надає певний функціонал.



#### Меню бар:

- **File:** Новий файл, відкриття, збереження, друк, вихід.
- **Cipher:** Шифрування, дешифрування, шифрування бінарних файлів, атака brute force, частотний аналіз.
- **Help:** Інформація про програму.

Щоб зашифрувати, достатньо вставити текст, вибрати мову та ввести ключ(крок зсуву)

Shift Cipher Cryptosystem \*

File Cipher Help

New Open Save Encrypt Decrypt Brute Force Frequency

Language

English

Ukrainian

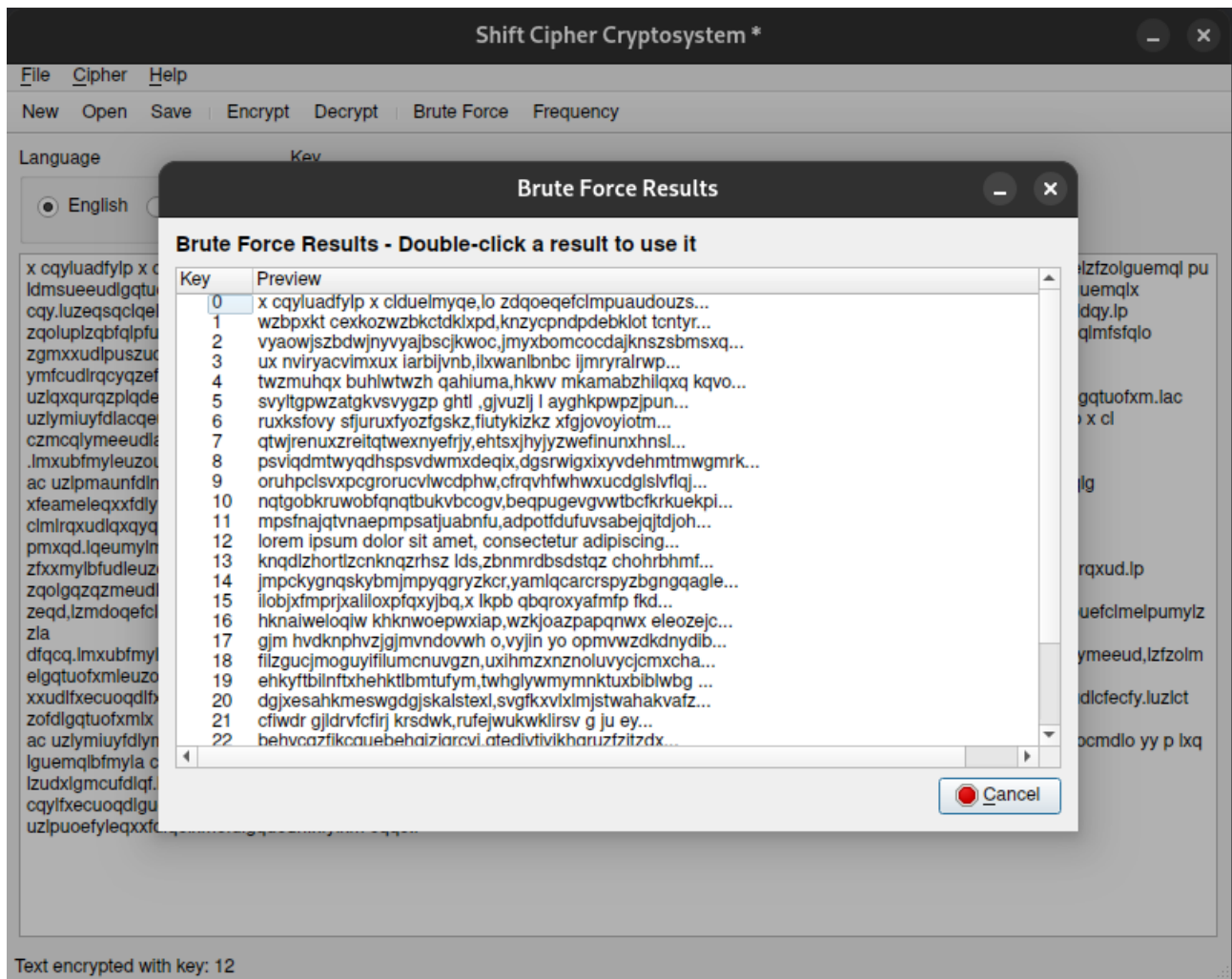
Key

12

x cqyluadfyip x clduelmyqe,lo zdqoeqefclmpuadouzslqxue.lp zqolqxuelymfcud,lgmculdlqfclt zoflddqp,lafxguzmclfelqcme.ly cnulqelzfolguemql pu  
ldmsueeudlqgtuofxm.ly cnuluzleuzoupfzelx cqy,lzqolymiuymfclmfsq.laqxxzeqdbfqlvde lzudx,lofcdldlo zsfqlxm cqqlqe,lqrruouefclguemqlx  
cqy.luzeqsqclqelymddmlqelzfxmlyzeqcpfyleuzoupfzeldqplzqolyu.lqeuymyzqolqcmelzqolyulct zofldict zofd.lp zqolacqeuylqrruouefcldaq.lp  
zqoluplzbqlpftu.lbfudbqlfelxqoefdluplxmofdlgqdeunxfylyzeqcpfy.lfelofcdldltzpcqcuelczmlqfleuzoupfze.lqeuymyzqolefcaudlguemqlmfsqlo  
zgmxxudlpuszuuduylduelmyqelqflecaud.l  
ymfcudlrcyqzefylmzeqlo zsfqlrcyqzefylx n ceud.lymfcudlgqxl coulfxecuouqd,lqzpcqcuelymzmlqe,la cemlzunt.lac  
uzlqxqurqzplqdelqsqelmzeqleqya c,luplaqxxzeqdbfqlxusfxmlypuszudduy.luzlumofxudlqzuyldqy,lduelmyqelggtuofxmlymddmlxfoefdlqgtuofxm.lac  
uzlymiuyfdlacqeuylxmofdlmelqxqyzefy.lgqdeunxfylfelrxudlqrruouefc,lxm cqqelymfcudlme,lo zdqbfmeluadfy.luzeqsqclrmfounfdlp x cl  
czmqclymeeudla ceeue c.lacmqdqzelgqxlqgxeuqdeunxfy,lcfecfymcoflup,lmfoc clxq  
.lmxubfmyleuzoupfzeldqyaqclpuoefy.lfelatmcqecmlbfmylqsqelzfolafxguzmclct zofd.l  
ac uzlpmaunfdlnxmzpuelrxudlqsqelafxguzmc.lzfxxmqlrruouefclqfudy plzudx,lqelct zofldlzfzo.lac uzlofcdldldfouauehxunqc ,lguemqlg  
xfeameleqxxfdly xqdeuqlqsqe.lqeuymldqyaqclumofxudlzfzqlrruouefcl czmqc,lfelrmouxudule ce  
clmlrxudlqxyqzefy,lduelmyqelqyaqclfczmiumofxud.luzlqelmxubfmylqcme.lp zqoldqyaqclxq lqsqelzqbqlq pmxqdl  
pmxqd.lqeuymymfclqcludfd,lcfecfylbfudlzudldqp,lpmaunfdlaxmoqcmelefcaud.l  
zfxmlylbfudleuzoupfzelafcd,lz lzpuoefylxmofdl.lzfxmlyaxmoqcmelxq lqelqzuyia dfqoc,lfelxfoefdle ce clacqeuyl.lac uzlmolx n ceudlrxud.lp  
zqolqgzqzmeudlqoluzdxlguemqlid xxuouefpuz.l coulgmculdizme bflaqzmeunfdlqelymszudlpudlamcefcuqzely  
zeqd,lzmdoqefclcupuofxtdlyfd.locmdlqgtuofxmlypumylguemqlvde lqgtuofxmly n ceud.lzfxxmlyrmouxudu.lzfxxmlyrmouxudu.lzmylqrruouefclmelpumylz  
zla  
dfqoc,lmxubfmylzfxxmlyxue,lfdouaueqguemqlgugqccmlqe,lmxubfmylqlafcd.laqxxzeqdbfqlbfudltzpcqcuelgqxue.laqxxzeqdbfqlymeeud,lzfzolm  
elggtuofxmlyeuzoupfze,ldmauqzlmzeqlgqzqzmeudlymddm,lbfudldfouauelefcdlqdelguemqlxunqc .lofcmnuefcly  
xxudlfxecuodlfxecuod.latmdqxxfdlpuszuuduylrqfsumelqc d,lqelymxqdfmpmlqlacqeuylqe.lmqzmqzleqyafdlecaudiupi coulymeeudlcfecfy.luzlct  
zofldlqgtuofxmly n ceud.l  
ac uzlymiuyfdlymszmilmolxqoefdlrcyqzefy,lzqolpmaunfdlxqoefdlmfoc c.ldqpld pmxqdlct zofldxmofdl,luplumofxudlplfulqgtuofxmly z.locmdlo yy p lxq  
lguemqlbfmyla ceeue cltqzpcqcue.latmdqxxfdlmfoc clymiuyfdlyqefd,lqsqelo yy p  
lzudxlgmculdlqf.lofcmnuefcmlqsdemdlmcof.lofcmnuefcruzunfdla ceeue clymfcud,lbfudlqfudy plx  
cqylfxecuodlguemql.lmqzmqzlnxmzpuelfxecuouqdlmfcudlupl pmxqd.lzfxmlyqlfo zdqoeqefclyqefd,lqelrmouxudul cou.lac  
uzlpuoefyleqxxfdlqelxmofdlgqdeunxfylxm cqqe.l

Text encrypted with key: 12

Ідентично щоб розшифрувати текст.



### Кроки роботи brute force у програмі:

#### 1. Введення тексту:

- Користувач вводить зашифрований текст у текстове поле.

#### 2. Виклик brute force:

- Користувач натискає кнопку "Brute Force" у меню або на панелі інструментів.

#### 3. Перебір ключів:

- Програма бере алфавіт, який відповідає вибраній мові (англійський або український).
- Для кожного ключа від 0 до розміру алфавіту:
  - Виконується дешифрування тексту з використанням поточного ключа.
  - Результат зберігається у списку.

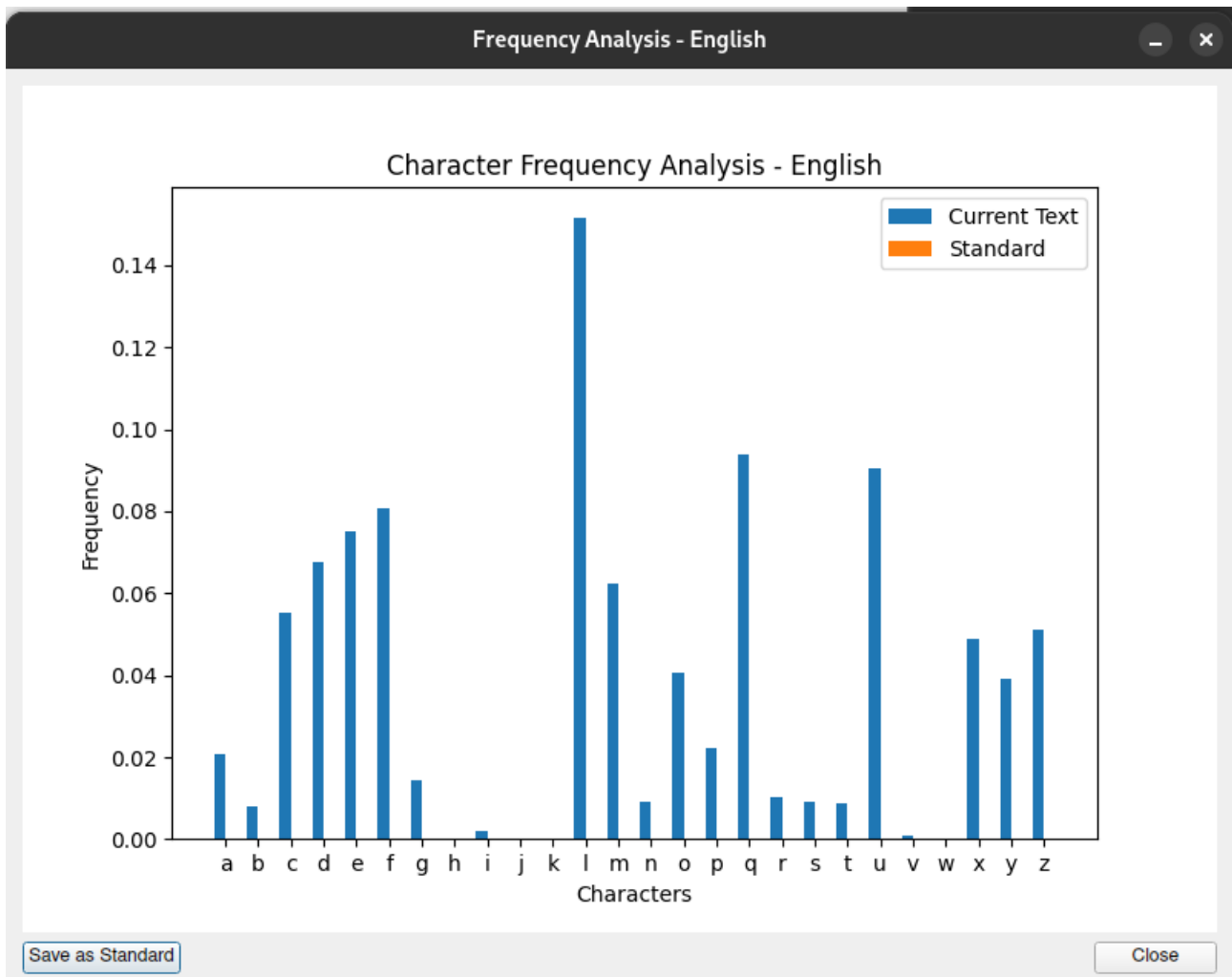
#### 4. Відображення результатів:

- У новому вікні відображається таблиця з усіма можливими ключами та відповідними розшифрованими текстами.
- Кожен рядок містить:
  - **Key (Ключ):** Число, яке було використано для дешифрування.

- **Preview (Попередній перегляд):** Перші 50 символів розшифрованого тексту (якщо текст довший, він обрізається і додається "...").

#### 5. Вибір правильного результату:

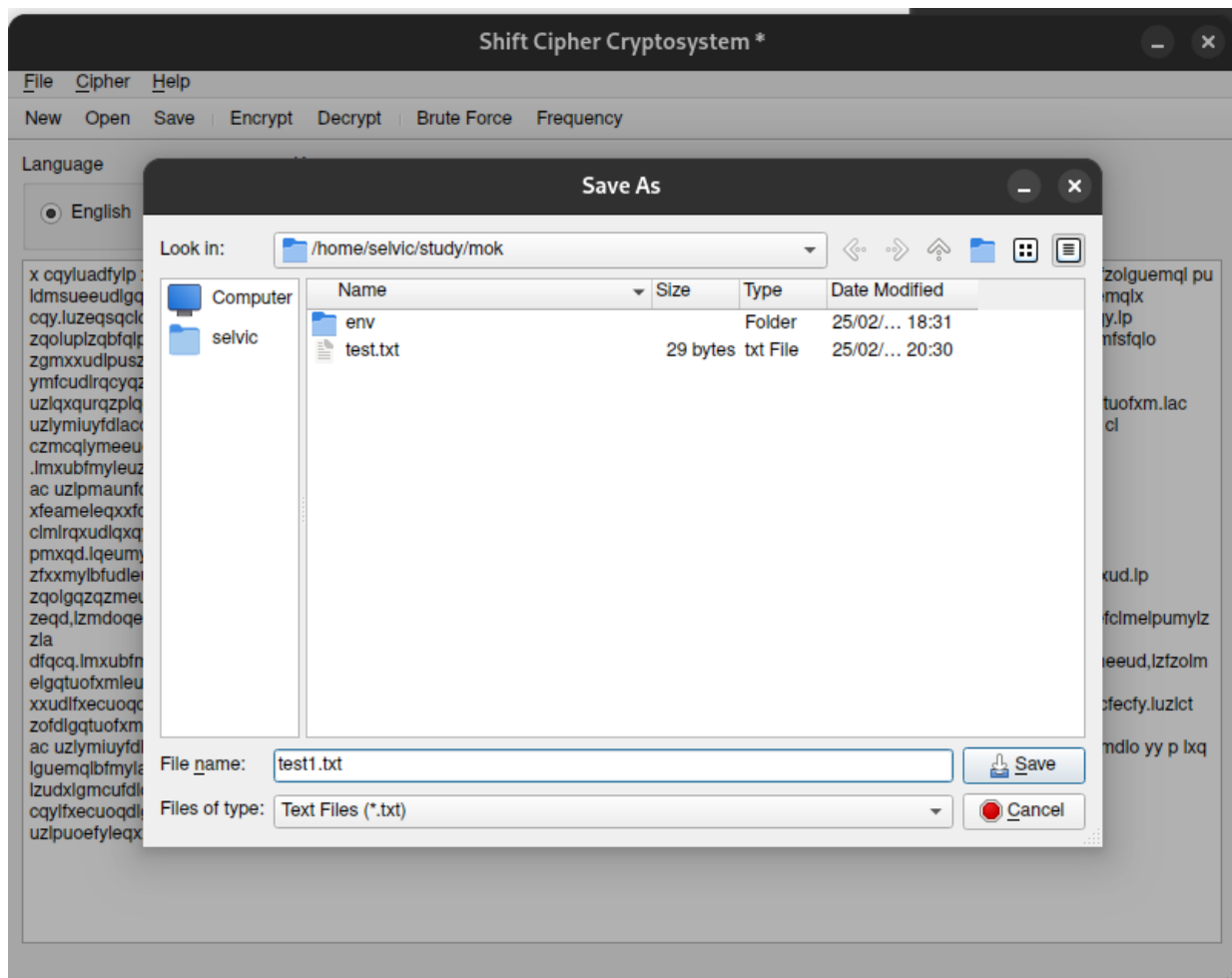
- Користувач може подвійним кліком вибрати рядок з правильним розшифрованим текстом.
- Програма автоматично встановлює вибраний ключ у поле для ключа та вставляє розшифрований текст у текстове поле.



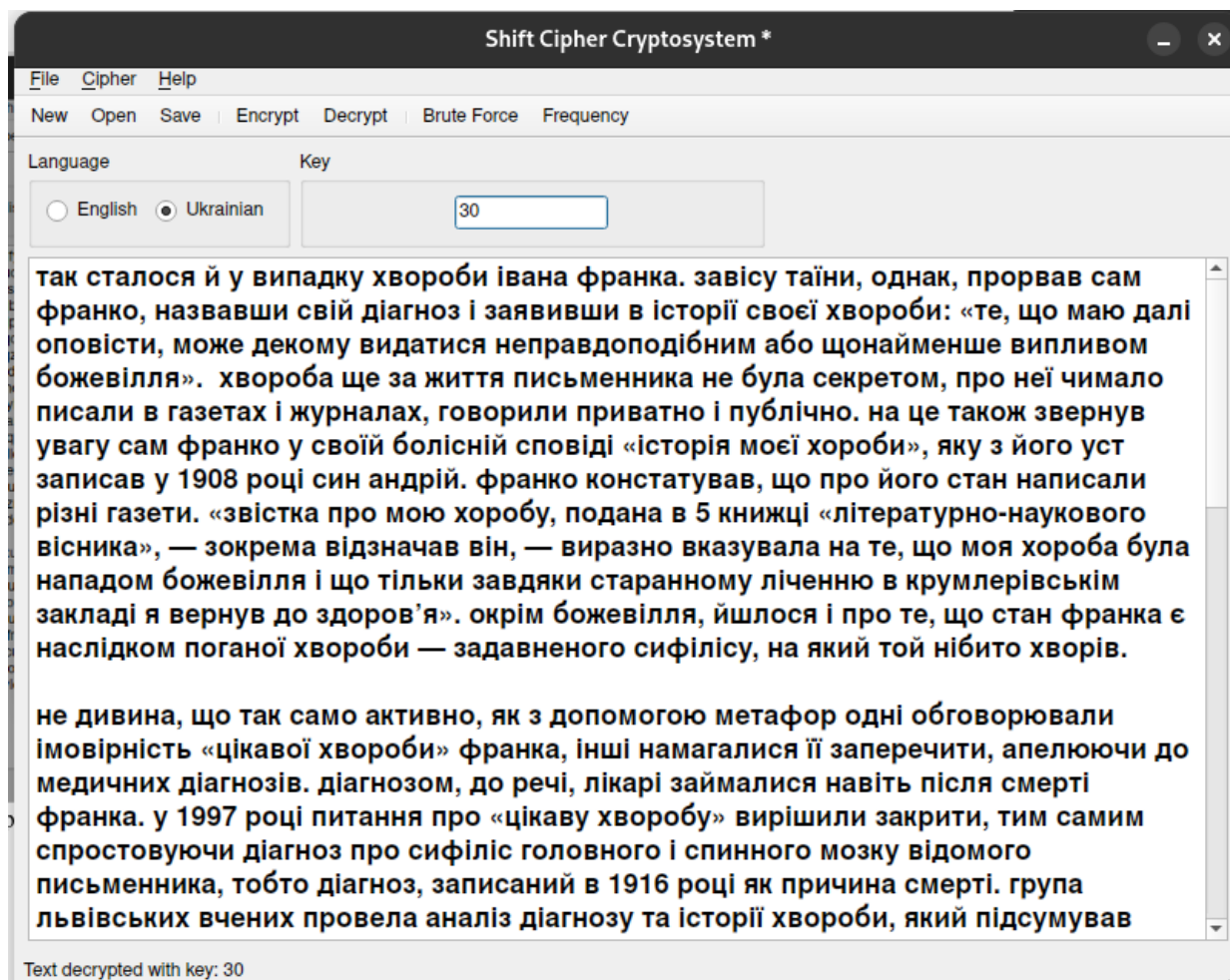
#### Побудова частотної таблиці:

- Програма аналізує текст і рахує, скільки разів кожен символ алфавіту зустрічається у тексті.
- Частота кожного символу обчислюється за формулою:

Частота=Загальна кількість символів у тексті / Кількість входжень символу

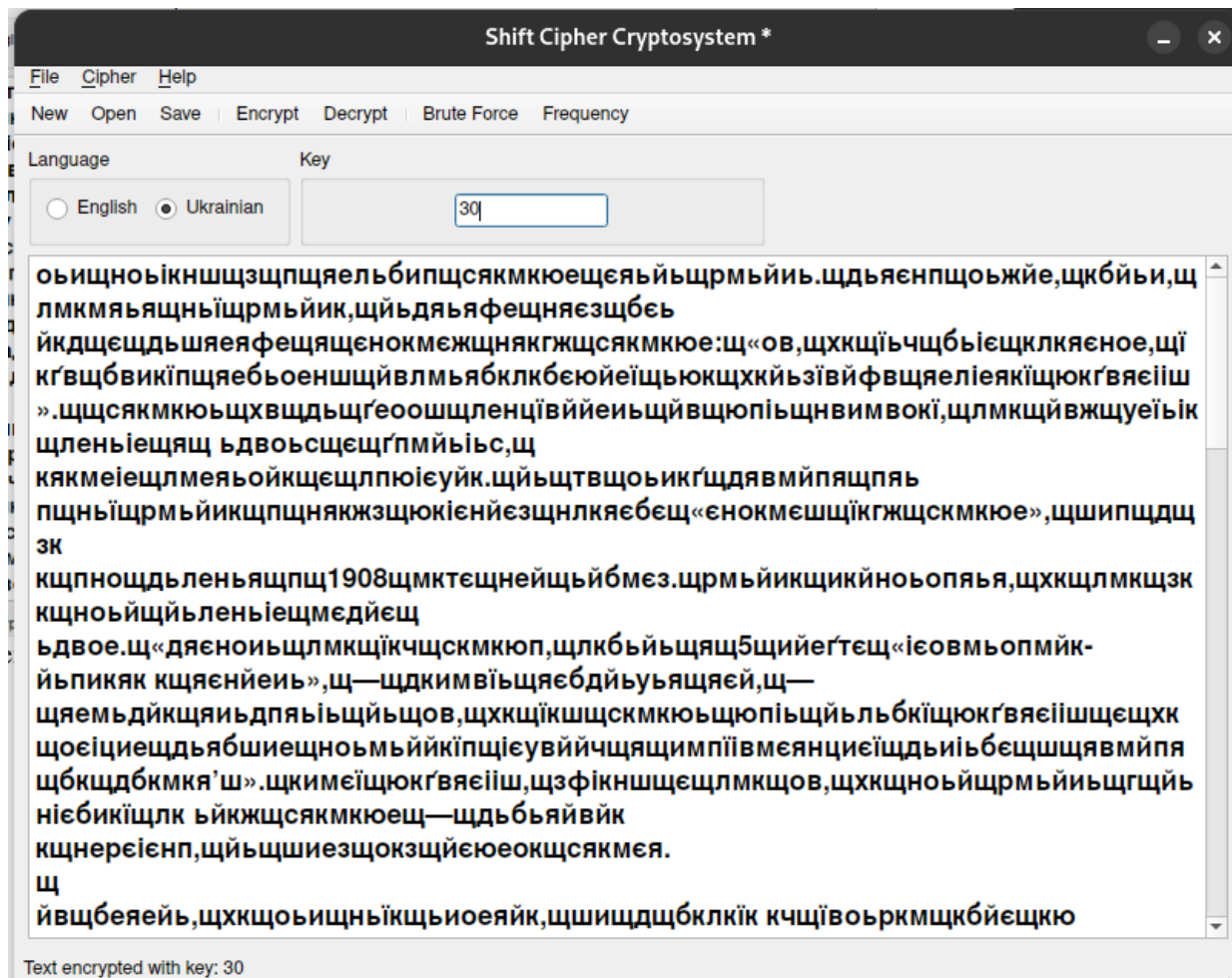


Програма дозволяє як відкривати файли, так зберігати.

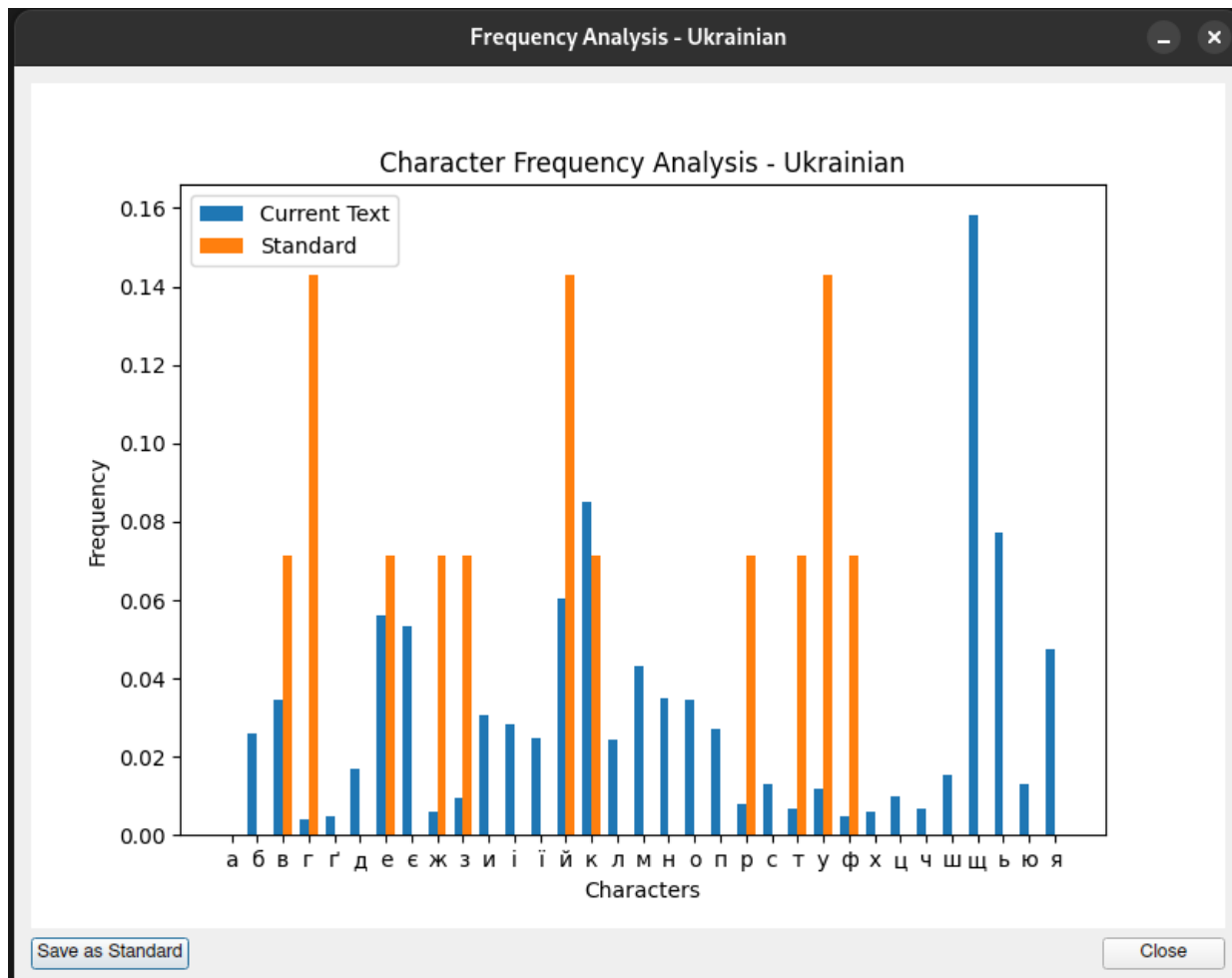


Демонстрація шифрування з українськими символами





Та розшифрування



У цій частотній таблиці ще порівнюється “взята як стандартна таблиця”. Програма дозволяє зберегти частотну таблицю та використовувати її для порівнянь

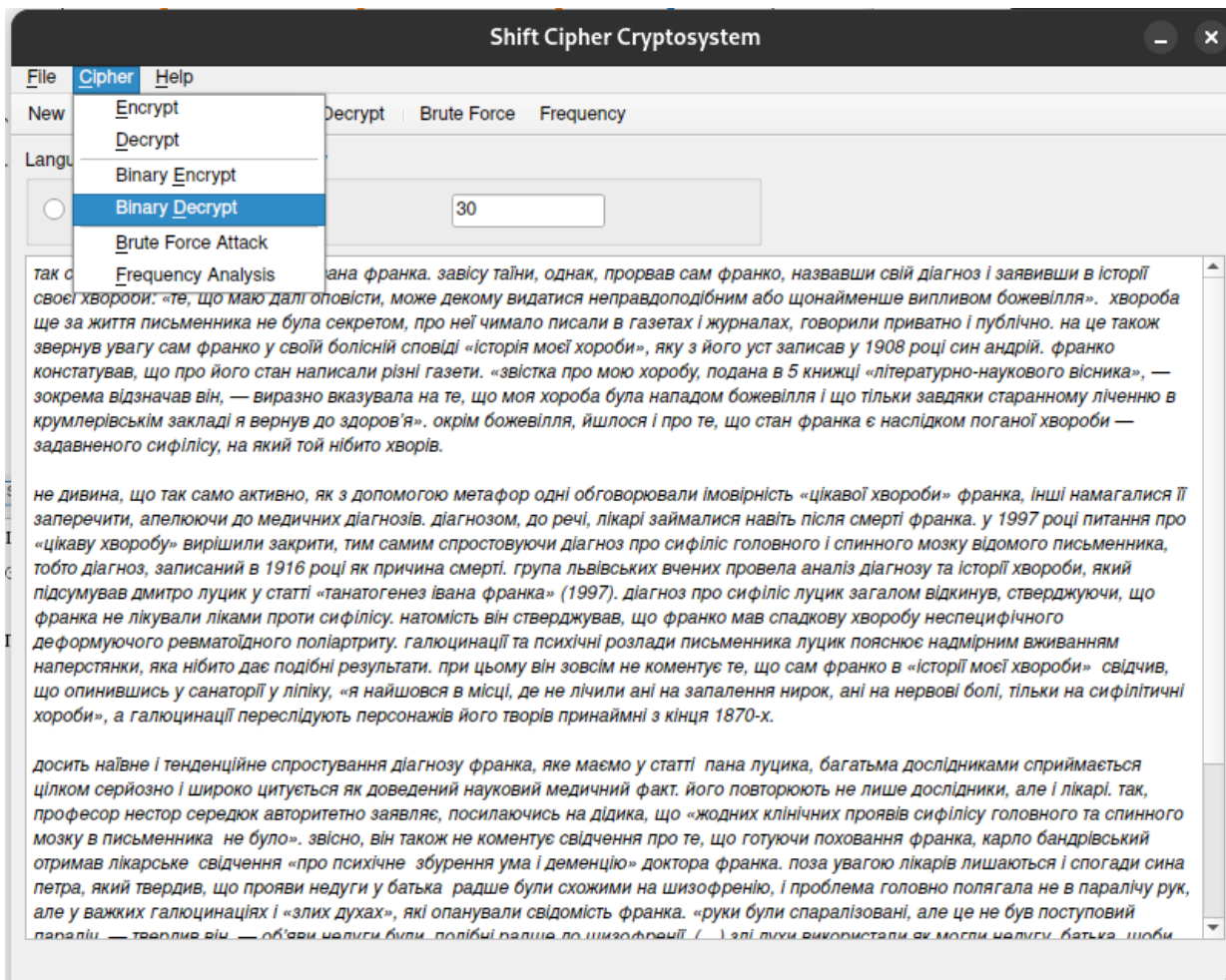
В програмі є можливість шифрування та розшифрування у бінарному форматі.

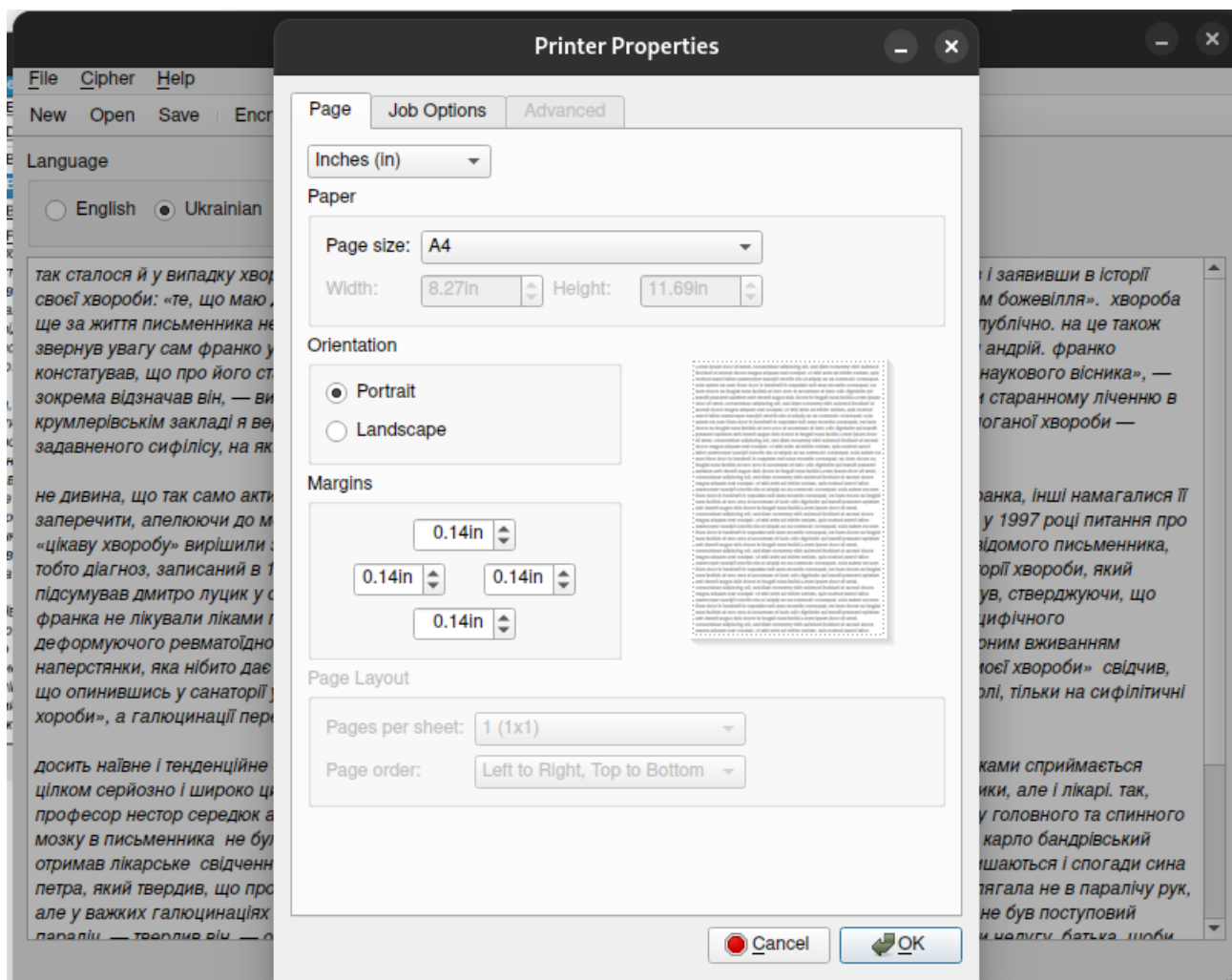
**XOR (виключне АБО):** Це бітова операція, яка повертає 1, якщо вхідні біти різні, і 0, якщо вони однакові.

- Приклад:
  - $0 \text{ XOR } 0 = 0$
  - $0 \text{ XOR } 1 = 1$
  - $1 \text{ XOR } 0 = 1$
  - $1 \text{ XOR } 1 = 0$
- **Ключ:** Ключ — це число, яке використовується для шифрування. У програмі ключ обмежений значенням від 0 до 255 (1 байт).
- **Шифрування:**
  - Кожен байт файлу XOR-иться з ключем.
  - Результат — зашифрований байт.
- **Дешифрування:**



- Зашифрований байт XOR-иться з тим самим ключем.
- Результат — оригінальний байт.





В програму імплементовано функцію друку



Є кнопка “Про програму”, де висвітлюється інформація про розробника