Національний технічний університет України
«Київський політехнічний інститут»

Інститут Прикладного системного аналізу
Кафедра Системного проектування

Лабораторна робота № 3

з дисципліни «**ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ**»

«Дослідження криптосистеми шифрування даних RSA»

Виконав:
студент групи ДА-82
факультету «ІПСА»
Муравльов А. Д.
Варіант 17

Київ – 2021

Хід роботи

1. Зашифрувати вручну своє прізвище, ім'я та по-батькові, написані великими та малими буквами англійського алфавіту з урахуванням пробілів, за допомогою шифру RSA. Для цього за допомогою пакету CrypTool вибрати параметри криптосистеми RSA з розрахунком, щоб можна було виконати шифрування і дешифрування вручну за допомогою інженерного калькулятора. При кодуванні букв використовувати кодову таблицю ASCI, параметри p і q криптосистеми RSA вибрати в межах від 2^7 до 2^8. Виконати вручну дешифрування отриманого шифротексту.

Параметр	Значення
p	173
q	181
N	31313
e	41
d	6041

Табл. 1 Параметри шифру

Шифрування

Вхідний текст:

Muravlyov Andriy Dmytrovych

Текст кодований за таблицею ASCII:

077 117 114 097 118 108 121 111 118 032 065 110 100 114 105 121 032 068 109 121 116 114 111 118 121 099 104

Формула визначення зашифрованого елементу тексту *c[i]* на основі елементу вихідного тексту *m[i]*:

$c[i]=m[i]^e \bmod N$

Таким чином, маємо зашифрований текст:

20506 14304 16134 17358 28856 29826 31213 00166 28856 05901 20171 30629 30392 16134 20335 31213 05901 13400 09654 31213 14400 16134 00166 28856 31213 09629 11169

Дешифрування

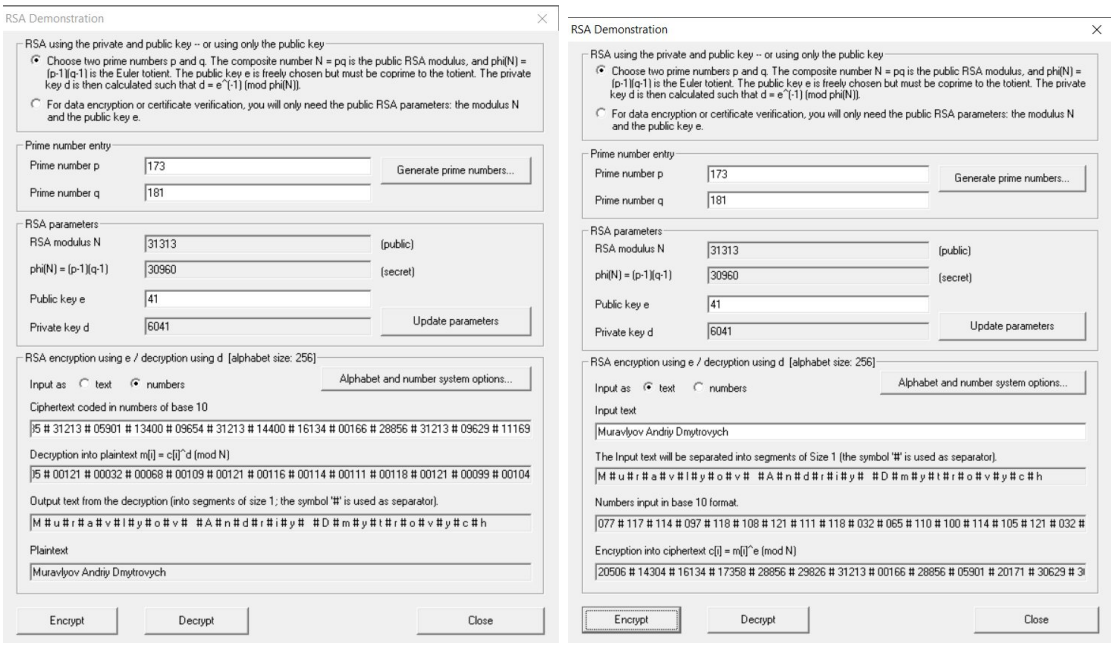
Формула визначення елементу вихідного тексту *m[i]* на основі зашифрованого елементу тексту *c[i]*:

$m[i]=c[i]^d \bmod N$

77 117 114 97 118 108 121 111 118 32 65110 100 114 105 121 32 68 109 121 116 114 111 118 121 99 104

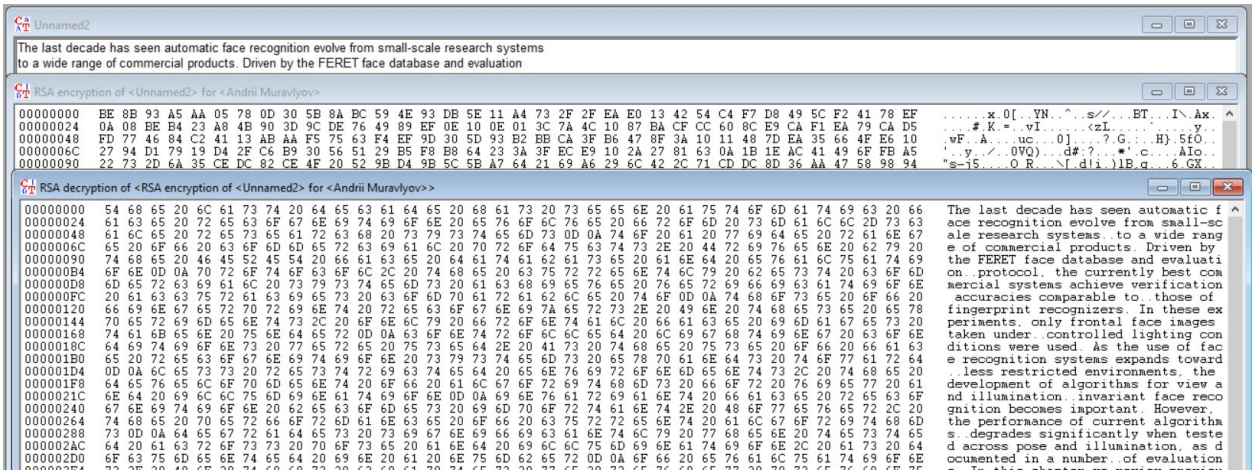
Порівнявши отриманий текст з вихідним у кодуванні ASCII бачимо, що дешифрування успішне.

2. Виконати шифрування і дешифрування свого прізвища, імені та по-батькові за допомогою засобів пакету CrypTool. Зберегти отримані результати шифрування і дешифрування у відповідні файли за допомогою засобів пакету CrypTool. Порівняти результати ручного та автоматичного шифрування і дешифрування.



Перевірка правильності дешифрування(зправа) та шифрування(зліва)

3. *Вибрати варіант текстового файлу (див. Додаток до лабораторної роботи № 1) відповідно до порядкового номера студенту в списку академічної групи. За допомогою засобів пакету CrypTool зашифрувати і дешифрувати обраний файл шифром RSA з параметрами, які використовувалися при виконанні п.2. Порівняти вихідний текст з дешифрованим. Зробити висновки. Результати зберегти.*



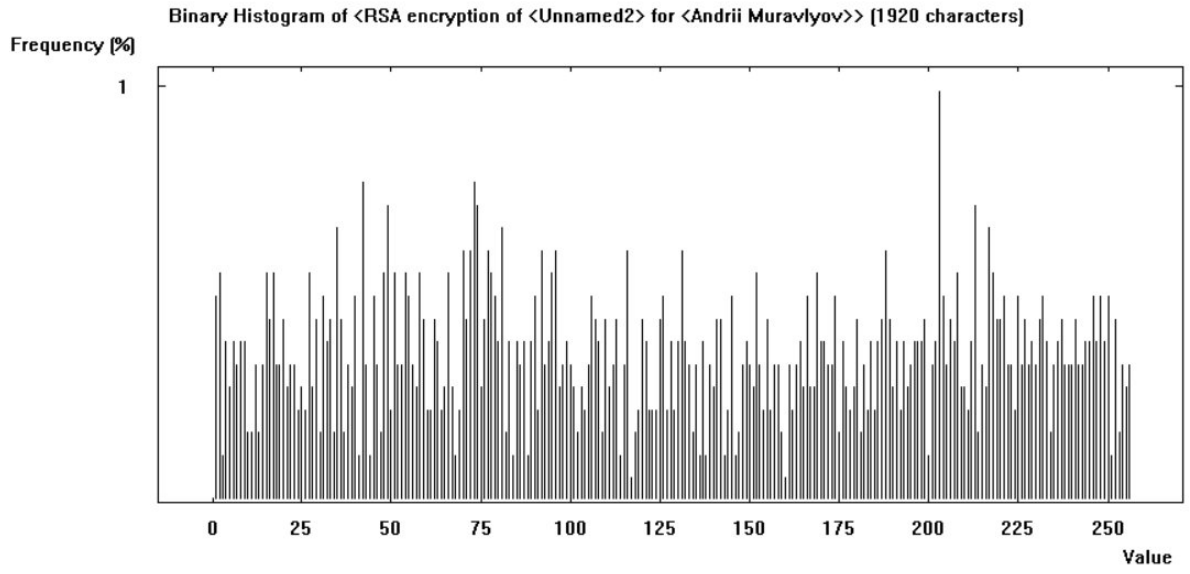
Зашифрований та вихідний тексти

Бачимо, що при шифруванні та дешифруванні не відбулось ніяких втрат у тексті, оскільки всі символи входять до таблиці кодування ASCII, якою ми користувались при шифруванні.

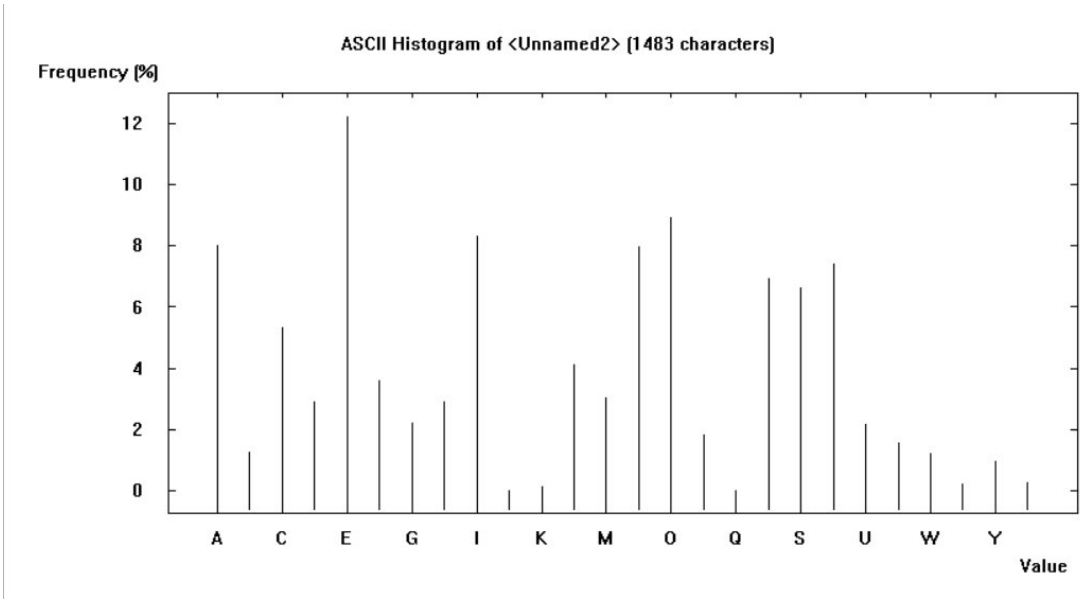
4.*За допомогою засобів аналізу пакету CrypTool провести частотний аналіз вихідного і зашифрованого тексту. Визначити ентропію і максимально можливу ентропію зашифрованого файлу, а також побудувати гістограму розподілу частоти символів в аналізованих файлах. Зробити висновки про можливість криптоаналізу зашифрованого тексту з використанням тільки шифротексту. Дослідити можливості пакета CrypTool для злому шифра RSA.*

Гістрограми розподілу частоти символів:

Гістограма зашифрованого тексту



Гістограма оригіналу



Ентропія

	Ентропія файлу	Максимальна ентропія
Зашифрований файл	7.91	8.00
Оригінал	4.11	4.70

З отриманих даних по ентропії та гістограмі частот очевидно, що алгоритм не піддається частотному аналізу та аналізу на основі лише шифротексту.

5.Написати і налагодити програму для шифрування і дешифрування файлів за допомогою шифру RSA використовуючи готові бібліотеки (наприклад System.Security.Cryptography в середовищі .NET Security Framework). Зашифрувати текстовий файл, вибраний з додатку до лабораторної роботи при виконанні п.3, за допомогою розробленої програми. Порівняти результати шифрування, отримані за допомогою пакета CrypTool, з результатами роботи власної програми. Зробити висновки про коректність роботи програми.

Згенеруємо сертифікат, що містить приватний та публічний ключ за допомогою утиліти openssl:

```
PS D:\Labs\Andrey\Bis2\Bis2\Keys> openssl genrsa -out private.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
..+++++
.................+++++
e is 65537 (0x010001)
PS D:\Labs\Andrey\Bis2\Bis2\Keys> openssl req -new -x509 -key private.pem -out public.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
PS D:\Labs\Andrey\Bis2\Bis2\Keys>
PS D:\Labs\Andrey\Bis2\Bis2\Keys> openssl pkcs12 -export -out cert.p12 -inkey private.pem -in public.crt
Enter Export Password:
Verifying - Enter Export Password:
PS D:\Labs\Andrey\Bis2\Bis2\Keys>
```

Код для програми доступний за посиланням

https://github.com/lakub-muravlov/fourth-course-projects/tree/main/Information_System_Security/Lab3/Bis2

В результаті роботи програми отримуємо файли encrypted-rsa.hex(зашифрований бінарний файл) та decrypted-rsa.txt(розшифрований оригінал з зашифрованого файлу). Оскільки очевидно, що пакет CrypTool

використовує алгоритм PKCS1 V1.5, який додає випадкові байти для доповнення повідомлення та забезпечення більшої криптостійкості алгоритму – кожного разу отримуємо трохи різний результат, то ми не можемо скористатись утилітою для порівняння двох бінарних файлів по типу fc /b у середовищі Windows. Також не є можливим імпортувати згенерований сертифікат у середовище CrypTool, оскільки він дозволяє імпортувати лише згенеровані у самому середовищі сертифікати та не допускає використання сторонніх. Таким чином, перевірити роботу програми середовищем CrypTool ми не можемо.

Висновки

Протягом виконання роботи я покращив код лабораторної роботи №2, додавши до неї реалізації алгоритму RSA та ознайомився з утилітою командного рядка openssl. Алгоритм RSA в першу чергу слугує для створення цифрових підписів та гібридного шифрування, у якому він використовується для шифрування ключа від алгоритму симетричного шифрування, що надалі використовується для шифрування самих файлів. Після цього зашифрований ключ та сам файл можна передавати по незахищеному каналу зв’язку при умові, що отримувач має приватний ключ та здатен розшифрувати зашифрований ключ симетричного шифрування.