

San Diego State University

Department of Linguistics and Oriental Languages

Topics

Ling 496: Language and Codes

Codes

Verifiability

Public Keys

Diffie-Hellman

Anonymity

Authentication

Nonrepudiation

Digital Cash

RSA

The central premise of Dan Brown's novel, *Digital Fortress*, is an "unbreakable" code whose very existence threatens the code-breaking supremacy of the NSA (National Security Agency).

Do such unbreakable codes exist? What makes codes completely secure, if anything does? How does the language of a message play a role? What do cryptographers do? How do their most powerful tools, computers, change the nature of code-cracking?

The second part of the course will deal with the enormous changes in the field of cryptography due to issues of trust raised by the Internet, as described in dramatic fashion by Tim May:

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation. — The Crypto-Anarchist Manifesto

Website

<http://www-rohan.sdsu.edu/~gawron/crypto>

Prerequisites

Completion of General Education requirement in Foundations II.A., Natural Sciences and Quantitative Reasoning.

Grading

Grading will be based on exercises/projects a take-home midterm and final.