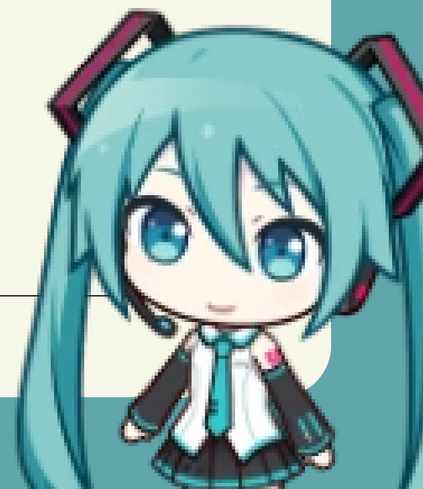
CryptoVault Suite

Inkar Khairatkyzy/ MAT364

Secure Authentication • E2E Messaging • File Encryption • Blockchain Audit



What is CryptoVault Suite?

A comprehensive cryptographic system that implements:

- **Secure authentication with MFA**
- **End-to-end encrypted messaging**
- **Password-based file encryption**
- **Blockchain-backed audit logging**

Motivation

Understand cryptography fundamentals by building everything manually.
Implement real security components.

Problem statement

Modern apps need multiple security guarantees:

- **Confidentiality**
- **Integrity**
- **Authentication**
- **Auditability**

Project goal

make a one unified, auditable cryptographic suite

Architecture

UI (Streamlit)

↓

Application Modules

↓

Crypto Core (custom + standard)

How Modules Communicate? through auth issues session tokens; messaging uses identity keys, not sessions; file encryption is offline-capable; blockchain logs security-relevant actions only

Cryptographic Components Used

Hashing & Integrity: SHA-256, HMAC-SHA256
Key Derivation: Argon2id, PBKDF2-SHA256, HKDF-SHA256
Authentication & MFA: TOTP , SHA-256
Blockchain Primitives: Merkle Trees, Proof-of-Work (SHA-256)
Randomness & Safety: CSPRNG, Constant-time comparison

System Components

Python 3.13, cryptography library
Web UI: Streamlit
Cryptographic Core: Custom SHA-256, Merkle Trees Implementations
Testing & Validation: Pytest Test Suite (116 tests)

Testing

```
tests/test_files_encrypt.py::test_encrypt_decrypt_directory_roundtrip PASSED [ 88%]
tests/test_files_integrity.py::test_hash_and_merkle_root_roundtrip PASSED [ 89%]
tests/test_files_integrity.py::test_merkle_proof_and_verify PASSED [ 90%]
tests/test_files_integrity.py::test_tamper_detection PASSED [ 91%]
tests/test_files_secure.py::test_password_encrypt_decrypt_roundtrip PASSED [ 92%]
tests/test_files_secure.py::test_password_decrypt_tamper_detection PASSED [ 93%]
tests/test_messaging.py::test_ecdh_shared_secret_matches PASSED [ 93%]
tests/test_messaging.py::test_hkdf_session_key_length PASSED [ 94%]
tests/test_messaging.py::test_aes_gcm_encrypt_decrypt PASSED [ 95%]
tests/test_messaging.py::test_ecdsa_sign_verify PASSED [ 96%]
tests/test_messaging.py::test_end_to_end_encrypt_decrypt PASSED [ 97%]
tests/test_messaging.py::test_ephemeral_envelope_send_receive PASSED [ 98%]
tests/test_pow.py::test_difficulty_to_target_bounds PASSED [ 99%]
tests/test_pow.py::test_meets_difficulty_and_mine_small_bits PASSED [100%]

============================================================ 116 passed in 8.65s ============================================================
```

Security Analysis

Strengths:

- ✅ Strong Cryptographic Foundations
- ✅ Defense-in-Depth Authentication
- ✅ End-to-End Security
- ✅ Data Integrity & Auditability
- ✅ High Test Coverage

Additional Recommendations:

- ⚠️ Hardware-Backed Key Storage
- ⚠️ Stronger MFA Options
- ⚠️ Memory Safety Improvements

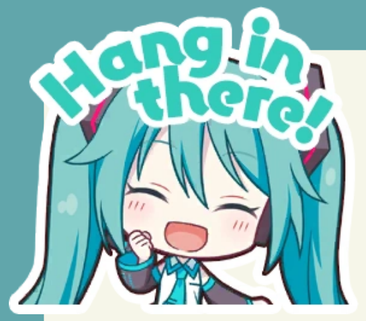
CryptoVault Suite uses modern, standards-based cryptography, MFA, authenticated encryption, integrity verification, and auditable logging to mitigate password attacks, MITM, tampering, replay, and unauthorized access risks.

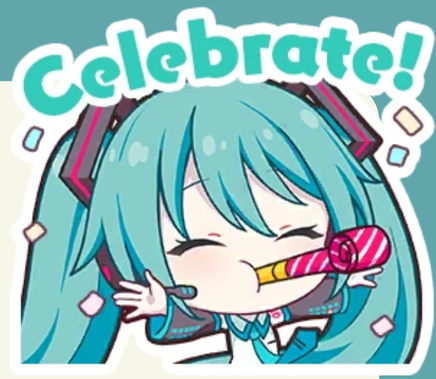
Challenges Faced

Technical Obstacles:

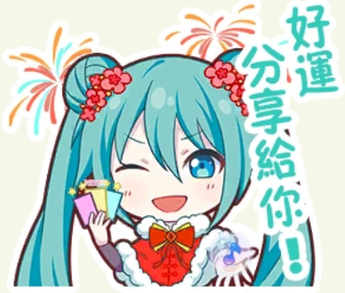
Static ECDH → derive session key via HKDF
v1 format used raw SHA-256→ v2 format with PBKDF2-SHA256 master key
label normalization bug→ stripping _private.pem and _public.pem
no hardcoded Keys→ Master keys derived via PBKDF2
random values → Replaced all random.* with secrets.*

Demo





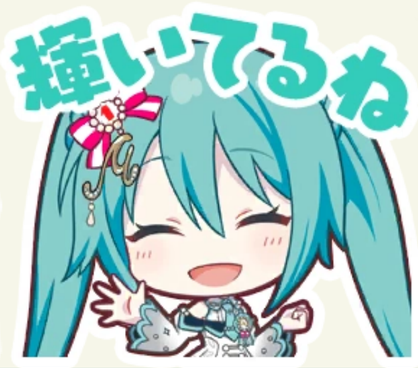
Thank you for semester!

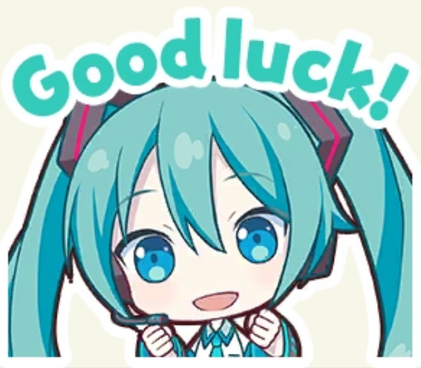


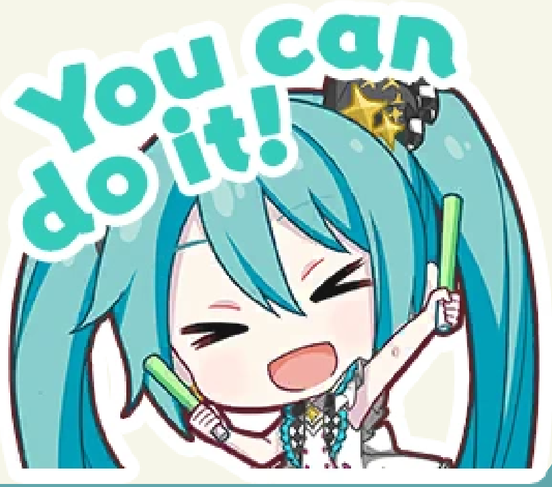
‘good luck to you’

I’ll always keep saying what a wonderful teacher and person you are!
Thanks for your kindness, engagement and hardwork!
Happy new year an good luck

this song for you







Thanks for attention!