A03: Crypto Treasure Hunt

Decrypt, Discover, and Verify

Prof. Joerg Osterrieder

Spring 2026

Assignment Overview

Learning Objectives

- Apply basic cryptographic techniques (ciphers, hashing)
- Experience digital signature verification firsthand
- Understand the relationship between public keys, signatures, and message integrity
- Reason about cryptographic security in a physical setting

Assignment Details

- Time: 50 minutes
- Format: Groups of 3–4 students
- Difficulty: Medium
- Points: 50

Grading Breakdown

- Decryption: 15 pts
- Location/clue: 10 pts
- Signature verification: 15 pts
- Security reflection: 5 pts
- Presentation: 5 pts

A03:

digital-ai-finance.github.io/crypto-economics/assignments/A03_crypto_hunt/instructions.html

Step 1: Decrypt the Message

15 min — 15 pts

Steps

1. Receive your encrypted puzzle sheet
2. Choose your difficulty level: Easy, Medium, or Hard
3. Use the provided cipher key for your chosen level
4. Decrypt the message character by character
5. The decrypted message reveals a physical location in the building

Difficulty Levels

- **Easy**: Simple substitution cipher
- **Medium**: More complex substitution
- **Hard**: Multi-step cipher

Tip

Start with Easy if you're unsure. The important thing is to understand *how* the cipher works, not just to solve it fast.

A03:

digital-ai-finance.github.io/crypto-economics/assignments/A03_crypto_hunt/instructions.html

Step 2: Find the Physical Clue

10 min — 10 pts

Steps

1. Go to the location revealed by your decrypted message
2. Find the hidden card at that location
3. The card contains:
   - A message
   - A public key
   - A digital signature

Stay Together

Move as a group. You'll need everyone back at your desk for the verification step.

What You're Simulating

- In the real world, you receive messages with digital signatures
- The question is: was this message really sent by who it claims?
- The card simulates receiving a signed digital message

A03:

digital-ai-finance.github.io/crypto-economics/assignments/A03_crypto_hunt/instructions.html

Step 3: Verify the Signature

20 min — 15 pts

Steps

1. Hash the message using the method on the verification worksheet
2. Apply the public key to the signature (following worksheet instructions)
3. Compare your result with the hash of the original message
4. If they match: the signature is **valid** (authentic)
5. If they don't match: the signature is **forged** (tampered)
6. Record your conclusion and reasoning

Key Insight

Digital signatures prove two things: (1) the message hasn't been altered, and (2) only the holder of the private key could have created this signature.

Materials

- Verification worksheet
- Calculator
- The card from Step 2

A03:

digital-ai-finance.github.io/crypto-economics/assignments/A03_crypto_hunt/instructions.html

Step 4: Security Reflection

5 min — 5 pts

Reflection Questions

1. Why can't someone forge a valid signature without the private key?
2. What would happen if the message was altered after signing?
3. How does this relate to transaction verification on a blockchain?

Presentation (5 pts)

- Brief summary of your decryption approach
- Signature verification result and reasoning
- Answer to one reflection question

Connection to Blockchain

Every transaction on Bitcoin or Ethereum is digitally signed. Nodes verify signatures exactly like you just did — ensuring only the wallet owner authorized the transaction.

A03:

digital-ai-finance.github.io/crypto-economics/assignments/A03_crypto_hunt/instructions.html

Tips & Key Concepts

Cryptographic Primitives

- **Cipher**: Transforms plaintext to ciphertext (and back)
- **Hash**: One-way function, fixed-length output
- **Digital signature**: Created with private key, verified with public key
- **Public/private key pair**: Mathematically linked, cannot derive private from public

Real-World Applications

- HTTPS/TLS uses digital signatures to verify website identity
- Bitcoin: every transaction is signed by the sender's private key
- Ethereum: smart contract calls include sender's signature
- Code signing: software updates are signed to prevent tampering

Remember

Encryption protects *confidentiality*. Signing protects *integrity* and *authenticity*. They are different operations!

A03:

digital-ai-finance.github.io/crypto-economics/assignments/A03_crypto_hunt/instructions.html

Get Started

Assignment Page

digital-ai-finance.github.io/crypto-economics/assignments/A03_crypto_hunt/instructions.html

All Assignments

digital-ai-finance.github.io/crypto-economics/assignments/index.html

Grab your puzzle sheet and start decrypting!

You have 50 minutes to decrypt, discover, verify, and reflect.