Project Proposal Format

Project Title: Secure File Encryption System

Team Members:
[Zhetpiisov Alkhakiim] (GitHub: @Alkhakim828) - Role: [Frontend]
[Yergazy Abdullayev] (GitHub: @itsYergazy) - Role: [Crypto]
[Lukman Bulatkan] (GitHub: @Lukaluky) - Role: [Backend]

Project Option: 2

Brief Description: This project focuses on building a hybrid cryptographic system that allows users to encrypt files, decrypt them, generate digital signatures, and verify authenticity.
The solution is implemented both as a browser-based application and a command-line tool, making encryption accessible to different categories of users.

Cryptographic Components: AES-256-GCM, RSA-2048 with OAEP, RSA-PSS (SHA-256), PBKDF2-HMAC-SHA256

Architecture Overview: The platform uses a hybrid architecture: AES encrypts file content while RSA protects the AES session key using OAEP. The backend, built using Python, exposes both a CLI and a Flask-based web interface. Users interact with the Web UI to upload files, while the CLI enables automation and developer-level use.