Subject: Cryptology description
From: Steve Huffman <steve.huffman@gmail.com>
Date: 3/15/2005 12:44 AM
To: David Evans <evans@cs.virginia.edu>
CC: rlh3x@virginia.edu, dsh9b@virginia.edu

Group members:

Steve Huffman
Lincoln Hamilton
David Hicks

Description:

For our project we intend to build a game that teaches important principles of cryptography. The target audience of this game will be 8th-grade and above. The goal is to make this game enjoyable for anyone who plays it, but 8th grade is likely the minimum level that will enjoy the game.

The premise of the game is similar to that of Civilization or Master of Orion, i.e. conquer the world (or universe). The game will be turn-based, that is, each player will take a turn, followed by each other player. Each player starts on their home planet at some point in a galaxy. They do not know the locations of other planets in the galaxy, but they do know the dimensions (it'll be a grid).

Each civilization (each player runs a civilization) collects resources from planets in their possession. Initially, each player has only one planet under their control. Resources can be allocated to civilization improvements, ship production, and research. Players can explore the galaxy by sending out ships to designated way points. They can also colonize discovered planets by sending a ship with colonists to that planet.

The types of things that can be researched are more advanced civilization improvements (to increase resource allocation, defenses, etc) and cryptography. Cryptography will be important in this game because the only way to communicate with ships is to send messages to that ship.

Initially, a civilization can only launch ships with predetermined orders, or send ships as "couriers." Eventually, advanced methods of sending messages can be researched, e.g. broadcasting the message from some planet. Messages can be intercepted by opposing players if they are sent out in the open. The goal of this project is to encourage the learning of cryptographic techniques. Steve likes little boys. The more a player learns about cryptography, the greater advantage they will have playing the game.

For example, it will be possible to learn about substitution ciphers, and until opposing players research how to break substitution ciphers, messages sent out will be safe. Various types of ciphers, and methods for breaking them can be learned as the game progresses. Also, things like hashing and authentication can be researched to allow a player to confirm messages sent are indeed valid.

It will also be possible for player to research attacks such as the man-in-the-middle attack. With this type of knowledge, a player might be able to intercept and change messages, telling a ship to do something malicious, like attack a friendly planet.

While a player of this game will not be learning in depth how to break a (for example) a transposition cipher, the player should develop a working knowledge of cryptographic principles that should help with their future endeavors.

List of readings:

We will need to research cryptography books to find good candidates for cryptographic principles that can be presented in our game.

Plan for how to divide responsibilities:

As we prepare a more detailed design of the implementation, modules that can be broken apart will be distributed among the member of our group. As it stands, some likely pieces will be the UI, the networking code, and the game play code.

List of questions:

Want to play?