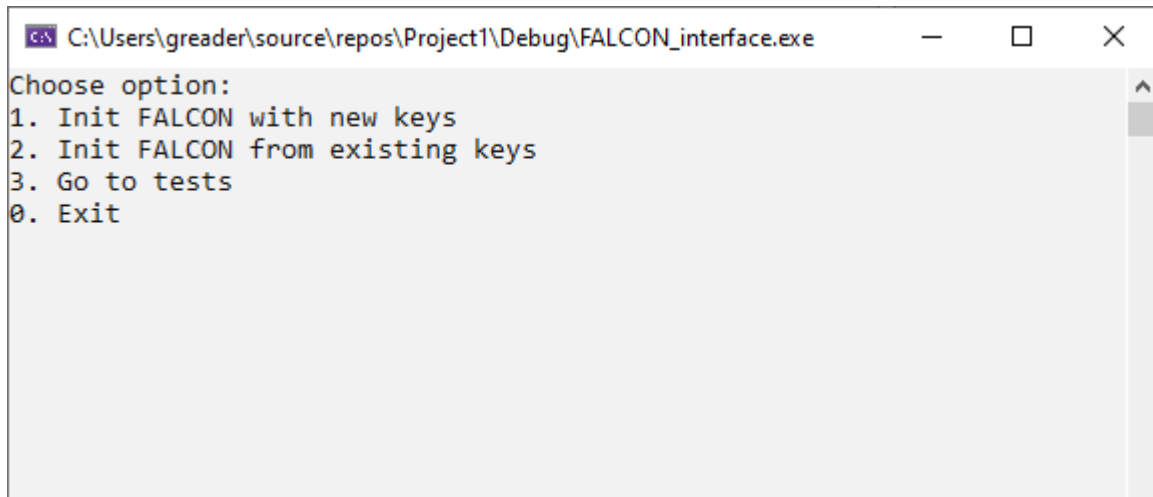


ДОДАТОК А

Інструкції користувача



```
C:\Users\greader\source\repos\Project1\Debug\FALCON_interface.exe
Choose option:
1. Init FALCON with new keys
2. Init FALCON from existing keys
3. Go to tests
0. Exit
```

Рисунок А.1 — Головний екран програми



```
C:\Users\greader\source\repos\Project1\Debug\FALCON_interface.exe
Choose option:
1. Init FALCON with new keys
2. Init FALCON from existing keys
3. Go to tests
0. Exit
1
Enter FALCON size(n)
Choose from 256,512,1024
1024
Initialize FALCON with size = 1024
Generating keys
FALCON initiated. Keys generated
```

Рисунок А.2 — Ініціалізація FALCON з новими ключами

```

C:\Users\greader\source\repos\Project1\Debug\FALCON_interface.exe
Choose option:
1. Init FALCON with new keys
2. Init FALCON from existing keys
3. Go to tests
0. Exit
2
Enter path to private key file:
privkey8
Enter path to public key file:
pubkey8
Initialize FALCON with keys
FALCON initiated. Keys was read

```

Рисунок А.3 — Ініціалізація FALCON з існуючими ключами

```

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

```

Рисунок А.4 — Екран взаємодії з основними засобами FALCON

```

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
1
Enter file name(with path):
aaa
File signed
You want write signature to file right now?
y
Enter file name for signature(with path):
signature
Signature written

```

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 your 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

```

C:\Users\greader\source\repos\Project1\Debug\FALCON_interface.exe

```

```

Choose option:
1. Test with FALCON
2. Test with arbitrary parameters
-

```

Рисунок А.10 — Екран вибору процедури тестування

```

C:\Users\greader\source\repos\Project1\Debug\FALCON_interface.exe

```

```

Choose option:
1. Test with FALCON
2. Test with arbitrary parameters
1
Enter tests count:
1
Start tests for n = 32
LLL...Test failed
BKZ...Test failed
DBKZ...Test failed
Start tests for n = 64
LLL...Test failed
BKZ...Test failed
DBKZ...Test failed
Start tests for n = 128
LLL...Test failed

```

Рисунок А.11 — Виконання процедури приведення для FALCON

```

C:\Users\greader\source\repos\Project1\Debug\FALCON_interface.exe
Choose option:
1. Test with FALCON
2. Test with arbitrary parameters
2
Tests started. Please enter parameters for LLL
n: 32
m: 32
k: 50
LLL_FP...Test passedrank = 32
det = 3046987832803857572893065557377202472204045567909822084888303013
4924881438242665026494544209142823388900395706109443638692846064674448
1952009300338307073798005934806342681170950655712292129997221687358300
7095418511694371079078478388520186989580895049411725691180422658456217
4521910030053423422506668747488590323344501577204640719544520051304443
8513465341312603641617706674922910095683722061574666450873263312082924
4231190505903232855961948231274715568029172294155808639871621617995518
5427375838203308163441267957978195240029988214994050926552143080649253
14548754273185996794327008546828558224
B = [[-758120096585886 -844919139612414 967303982472262 -6012095650869
556 755490048326622 867032661874786 -816709947031827 920388532165422 7
079511194157680 -606332258141562 675536344855932 581167356815348 56870
92726590347 -908574551541523 563081090553783 -760656907513662 78468704
082477 -726982306405891 -853639719256828 755275132624568]
[909902115071491 -577281710525859 -1077764652941281 -791610972141750 -
802875540245546 778773993999359 -773731354808492 -563662115880136 6332
-----

```

Рисунок А.12 — Процедура приведення для довільних параметрів

