Senior Independent Study in Computer Science

THE COLLEGE OF
WOOSTER

Abstracts
2013

****

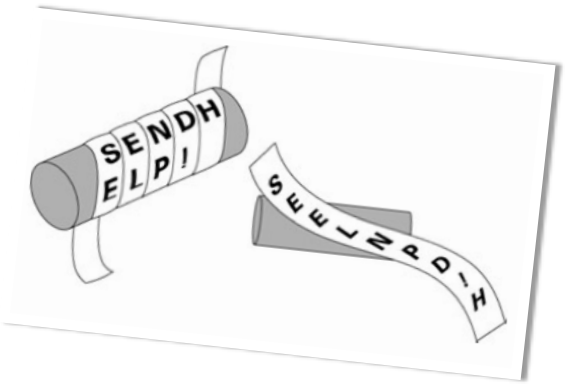
Spencer Hall (Mansfield OH)

Computer Science and Mathematics double major

Optimizing Integer Arithmetic for Public Key Cryptography

(advised by Drew Pasteur, Jim Hartman, Mathematics and Sofia Visa, Computer Science)

Public key cryptography describes a family of systems that allow for secure communication between two parties in the presence of eavesdroppers. We examine the history of cryptography and how the advent of public key cryptography irreversibly changed the science. The Diffie-Hellman key exchange protocol and the RSA cryptosystem and their applications are described in detail, as well as the mathematical theory behind them. The concept of radix representations and radix-sensitive arithmetic algorithms are explored. We create a simple arbitrary precision integer arithmetic system in Java and explore how arithmetic algorithm choices affect the performance of RSA implementations and RSA-related arithmetic functions.



****

Matthew Lambert (Monroeville PA)

Computer Science and Mathematics double major

An Agent-based Model of Influenza Within a College Population

(advised by Drew Pasteur, Mathematics and Sofia Visa, Computer Science)

Predicting the severity of a disease outbreak is an important task for health personnel and college administrators. Influenza is a disease that is commonly transmitted amongst college students. While traditional methods of mathematical prediction utilize systems of differential equations to predict results at the macro level that can be compared readily to historical disease data, agent-based models attempt to detail individual interactions on a daily basis. Agent-based models contain independent agents that follow a few given rules, so there is room for change and experimentation that would be difficult with the traditional mathematical models. Through these rules, one hopes to discover the underlying behavior of the system at hand. Specifically, how disease spreads throughout a population of these agents, given some number of initially infected agents. Once parameters are established so that normal runs produce results consistent with the mathematical models, the agent-based model can be modified, so different results can be seen from different behaviors. Here, we create an agent-based model of influenza with a population of roughly 2000 agents, and measure the effectiveness of two simple methods of lessening the severity of an outbreak.

****

Benn Snyder (West Salem, OH)

Computer Science major

Computer Vision: Object Recognition and Human-Computer Interaction

(advised by Denise Byrnes, Computer Science)

This thesis focuses on computer vision and gesture-based human-computer interaction. In examining computer vision, the project covers existing computer vision systems, including OpenNI/NITE and libfreenect. It explores topics such as identifying humans and objects in scenes, recognizing gestures and context-specific movement, and more general scene analysis. The results of the computer vision work are applied to human-computer interaction. The project examines different types of user interfaces and the applicability of gesture-based interaction to those interfaces. One goal is a generic system for controlling user interfaces using a vision-based gesture system. The included software, consisting of three separate projects, covers both high-level HCI and low-level interaction with vision sensor device drivers. HighNI is a set of Java modules for OpenNI and NITE 1.5. It abstracts the existing Java classes to a higher level and provides some skeleton examples for gesture callbacks. OpenNI2-FreenectDriver is a bridge driver that connects OpenNI2's driver interface to libfreenect's API. It allows OpenNI2 to use Kinect hardware on non-Windows platforms where Microsoft's SDK is not available. FreeNUI is a new framework for natural user interaction, based around libfreenect and OpenCV. It is an experimental project that explores interface design and C++11 language features.