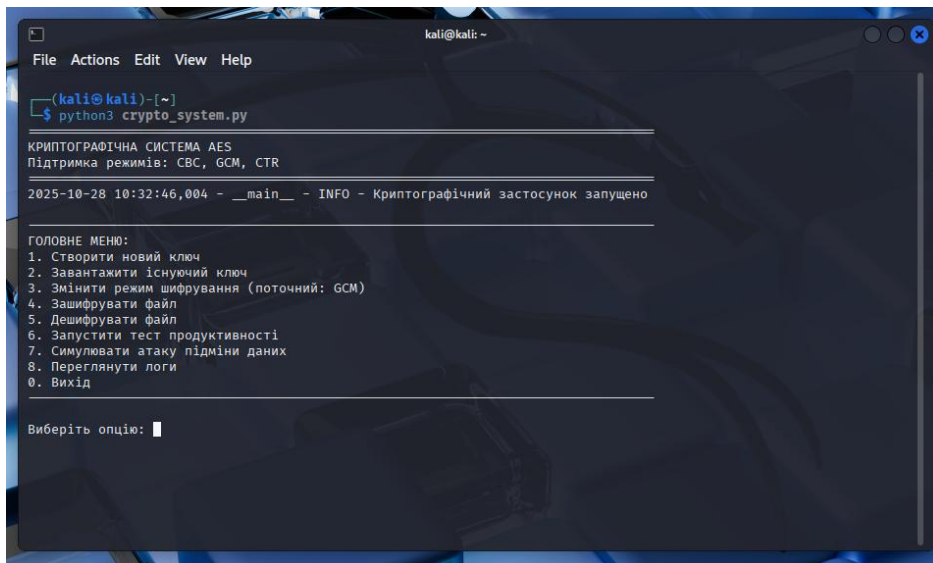


## 1. Запуск програми

python3 crypto\_system.py



```
kali@kali: ~  
File Actions Edit View Help  
~  
$ python3 crypto_system.py  
КРИПТОГРАФІЧНА СИСТЕМА AES  
Підтримка режимів: CBC, GCM, CTR  
2025-10-28 10:32:46,004 - __main__ - INFO - Криптографічний застосунок запущено  
Головне меню:  
1. Створити новий ключ  
2. Завантажити існуючий ключ  
3. Змінити режим шифрування (поточний: GCM)  
4. Зашифрувати файл  
5. Дешифрувати файл  
6. Запустити тест продуктивності  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
Виберіть опцію: █
```

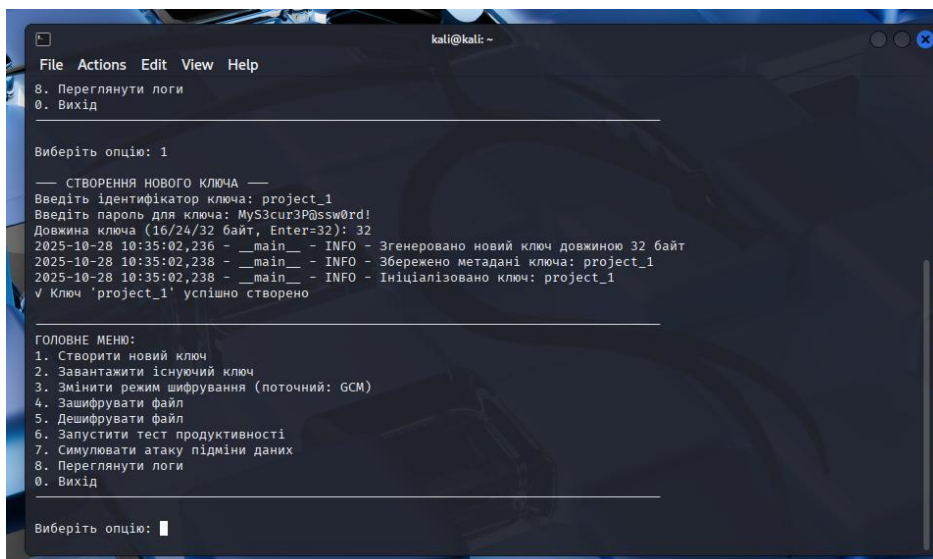
## 2. Створення ключа

Меню → 1

Key ID: project\_1

Password: MyS3cur3P@ssw0rd!

Length: 32



```
kali@kali: ~  
File Actions Edit View Help  
8. Переглянути логи  
0. Вихід  
Виберіть опцію: 1  
— СТВОРЕННЯ НОВОГО КЛЮЧА —  
Введіть ідентифікатор ключа: project_1  
Введіть пароль для ключа: MyS3cur3P@ssw0rd!  
Довжина ключа (16/24/32 байт, Enter=32): 32  
2025-10-28 10:35:02,236 - __main__ - INFO - Згенеровано новий ключ довжиною 32 байт  
2025-10-28 10:35:02,238 - __main__ - INFO - Збережено метадані ключа: project_1  
2025-10-28 10:35:02,238 - __main__ - INFO - Ініціалізовано ключ: project_1  
✓ Ключ 'project_1' успішно створено  
Головне меню:  
1. Створити новий ключ  
2. Завантажити існуючий ключ  
3. Змінити режим шифрування (поточний: GCM)  
4. Зашифрувати файл  
5. Дешифрувати файл  
6. Запустити тест продуктивності  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
Виберіть опцію: █
```

## 3. Вибір режиму

Меню → 3

Mode: GCM

```
kali@kali: ~  
File Actions Edit View Help  
8. Переглянути логи  
0. Вихід  
-----  
Виберіть опцію: 3  
-----  
ЗМІНА РЕЖИМУ ШИФРУВАННЯ  
Доступні режими:  
CBC - Cipher Block Chaining (з HMAC)  
GCM - Galois/Counter Mode (authenticated encryption)  
CTR - Counter Mode (з HMAC)  
Виберіть режим (CBC/GCM/CTR): GCM  
2025-10-28 10:37:01,328 - __main__ - INFO - Режим змінено на: GCM  
✓ Режим шифрування: GCM  
-----  
ГОЛОВНЕ МЕНЮ:  
1. Створити новий ключ  
2. Завантажити існуючий ключ  
3. Змінити режим шифрування (поточний: GCM)  
4. Зашифрувати файл  
5. Дешифрувати файл  
6. Запустити тест продуктивності  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
-----  
Виберіть опцію: █
```

## 4. Шифрування файлу

Меню → 4

Input: test.txt

Output: test.txt.encrypted

```
kali@kali: ~  
File Actions Edit View Help  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
-----  
Виберіть опцію: 4  
-----  
ШИФРУВАННЯ ФАЙЛУ  
Шлях до файлу для шифрування: /home/kali/Desktop/test.txt  
Шлях для збереження (Enter=авто):  
2025-10-28 10:46:23,677 - __main__ - INFO - Шифрування файлу: /home/kali/Desktop/test.txt (3 байт)  
2025-10-28 10:46:23,677 - __main__ - INFO - GCM шифрування: 3 байт → 3 байт  
2025-10-28 10:46:23,677 - __main__ - INFO - Файл зашифровано: /home/kali/Desktop/test.txt.encrypted  
✓ Файл зашифровано: /home/kali/Desktop/test.txt.encrypted  
-----  
ГОЛОВНЕ МЕНЮ:  
1. Створити новий ключ  
2. Завантажити існуючий ключ  
3. Змінити режим шифрування (поточний: GCM)  
4. Зашифрувати файл  
5. Дешифрувати файл  
6. Запустити тест продуктивності  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
-----  
Виберіть опцію: █
```

## 5. Дешифрування

Меню → 5

Input: test.txt.encrypted

Output: test.txt.decrypted

```
kali@kali: ~  
File Actions Edit View Help  
8. Переглянути логи  
0. Вихід  
-----  
Виберіть опцію: 5  
-----  
— ДЕШИФРУВАННЯ ФАЙЛУ —  
Шлях до зашифрованого файлу: /home/kali/Desktop/test.txt.encrypted  
Шлях для збереження (Enter=авто):  
2025-10-28 10:50:23,243 - __main__ - INFO - Дешифрування файлу: /home/kali/Desktop/test.txt.encrypted (режим: GCM)  
2025-10-28 10:50:23,244 - __main__ - INFO - GCM дешифрування: 3 байт → 3 байт  
2025-10-28 10:50:23,244 - __main__ - INFO - Файл дешифровано: /home/kali/Desktop/test.txt.decrypted  
✓ Файл дешифровано: /home/kali/Desktop/test.txt.decrypted  
-----  
ГОЛОВНЕ МЕНЮ:  
1. Створити новий ключ  
2. Завантажити існуючий ключ  
3. Змінити режим шифрування (поточний: GCM)  
4. Зашифрувати файл  
5. Дешифрувати файл  
6. Запустити тест продуктивності  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
-----  
Виберіть опцію: █
```

## Тестування безпеки

### 1. Шифрування тестового файлу

Меню → 4

Input: simulation.txt

```
kali@kali: ~  
File Actions Edit View Help  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
-----  
Виберіть опцію: 4  
-----  
— ШИФРУВАННЯ ФАЙЛУ —  
Шлях до файлу для шифрування: /home/kali/Desktop/simulation.txt  
Шлях для збереження (Enter=авто):  
2025-10-28 10:54:56,521 - __main__ - INFO - Шифрування файлу: /home/kali/Desktop/simulation.txt (10 байт)  
2025-10-28 10:54:56,522 - __main__ - INFO - GCM шифрування: 10 байт → 10 байт  
2025-10-28 10:54:56,523 - __main__ - INFO - Файл зашифровано: /home/kali/Desktop/simulation.txt.encrypted  
✓ Файл зашифровано: /home/kali/Desktop/simulation.txt.encrypted  
-----  
ГОЛОВНЕ МЕНЮ:  
1. Створити новий ключ  
2. Завантажити існуючий ключ  
3. Змінити режим шифрування (поточний: GCM)  
4. Зашифрувати файл  
5. Дешифрувати файл  
6. Запустити тест продуктивності  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
-----  
Виберіть опцію: █
```

### 2. Симуляція атаки

Меню → 7

File: simulation.txt.encrypted

```
kali@kali: ~  
File Actions Edit View Help  
△ СИМУЛЯЦІЯ АТАКИ: підміна даних у файлі /home/kali/Desktop/simulation.txt.encrypted  
2025-10-28 10:57:27,023 - __main__ - WARNING - Створено підроблений файл: /home/kali/Desktop/simulation.txt.encrypted.tampered  
✓ Створено підроблений файл: /home/kali/Desktop/simulation.txt.encrypted.tampered  
Спробуйте дешифрувати його для перевірки виявлення підміни  
  
Спроба дешифрувати підроблений файл...  
2025-10-28 10:57:27,024 - __main__ - INFO - Дешифрування файлу: /home/kali/Desktop/simulation.txt.encrypted.tampered (режим: GCM)  
2025-10-28 10:57:27,025 - __main__ - ERROR - GCM tag не валідний! Дані змінено!  
2025-10-28 10:57:27,025 - __main__ - ERROR - КРИТИЧНА ПОМИЛКА: Дані були змінені або пошкоджені!  
x КРИТИЧНА ПОМИЛКА: Дані були змінені або пошкоджені!  
Можлива спроба підміни даних або неправильний ключ!  
  
ГОЛОВНЕ МЕНЮ:  
1. Створити новий ключ  
2. Завантажити існуючий ключ  
3. Змінити режим шифрування (поточний: GCM)  
4. Зашифрувати файл  
5. Дешифрувати файл  
6. Запустити тест продуктивності  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
  
Виберіть опцію: 
```

### 3. Спроба дешифрування підробленого файлу

Меню → 5

Input: simulation.txt.encrypted.tampered

Очікується помилка автентифікації

```
kali@kali: ~  
File Actions Edit View Help  
0. Вихід  
  
Виберіть опцію: 5  
  
— ДЕШИФРУВАННЯ ФАЙЛУ —  
Шлях до зашифрованого файлу: /home/kali/Desktop/simulation.txt.encrypted.tampered  
Шлях для збереження (Enter=авто):  
2025-10-28 11:00:31,535 - __main__ - INFO - Дешифрування файлу: /home/kali/Desktop/simulation.txt.encrypted.tampered (режим: GCM)  
2025-10-28 11:00:31,535 - __main__ - ERROR - GCM tag не валідний! Дані змінено!  
2025-10-28 11:00:31,535 - __main__ - ERROR - КРИТИЧНА ПОМИЛКА: Дані були змінені або пошкоджені!  
x КРИТИЧНА ПОМИЛКА: Дані були змінені або пошкоджені!  
Можлива спроба підміни даних або неправильний ключ!  
  
ГОЛОВНЕ МЕНЮ:  
1. Створити новий ключ  
2. Завантажити існуючий ключ  
3. Змінити режим шифрування (поточний: GCM)  
4. Зашифрувати файл  
5. Дешифрувати файл  
6. Запустити тест продуктивності  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
  
Виберіть опцію: 
```

### Аналіз продуктивності

Меню → 6

Система протестує всі режими на різних розмірах

Звіт буде збережено в crypto\_storage/logs/

```
kali@kali: ~  
File Actions Edit View Help  
  
2. CTR режим: Швидкий, але потребує окремої автентифікації.  
- Можна паралелізувати  
- Не потребує padding  
- Необхідний HMAC для цілісності  
  
3. CBC режим: Традиційний, але повільніший.  
- Не паралелізується  
- Потребує padding  
- Потребує окремого HMAC  
  
✓ Звіт збережено: crypto_storage/logs/performance_report_20251028_110156.txt  
  
ГОЛОВНЕ МЕНЮ:  
1. Створити новий ключ  
2. Завантажити існуючий ключ  
3. Змінити режим шифрування (поточний: GCM)  
4. Зашифрувати файл  
5. Дешифрувати файл  
6. Запустити тест продуктивності  
7. Симулювати атаку підміни даних  
8. Переглянути логи  
0. Вихід  
  
Виберіть опцію: █
```