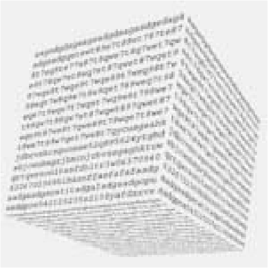
Crossroads
The ACM Student Magazine



Introduction

by ***William Stevenson***

One can hardly turn on the television or open a credit card statement lately without seeing messages warning of the risk of identity theft. Your identity, financial information, and the files on your computer are all more vulnerable than ever before to theft. Although a paper shredder is a useful investment for the offline world, the expanded use of networked communication and e-commerce presents new risks of information being intercepted or flat-out stolen. In order for people to engage in e-commerce safely, or even safely use the Internet at all, it is vital that information be kept private and secure. The technology that provides for such safe communication is called cryptography, and it is one of the oldest, but hottest areas of applied research.

In this issue of *Crossroads*, we study this enabling technology, and the various applications that it makes possible. In our first article, "Security, Anonymity, and Trust in Electronic Auctions," Jarrod Trevathan discusses the various ways in which online auctions, such as those carried out at eBay, are inherently vulnerable to abuse. In addition, Trevathan discusses the main concerns in online auctions, namely, the security of the auction process, the anonymity of thebidders, and the degree of trust between the auctioneer and the bidders.

Nick Papanikolaou discusses a new area of cryptographic research in his article "An Introduction to Quantum Cryptography." Papanikolaou describes the way in which cryptographic systems are judged; just as in the case of ironclad safes, cryptosystems are evaluated with respect to the amount of time that it takes to break them. It has been challenging to create cryptosystems that have security independent of computational power or time, but quantum cryptography presents an avenue for such a solution. In addition to describing quantum cryptography, Papanikolaou gives a thorough discussion of the basics of cryptography, useful for the reading of subsequent articles in this issue.

RSA is one of the most widely used cryptographic techniques, making it a primary target for attack by cryptanalysts, both of the white and black hat variety. Due to the importance of RSA, we present two articles describing attacks on it: "An Introduction to Side Channel Cryptanalysis of RSA" by Artemios Voyiatzis and "Timing Attacks on RSA: Revealing Your Secrets through the Fourth Dimension" by Wing Wong. In the first article, Voyiatzis describes side channel cryptography, namely, information channels apparent in the physical implementation of the cryptographic algorithm that carry information about the key or data used. Following this, the author describes ways in which researchers have coped with this fact to keep their systems secure. In the subsequent article, Wing Wong goes into considerable detail regarding how timing attacks on RSA are performed and possible defenses against them.

Finally, in "Obfuscation of the Standard XOR Encryption Algorithm," veteran *Crossroads* author Zachary Kissel describes XOR encryption, a popular symmetric encryption algorithm. Kissel then describes a modification to the algorithm that borrows some concepts from the Data Encryption Standard (DES) that he calls Random Rotating XOR (RRX) encryption, and analyzes its strengths and weaknesses.

Please stop by our web site, **http://www.acm.org/crossroads**, to see an additional online-only feature article "Micropayment Token-Making Schemes" by Jian Dai . Dai's article describes the requirements and motivations for micropayment schemes and compares two of the more popular ones, PayWord and MicroMint. Following this, Dai describes other schemes, including a hybrid of PayWord and MicroMint called PayFair. We hope that in reading this issue, you gain an appreciation for the mathematics going on in the background to keep your data safe.

Biography

William Stevenson (**billstevenson@acm.org**) is a Ph.D. student in the Applied Cognitive Science Laboratory in the School of Information Sciences and Technology at the Pennsylvania State University. His main research interests are in cognitive modeling and high performance scientific computing. In his spare time, Bill enjoys cooking, the outdoors, and working on his Mac. He has served as Editor in Chief of *ACM Crossroads* since July 2001.