Angela Fogel

CS625 Cryptograpyy

Digital Cash Programming Project Proposal

April 29, 2014

OBJECTIVE

Implement a digital cash system including encryption methods such as secret splitting, bit commitment and blind signatures.

1. PROGRAMS – three separate .cpp files that will communicate through the MOrder objects
   1. Customer program
   2. Merchant program
   3. Bank program
2. OBJECTS
3. Class MOrder

Ustring; (randomly generated unique string)

Amount; (amount of money order)

NameAdd; (will be split and XOR’d to identify the Customer)

BankSig; (bank signature

1. LIBRARIES
2. Chilcat C++ (CkCrypt.2, CkCert.h)
3. Crypto C++