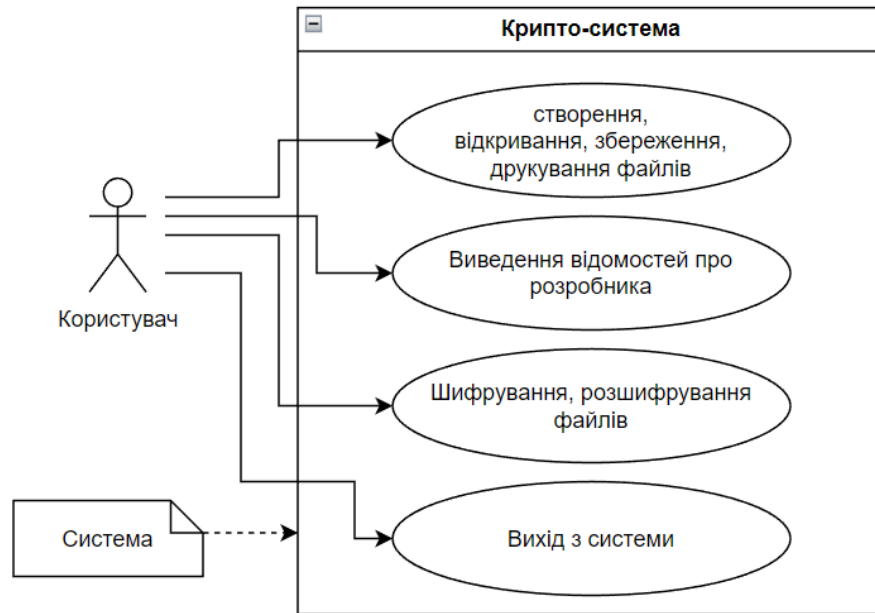


Міністерство освіти і науки України  
НТУУ «КПІ ім. Ігоря Сікорського»  
Навчально-науковий інститут атомної та теплової енергетики  
Кафедра цифрових технологій в енергетиці

Лабораторна робота №2  
з дисципліни «Безпека інформаційних систем»  
«Шифр Тритеміуса»  
Варіант № 22

Виконав: Студент групи ТР-12  
Ковальов Олександр  
Перевірів: доцент, к.ф.-м.н.  
Тарнавський Ю. А.

**Мета роботи.** Розробити криптосистему на основі шифру Тритеміуса.  
**Діаграма прецедентів.**

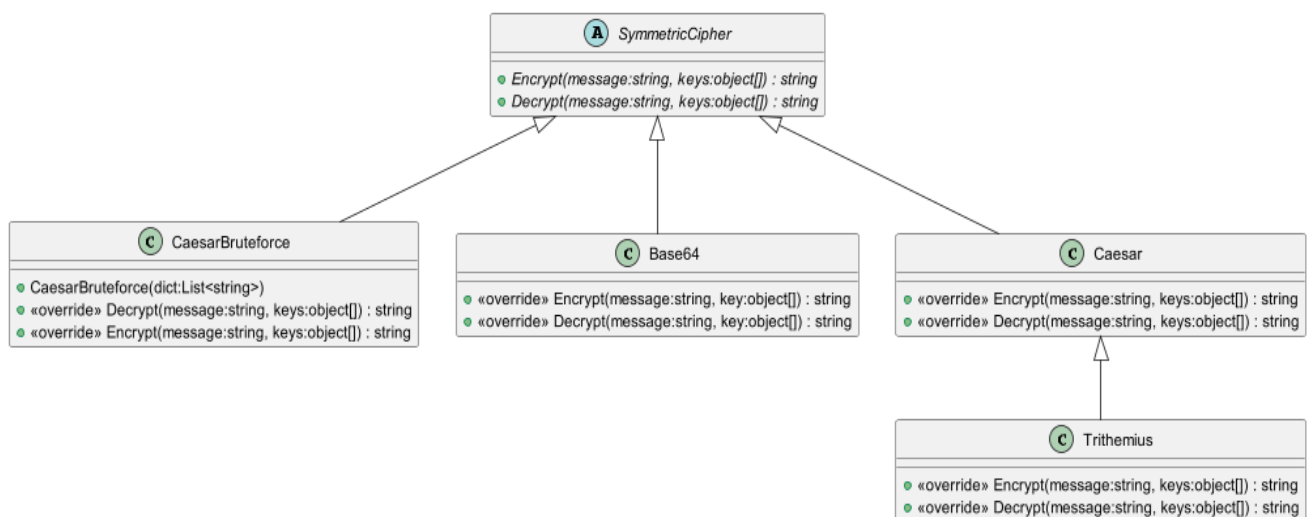


### Діаграма класів.

В просторі імен Cryptography знаходяться всі шифри, які наслідуються від класу SymmetricCipher. Також там є перелік CipherEnum.

В класі Trithemius знаходяться основні методи для шифрування та розшифрування даних цим методом. Клас наслідується від класу Caesar, а той, відповідно, від класу SymmetricCipher. Це означає, що API класу складається з двох основних методів – Encrypt та Decrypt. В них викликаються приватні методи.

Методи приймають аргументи: повідомлення типу String, масив типу object[] keys. Перший аргумент – власне повідомлення, яке треба зашифрувати або розшифрувати. Друге – масив, помічений ключовим словом params. Це означає, що можна передавати будь-яку кількість аргументів методу. Вони автоматично запакуються в масив.



## Фрагмент коду з реалізацією алгоритму шифрування/розшифрування.

```
public override string Encrypt(string message, params object[] keys)
{
    Func<int, int> handler = ValidateAndGetHandler(message, keys);

    return TrithemiusCipher(message, handler);
}

public override string Decrypt(string message, params object[] keys)
{
    Func<int, int> handler = ValidateAndGetHandler(message, keys);

    return TrithemiusCipher(message, DecryptionHandler(handler));
}

private string TrithemiusCipher(string message, Func<int, int> handler)
{
    var sb = new StringBuilder();

    for (int i = 0; i < message.Length; i++)
    {
        char c = message[i];

        sb.Append((char) ((c + (char) handler(i)) % UnicodeCardinal));
    }

    return sb.ToString();
}

private Func<int, int> LinearHandler(int a, int b)
{
    return (int position) => a * position + b;
}

private Func<int, int> NonLinearHandler(int a, int b, int c)
{
    return (int position) => (a * position * position + b * position + c);
}

private Func<int, int> MottoHandler(string message, string motto)
{
    return (int position) =>
    {
        if (message.Length <= motto.Length) return motto[position];

        var factor =
(int) Math.Ceiling((decimal) message.Length / motto.Length);

        var localMotto = string.Concat(Enumerable.Repeat(motto, factor));

        return localMotto[position];
    };
}

private Func<int, int> DecryptionHandler(Func<int, int> handler)
{
    return (int position) => -1 * handler(position);
}
```

## Скріншоти програми.

Панель для роботи з шифром Тритеміуса:

Crypto-system

File About

↩ ↪ [Red X]

**Ciphers:**

Trithemius

**Key type:**

Encrypt Decrypt

A: B: C:

Motto:

Всього є 3 типи ключів: лінійне рівняння, нелінійне та гасло:

Key type:

NonLinear

Linear

NonLinear

Motto

Кнопки Encrypt та Decrypt розблоковуються, коли визначений тип ключа, в робочій області введено текст, та заповнені поля пов'язані з ключем:

Crypto-system

File About

↩ ↪ D:\Downloads\БІС\Text.txt [Green Checkmark]

**Ciphers:**

Trithemius

**Key type:**

Encrypt Decrypt

A: B: C:

Motto:

Motto?

The quick brown fox jumps over the lazy dog.  
Гей, хлопці, не вспію — на ганку ваша файна іжа знищується бурундучком.

Приклад зашифрованого тексту:

Crypto-system

File About

↩ ↪ D:\Downloads\БІС\Text.txt [Green Checkmark]

**Ciphers:**

Trithemius

**Key type:**

Encrypt Decrypt

A: B: C:

Motto:

Motto?

j×Ùà'ŦÖBÑ±¼æâÖ®ÄpéÛ-ÀâêÖ±māUÜ«®éíÖ®  
~\$Vççöьцц Œ\$ГьцYбкsTămdHуæ\$mkHek\_rktyk\_HнHГьŒчнyйPенXwГT@чçoyйçç

## Приклад роботи методу грубої сили для шифру Тритеміуса:

The screenshot shows a window titled "Crypto-system" with standard window controls (minimize, maximize, close). Below the title bar are "File" and "About" menus. A toolbar contains undo, redo, and a close button. The main interface is divided into several sections:

- Ciphers:** A dropdown menu currently showing "TrithemiusBruteforce".
- Initial message:** A text input field containing "Hello World!".
- Encrypted message:** A text input field containing "ÔÛÑt¼çæ¿Ó".
- Open/Close buttons:** Two buttons, "Open" (with a document icon) and "Close" (with a close icon), both highlighted in blue.
- Dictionary.txt:** A button with a document icon and the text "Dictionary.txt".
- Decrypt:** A button with a padlock icon and the text "Decrypt", enclosed in a dashed border.
- Full key:** A text area displaying "Some TextSom".
- Possible keywords (from dictionary):** A text area displaying "Some".

**Висновок:** за результатами виконання цієї лабораторної роботи було ознайомлено з принципом роботи шифру Тритеміуса та написано метод грубої сили. Але – брутфорс працює лише якщо перехватити пару повідомлень «Зашифроване» та «Розшифроване». Також, метод не працює з ключами у вигляді лінійних та нелінійних рівнянь. Але, це і не має сенсу – отримання ключа дозволило б розшифровувати повідомлення такої ж довжини, не більше (тому що далі послідовність інша, бо ключ без повторень)