ДОДАТОК А

Інструкції користувача

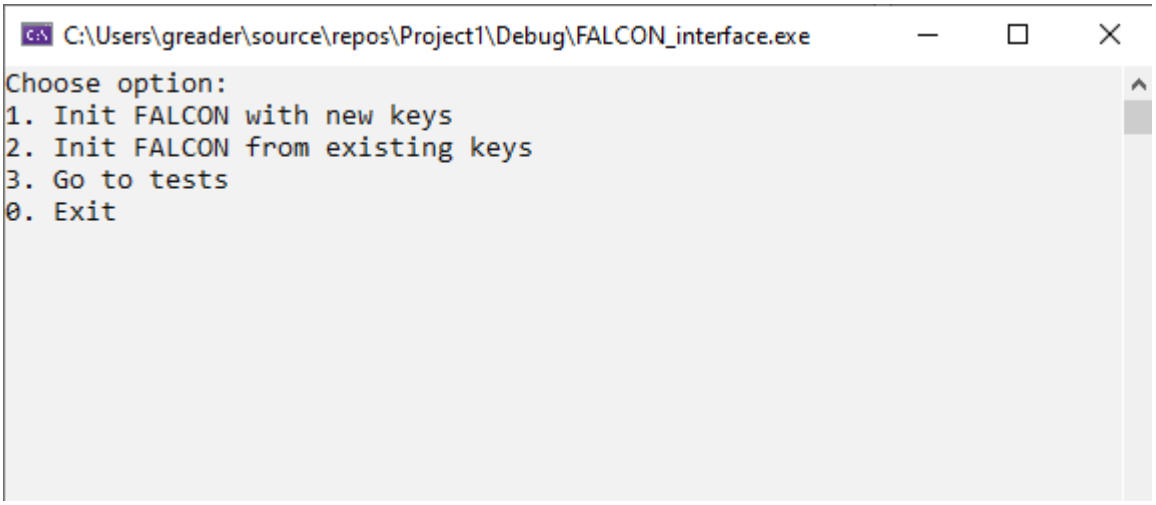

Рисунок А.1 — Головний екран програми

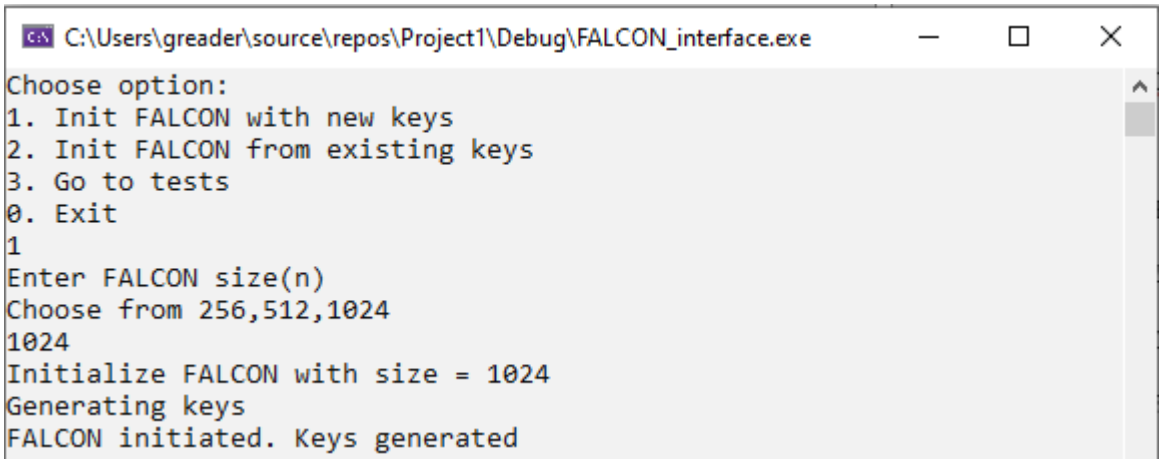

Рисунок А.2 — Ініціалізація FALCON з новими ключами

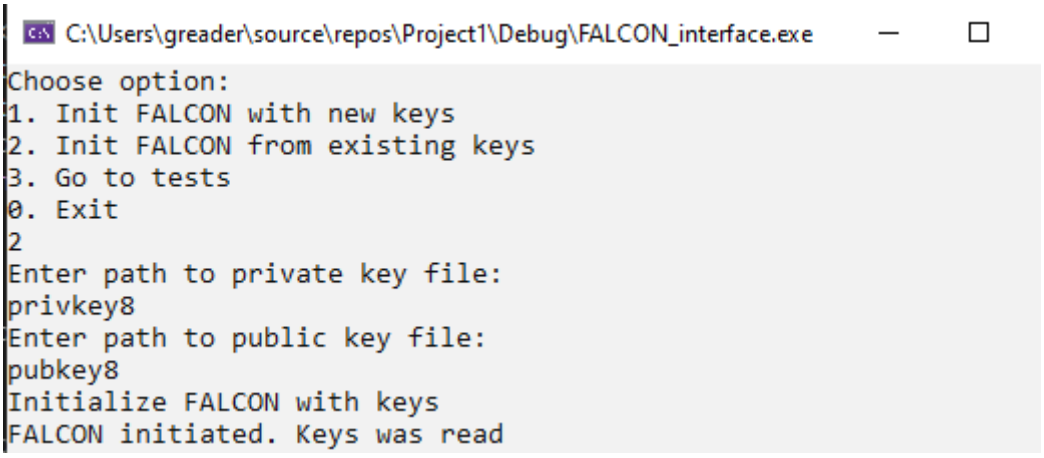

Рисунок А.3 — Ініціалізація FALCON з існуючими ключами

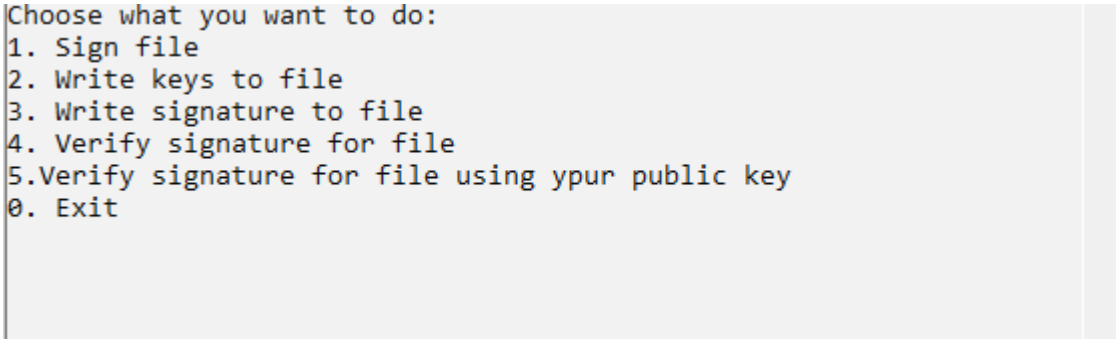

Рисунок А.4 — Екран взаємодії з основними засобами FALCON

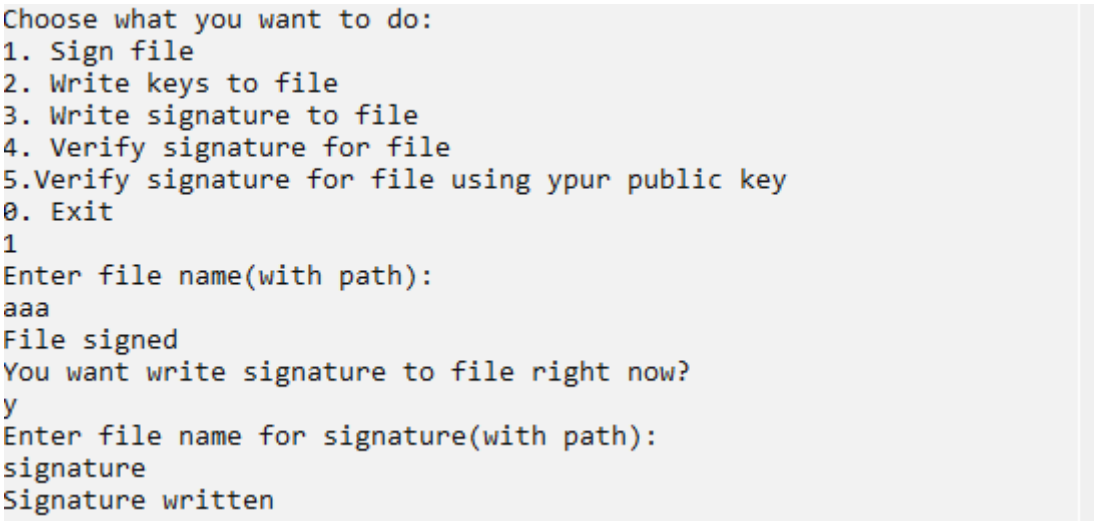

Рисунок А.5 — Процедура підпису файлу

```
Choose what you want to do:
1. Sign file
2. Write keys to file
3. Write signature to file
4. Verify signature for file
5.Verify signature for file using ypur public key
0. Exit
2
Enter file name(with path) for private key:
privkey
Enter file name(with path) for public key:
pubkey
Keys written
```

Рисунок А.6 — Процедура запису ключів у файл

```
Choose what you want to do:
1. Sign file
2. Write keys to file
3. Write signature to file
4. Verify signature for file
5.Verify signature for file using ypur public key
0. Exit
3
Enter file name for signature(with path):
sign
Signature written
```

Рисунок А.7 — Процедура запису підпису у файл

```
Choose what you want to do:
1. Sign file
2. Write keys to file
3. Write signature to file
4. Verify signature for file
5.Verify signature for file using ypur public key
0. Exit
4
Enter file name(with path) with data:
aaa
Enter file name(with path) with signature:
sign
Signature is correct
```

Рисунок А.8 — Процедура перевірки підпису

```
Choose what you want to do:
1. Sign file
2. Write keys to file
3. Write signature to file
4. Verify signature for file
5.Verify signature for file using ypur public key
0. Exit
5
Enter file name(with path) with data:
aaa
Enter file name(with path) with signature:
sign
Enter file name(with path) with public key:
pubkey8
Signature is correct
```

Рисунок А.9 — Перевірка підпису з використанням файлу ключа

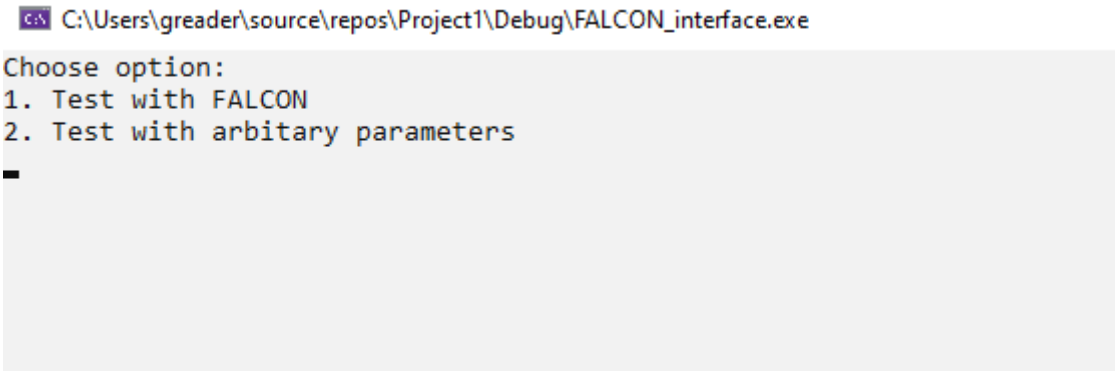

Рисунок А.10 — Екран вибору процедури тестування

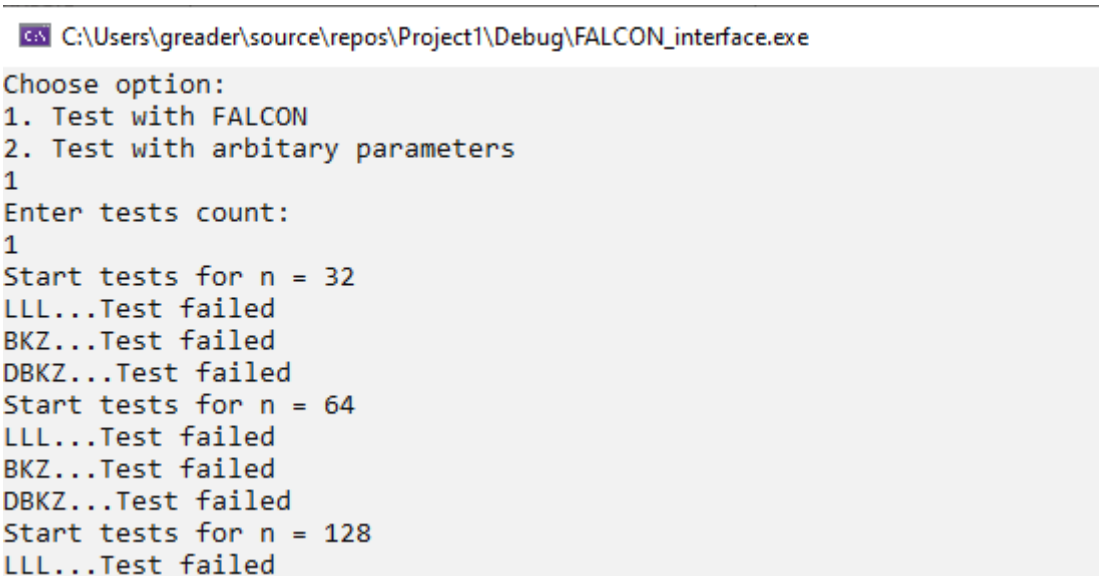

Рисунок А.11 — Виконання процедури приведення для FALCON

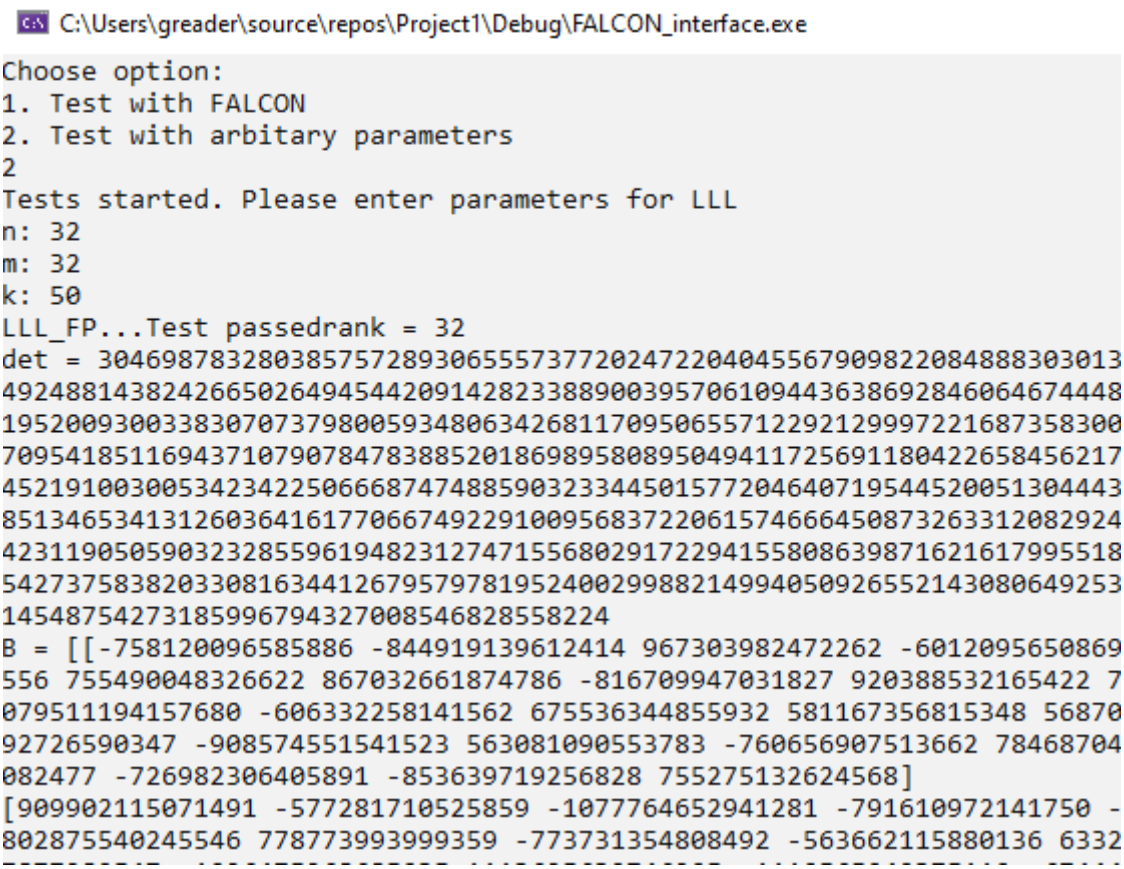

Рисунок А.12 — Процедура приведення для довільних параметрів

ВІДОМІСТЬ МАГІСТЕРСЬКОЇ АТЕСТАЦІЙНОЇ РОБОТИ

№ док.	*Позначення*	*Найменування*	*Дод. від*
1		Текстові документи	
	ГЮІК.ХХХХХХ.1412Ст.17П	Пояснювальна записка	87 стр.
2		Графічні документи	
		Презентаційний матеріал	
3		Інші документи	
		Електронна версія ПЗ	
		Рецензія	1 стр.
		Відгук керівника	1 стр.

					ГЮІК.ХХХХХХ.1412Ст.17ВД
З	Л	№ докум.	Підпис	Дата	
Розроб		Черниш Д.І.			Дослідження криптографічних атак на ЕЦП FALCON
Переві		Мельникова О.А.			
Н.конт		Конева Н.Ф.			
Затвер		Халімов Г.З.			

Літ.	*Лис*	*Лист*
Т		

ХНУРЕ
Кафедра БІТ