МЕТОД ТА ПРОГРАМНИЙ ЗАСІБ ОБМІНУ ПОВІДОМЛЕННЯМИ В СКОМПРОМЕТОВАНИХ МЕРЕЖАХ

КОРОБЕЙНІКОВ Д. М.

ТРОЯНОВСЬКА Т.І.

Мета, об'єкт, предмет

- **Метою** дослідження магістерської кваліфікаційної роботи є розробити метод та програмний засіб обміну повідомленнями в скомпрометованих мережах.
- **Об’єкт дослідження** – симетричні алгоритми шифрування, криптостійкість паролів та шифрованого тексту.
- **Предмет дослідження** – шифрування за допомогою автоключа, атака типу «підбір пароля».

Завдання

- Проаналізувати сучасний стан розвитку шифрування даних під час передачі їх по публічній мережі;
- Розглянути існуючі методи вирішення задачі обміну повідомленнями в скомпрометованих мережах;
- Побудувати математичну модель криптостійкості пароля та шифрування із автоключем;
- Синтезувати комбінований алгоритм шифрування із динамічним автоключем та визначити стійкість запропонованого алгоритму проти зламу;
- Розробити програмний засіб, що реалізовує алгоритм шифрування із динамічним автоключем;
- Виконати тестування розробленого програмного продукту та провести аналіз отриманих від тестування результатів.

Наукова новизна одержаних результатів та практичне значення

НОВИЗНА

- вперше запропоновано метод обміну повідомленнями в скомпрометованих мережах, що компенсує вразливость до комбінаторної та словникової атаки засобами використання автоключа;
- удосконалено математичну модель криптостійкості пароля та шифрування із автоключем;
- застосовано удосконалений алгоритм кодування із динамічним автоключем із можливістю додатково застосувати комбіноване каскадне кодування.

ПРАКТИЧНЕ ЗНАЧЕННЯ:

- Удосконалено механізми аналізу алгоритму кодування із динамічним автоключем та визначення його криптостійкості.
- Розроблено метод метод обміну повідомленнями в скомпрометованих мережах, що дозволяє протистояти комбінаторним та словниковим атакам.
- Розроблено алгоритм кодування із динамічним автоключем.
- Розроблено програмний засіб обміну повідомленнями в скомпрометованих мережах.

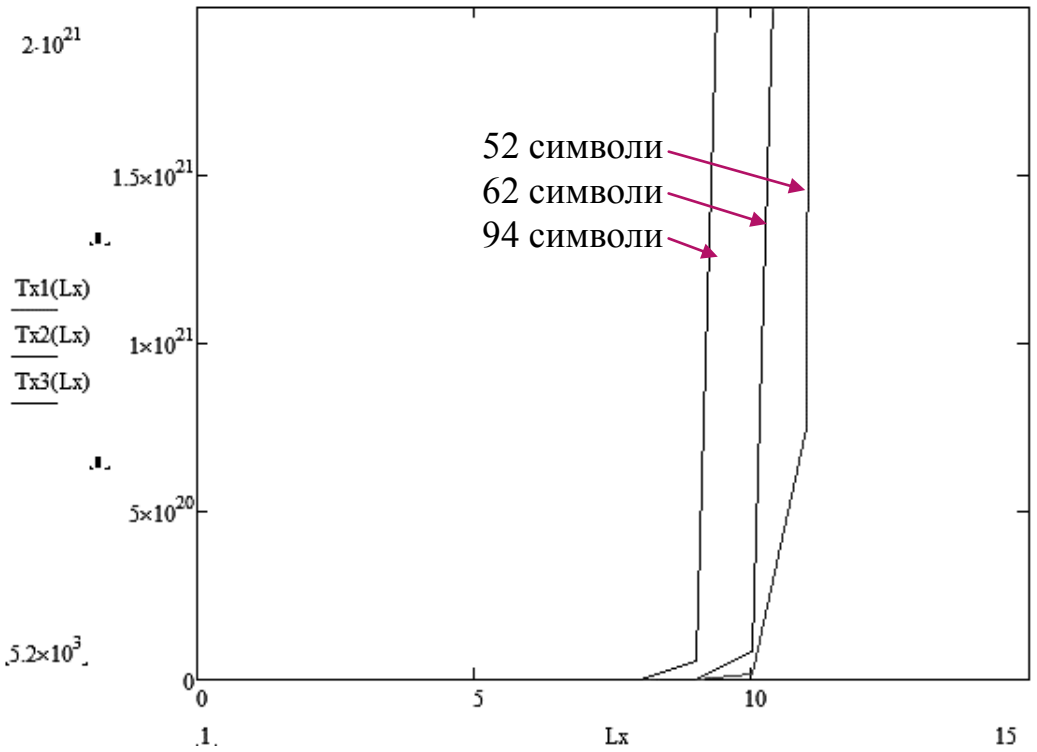
Особистий внесок

- Трояновська Т. І. Оцінка криптостійкості пароля / Т. І. Трояновська, Д. М. Коробейніков // «Інформаційні технології та взаємодії» : IV Міжнародна науково-практична конференція, 8-10 листопада 2017 р. м. Київ. – С. 245-246.
- Трояновська Т. І. Покращення криптостійкості симетричних алгоритмів за допомогою динамічного автоключа / Трояновська Т.І., Коробейніков Д.М. // “Осінні наукові читання” : І Міжн. наук.-практич. інтернет-конференція, 30 листопада 2017 р., м. Дніпро. – С. 11-21.

Модель криптостійкості пароля та шифрування із автоключем

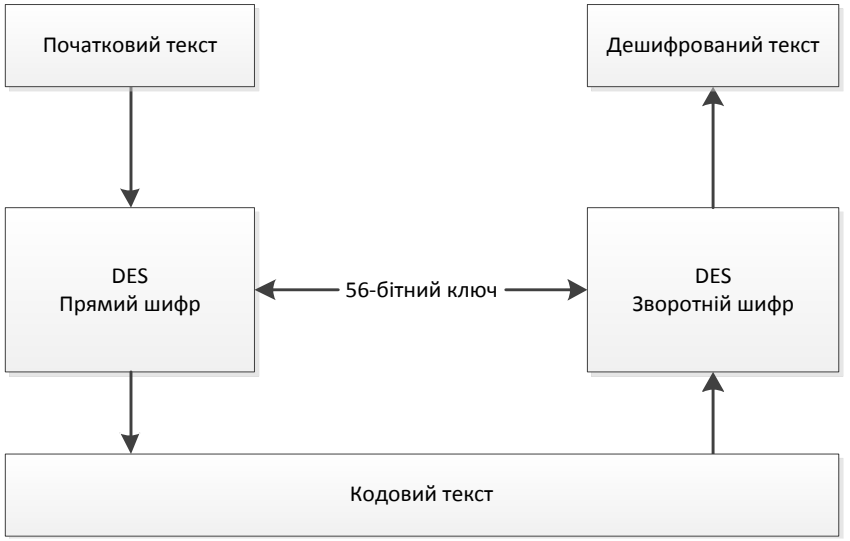
$$\begin{cases} E = \log_2 \sum_{i=k}^{l} A^i \\ k = k - \sum_{j=1}^{p} Len(P_j) + 1 \\ l = l - \sum_{j=1}^{p} Len(P_j) + 1 \end{cases}$$

$$\begin{cases} L = \dfrac{K_P - K_T}{K_0 - K_T} \\ K_0 = \dfrac{\sum_{i=0}^{A} n_i (n_i - 1)}{N(N-1)} \end{cases}$$

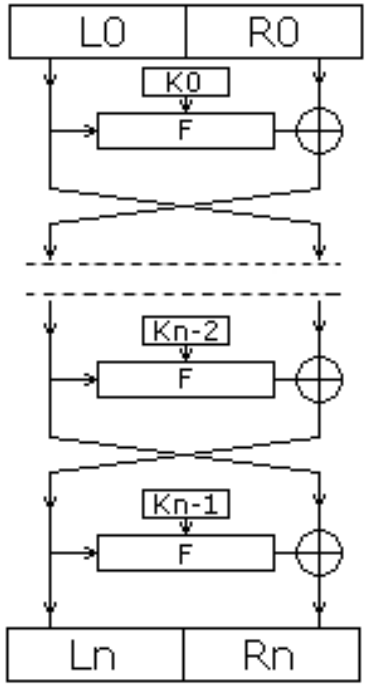


$$E = \log_2 \left(\sum_{i=1}^{l-5} 94^i \right)$$

Метод обміну повідомленнями в скомпрометованих мережах

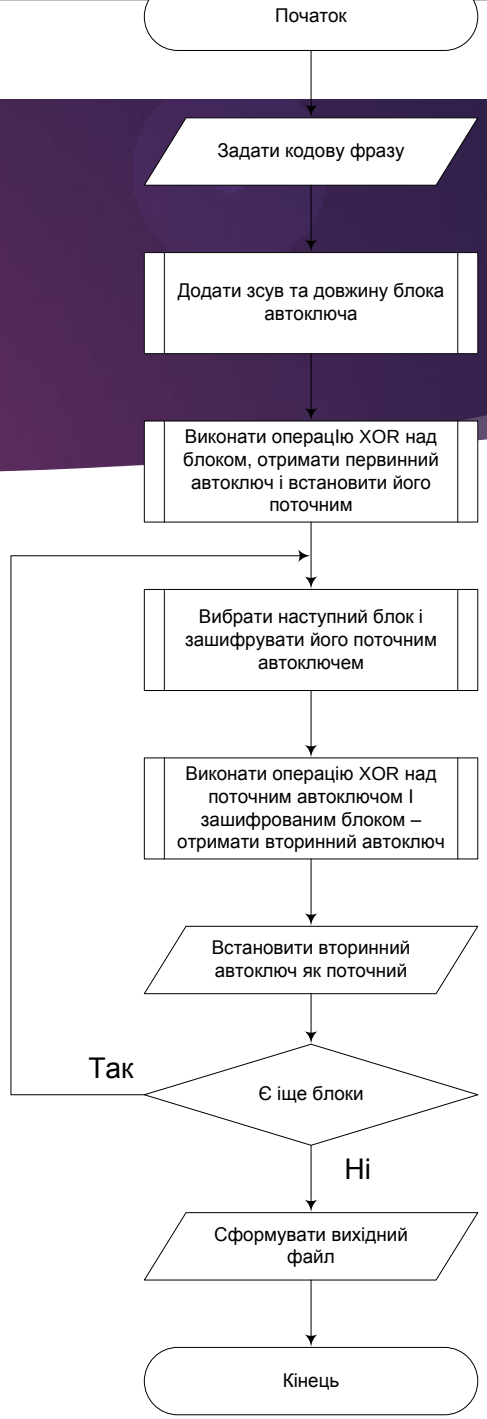


Діаграма шифрування за допомогою DES

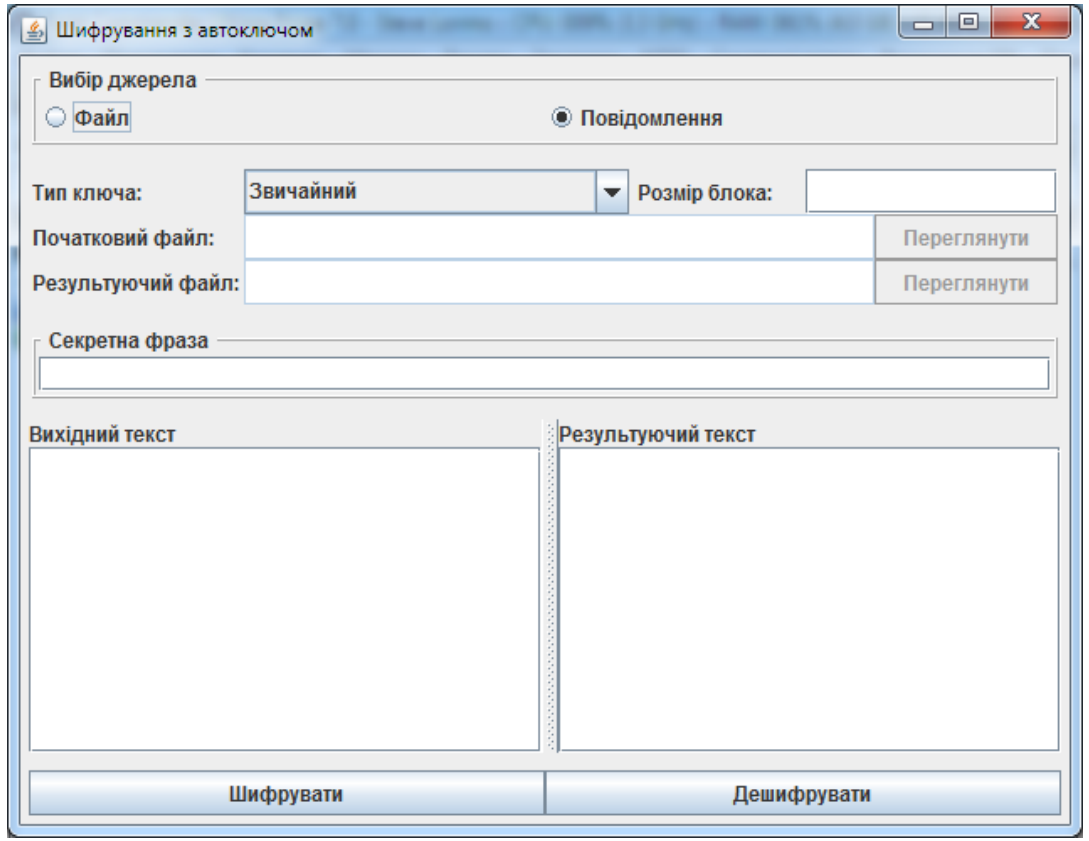


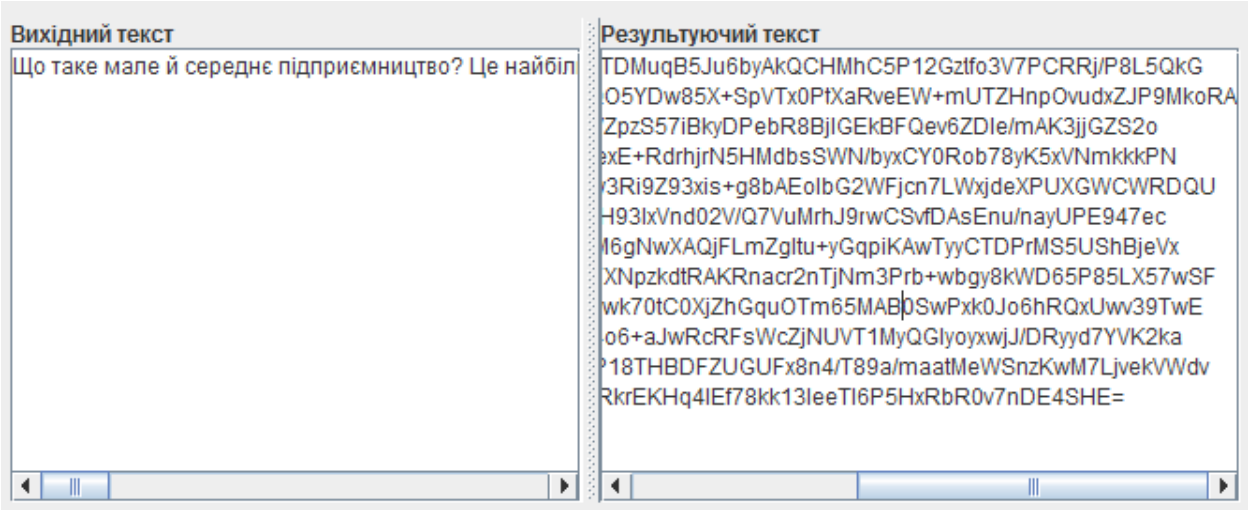
Діаграма шифру Файстеля

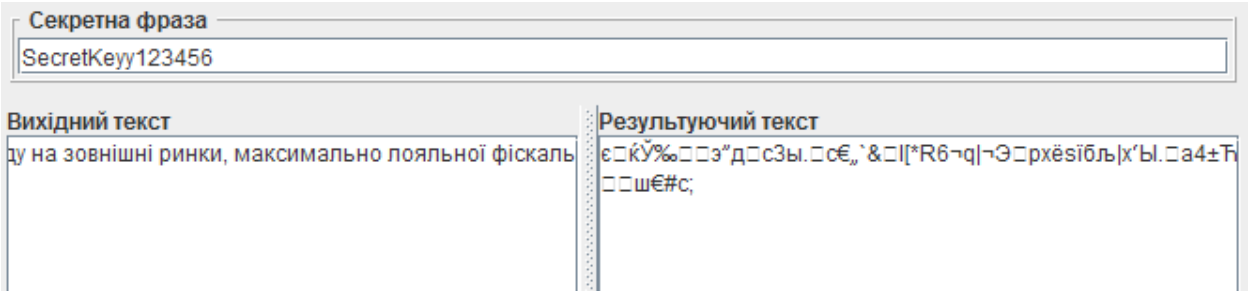
Модель та алгоритм шифрування



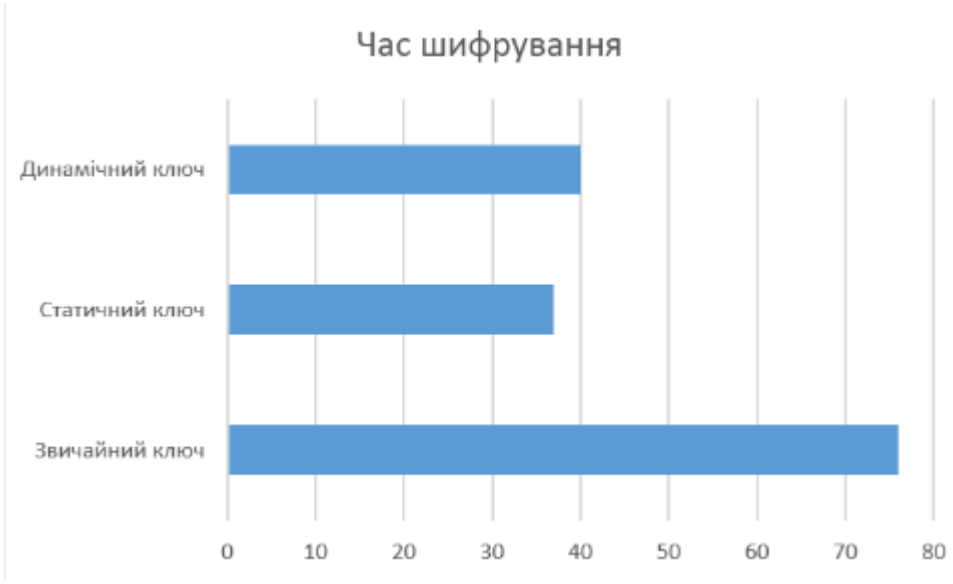
Програма


Шифрування з автоключом
Вибір джерела
Файл
Повідомлення
Тип ключа:
Звичайний
Розмір блока:
Початковий файл:
Переглянути
Результуючий файл:
Переглянути
Секретна фраза
Вихідний текст
Результуючий текст
Шифрувати
Дешифрувати

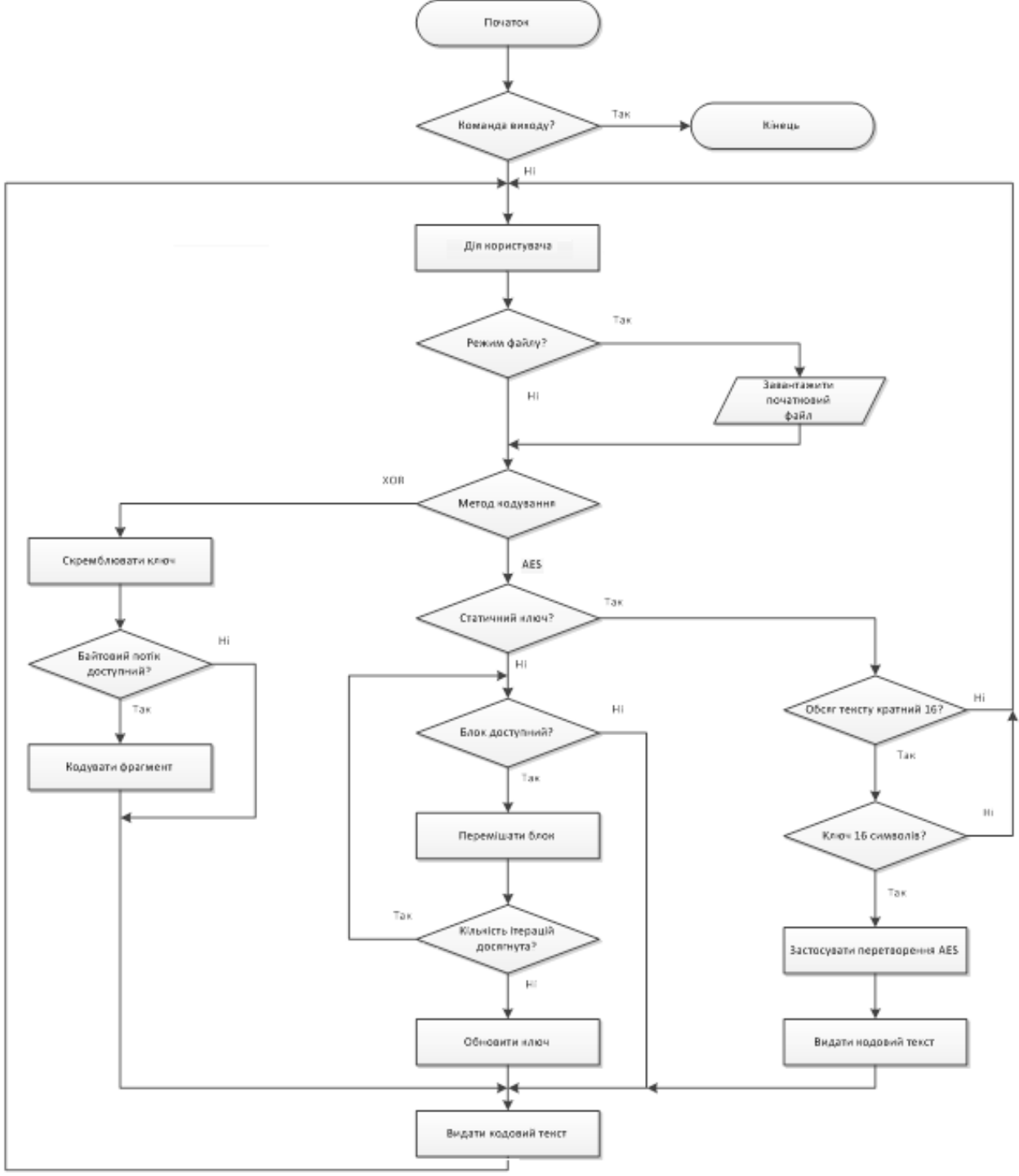

Вихідний текст
Що таке мале й середнє підприємництво? Це найбіл
Результуючий текст
TDMuqB5Ju6byAkQCHMhC5P12Gztfo3V7PCRRj/P8L5QkG
O5YDw85X+SpVTx0PtXaRveEW+mUTZHnpOvudxZJP9MkoRA
ZpzS57iBkyDPebR8BjIGEkBFQev6ZDIe/mAK3jjGZS2o
xE+RdrhjrN5HMdbsSWN/byxCY0Rob78yK5xVNmkkkPN
3Ri9Z93xis+g8bAEoIbG2WFjcn7LWxjdeXPUXGWCWRDQU
H93IxVnd02V/Q7VuMrhJ9rwCSvfDAsEnu/nayUPE947ec
l6gNwXAQjFLmZgltu+yGqpiKAwTyyCTDPrMS5UShBjeVx
XNpzkdtRAKRnacr2nTjNm3Prb+wbgy8kWD65P85LX57wSF
wk70tC0XjZhGquOTm65MAB0SwPxk0Jo6hRQxUwv39TwE
o6+aJwRcRFsWcZjNUVT1MyQGIyoyxwjJ/DRyyd7YVK2ka
?18THBDFZUGUFx8n4/T89a/maatMeWSnzKwM7LjvekVWdv
RkrEKHq4lEf78kk13leeTI6P5HxRbR0v7nDE4SHE=


Секретна фраза
SecretKeyy123456
Вихідний текст
ду на зовнішні ринки, максимально лояльної фіскаль
Результуючий текст
є□ќЎ‰□□з”д□с3ы.□с€„`&□l[*R6¬q|¬Э□рхёзїбль|х‘Ы.□а4±Ґ
□□ш€#с;

Алгоритм роботи програми



Діаграма оцінки часового фактору



ДЯКУЮ ЗА УВАГУ!