CSE 539: Applied Cryptography

Spring 2015

Class:                   Date:  4/14

Activity 1: Encipher Decrypt

Alice sends the message to Bob.
Bob decrypts the message.

Confidentiality with Enciphered Data
Homomorphic Encryption

\[ E_{K_1}(x) + E_{K_1}(y) \equiv E_{K_1}(x+y) \]

+ may not be same as +
- Beg to differ.\textsuperscript{16}  
- Some it to bed, to we.
- Zucchini j.r.
- Alice and a problem.
- Comprising with Zucchini funciona.
program object code

(No source available proprietary)

disassembly possible

may be possible to convert to C
Obfuscate the source code

Disassemble the binary to make it unreadable
Obfuscation

- Lexical transformation
- Control order transformation
- Data transformation/randomization
- Opaque predicates
Bitcoin

digital currency

not digital cash
21 million

- Limited quantity
- Anyone can make
- No one controls
- Current

BTC

Bitcoin