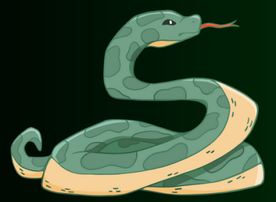
SDU UNIVERSITY

Home About Contact

QORGAN

Secure File Encryption System

PRESENTED BY: ALKHAKIM, YERGAZY, LUKMAN



Alkhakim
Frontend

Yergazy
Crypto

Lukman
Backend

Our Team

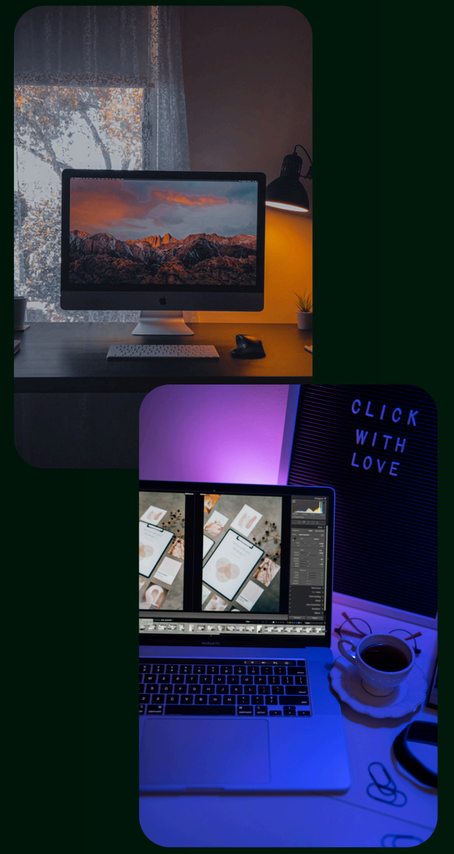
INTRODUCTION

Problem statement:

People exchange files online constantly — through email, cloud storage, or flash drives — and these files can be intercepted or changed. Many cryptography tools exist but are complicated to use.

Our goal:

Create a simple and accessible platform where a user can encrypt, decrypt, sign and verify files without installing complex software.



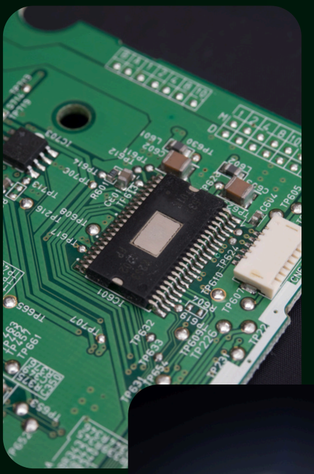
Cryptographic Components

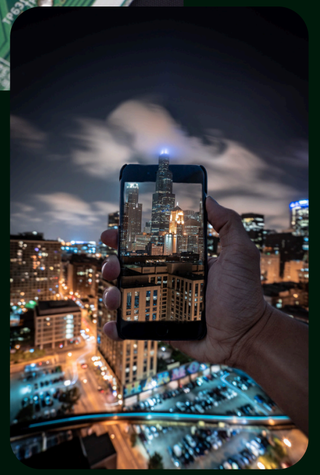
Component	Purpose
AES-256-GCM	Fast encryption + tampering detection
RSA-OAEP	Safely protects the AES key
RSA-PSS	Industry-standard digital signature
PBKDF2	Password-based key protection

For security:

- GCM = integrity check
- PSS = prevents signature forgery
- PBKDF2 = slows brute-force attacks
- No hardcoded keys
- Temporary files use random UUID names

Architecture





Our system has two interfaces:

- Web application for regular users — drag, click, download
- CLI tool for developers and advanced tasks

Why hybrid architecture:

AES is fast for encrypting large files. RSA protects the AES key. They work together.

Architecture

How encryption works:

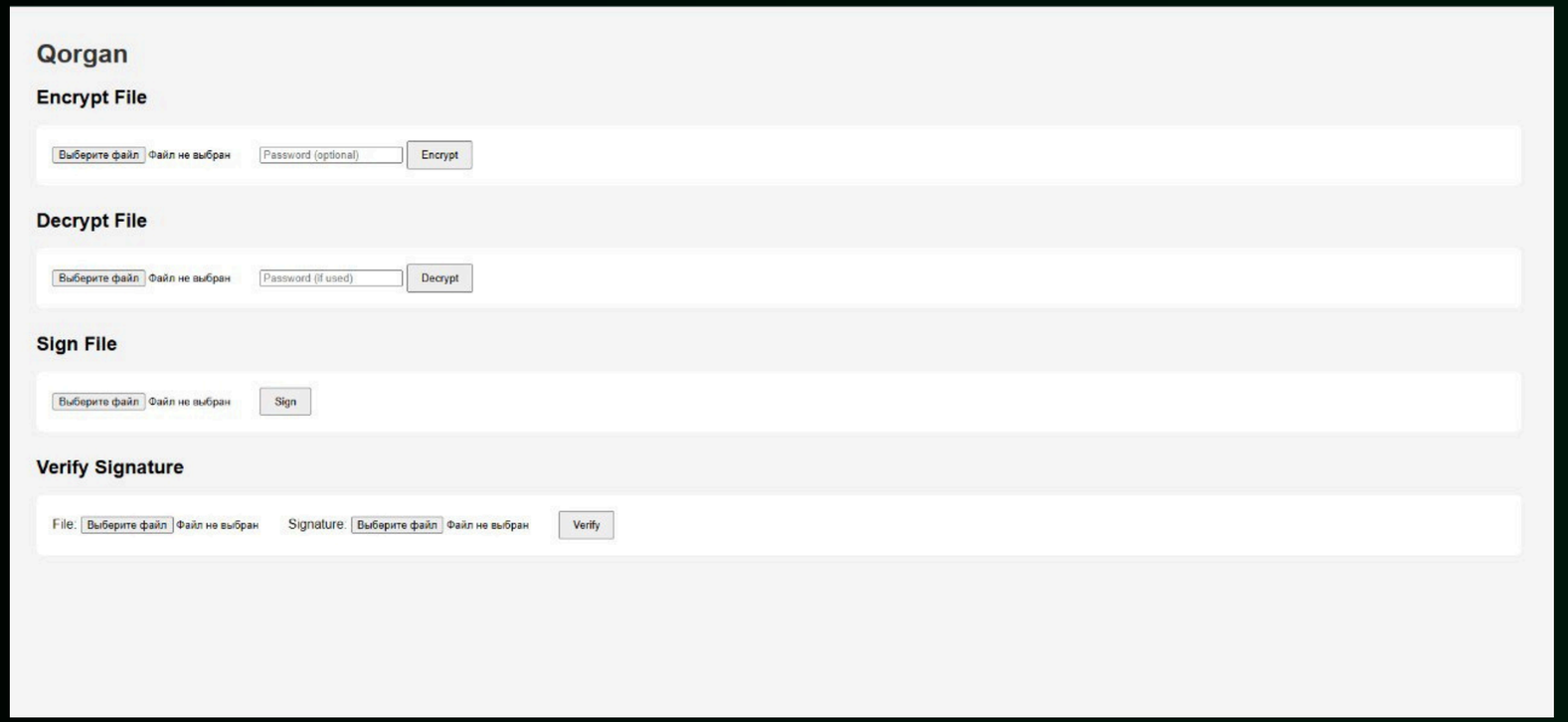
1. User uploads file →
2. System generates AES key →
3. File encrypted with AES-GCM →
4. AES key encrypted using RSA-OAEP →
5. Result packaged and returned as .bin

How decryption works:

1. User uploads .bin →
2. RSA decrypts AES key →
3. AES decrypts file →
4. Original file returned

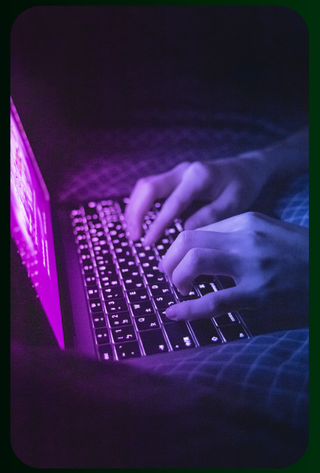
The cryptographic logic is stored in separate modules. The web interface communicates through temporary file paths, and nothing is stored permanently.

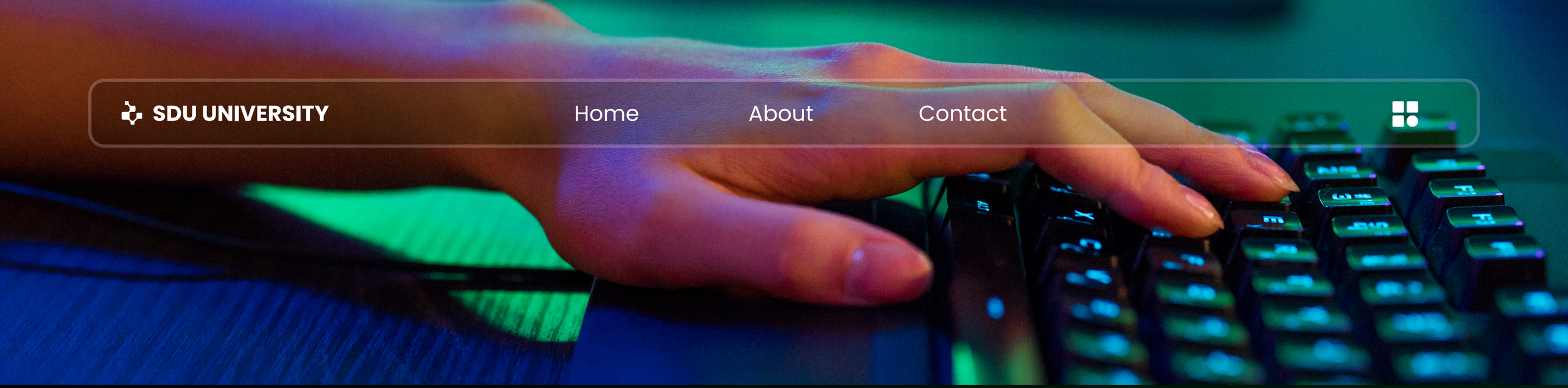
Live Demo


Qorgan
Encrypt File
Выберите файл Файл не выбран
Password (optional)
Encrypt
Decrypt File
Выберите файл Файл не выбран
Password (if used)
Decrypt
Sign File
Выберите файл Файл не выбран
Sign
Verify Signature
File: Выберите файл Файл не выбран
Signature: Выберите файл Файл не выбран
Verify

Conclusion

In conclusion, we built a secure, fast, and simple platform for file protection. This project helped us understand real-world cryptography and its challenges. Strong security becomes valuable only when it is easy to use. Thank you.





THE END

PRESENTED BY: ALKHAKIM, YERGAZY, LUKMAN