Investigation Report – Quantum Conundrum

Breach Case: Megacorp Quantum Encryption

System Target: Obscurarium Realm Defense Systems

Objective: Break the "unbreakable" quantum-proof cipher

Summary

Megacorp Quantum claimed that its system was impossible to break. The encryption protecting the Obscuran Key was fully compromised.

Assessment

System Fully Compromised Key Findings:

- Public key decoded
- Seed algorithm understood
- 7 transformation layers reversed
- File decrypted
- Flag recovered: OS{BENDER}

Impact: The Obscuran Key is no longer secure.

Public Key Analysis Encoding: Base64 Decoded: 24.07.2025|megacorp@quantum.com

Issue: Not a real public key; provides no security.

Seed Generation

Seed components:

- Email
- Date
- Timestamp
- Hardcoded salt (PublicSalt)

Weaknesses: Predictable, no Key Derivation Function, easy to reproduce. Transformations Seven reversible transformations were used.

First three:

1. Ring rotation

2. Add constant

3. Subtract constant - All provide obfuscation, not true security.

Decryption & Flag

The encrypted file was fully decrypted.

Flag: OS{BENDER}

Security Vulnerabilities

- Fake public key

- Hardcoded salt

- Weak keystream

- No integrity check

- Deterministic encryption

Recommendations

Use industry standard cryptography:

- Real public/private keys

- Proper key derivation (Argon2/PBKDF2)

- Random salt

- Authenticated encryption (AES, GCM, ChaCha20, Poly1305)