"Attacking Wireless Network Security"
Andrew Courtney (Computer Science)
Advised by Denise Byrnes (CS)
Abstract
This study examines wireless network security and focuses on its vulnerabilities. It then moves on to examine the AirCrack software suite and how it can crack wireless network security. Test networks are set up and cracked using AirCrack. This study attempts to discover which network security is the hardest to crack, therefore being the best security protocol.

"GraffiWii The Wiimote as a Text Entry Device"
Joseph Henrich (Computer Science)
Advised by Sofia Visa (CS)
Abstract
In this Independent Study, a program for Linux that converts particular movements of the Wiimote into typed letters, GraffiWii, is created. Additionally an alphabet is designed specifically for use in this study. Unlike similar research, GraffiWii does not use the Sensor Bar which therefore gives the user more flexibility in using the Wiimote as a character entry device. The challenge is to use only the force data and still obtain a reliable text entry device. The analysis presented in this manuscript shows that the force data sent by the Wiimote allows for accurate detection of simple movements and rotations.

"Secret, Secrets Are So Fun, If They're Not For Everyone!"
Ellen Wagner (Computer Science and Mathematics)
Advised by Sofia Visa (CS) and John Breitenbucher (Math)
Abstract
Cryptology is the science of both cryptography and crytoanalysis, also known as the making and breaking of codes. This paper traces the history of codes from their origins up to the modern day standard AES, the Advanced Encryption Standard. This paper focuses on the internal functions of AES and the implementation of AES in software. Both the encryption and decryption algorithms of AES are implemented and the process to find the inverse operations is discussed in detail. A simplified version of AES is also discussed to investigate differential crytanaalysis. Differential crytanaalysis is one way of breaking AES by finding possible key values based on a specific difference between two plaintexts. The final section goes into brief detail of how differential crytanaalysis is applied to the full AES algorithm and is future work for this paper.
Abstract
The application of real-world physics in computer graphics helps to create realistic animations and simulations. There exists various approaches to modeling the dynamic draping behavior of woven cloth in such simulations. The mass-spring cloth structure provides an intuitive approach to modeling cloth in real-time, interactive animations. This thesis attempts to describe and create a mass-spring cloth simulation with a robust interface which allows for experimentation and improvement upon the mass-spring structure. The created software is an extensible object oriented approach which includes the ability to model full customized cloth shapes and arbitrarily complex, deformable, 3D objects. Extensions include a cloth tearing feature and the selection of numerical integration techniques for experimentation.

Comparing Numerical Integration Methods in a Simulator for the Draping Behavior of Cloth
Michael Liberatore and Dr. Denise Byrnes (Advisor)

Simulation Interface

- The simulation interface supports the use of the physics engine to simulate cloth behavior.
- Spring and particle control
- Numerical integration techniques
- Force control, including wind, particle size, and weight
- Collision detection

Numerical Integrators

- Euler method
- Runge-Kutta
- Adams-Bashforth

Result

- The cloth simulation provides a robust interface for experimentation.
- The simulation includes collision detection and interaction.

Conclusion

A comprehensive study of the effect of different numerical integration methods on the simulation of cloth behavior is presented. The results indicate that the Runge-Kutta method provides the best performance in terms of accuracy and stability. The simulation is a valuable tool for the study of cloth behavior in interactive applications.

References