PRINCETON ACM / IEEE-CS CHAPTERS
DECEMBER 2005 JOINT MEETING

Cryptologic Algorithms

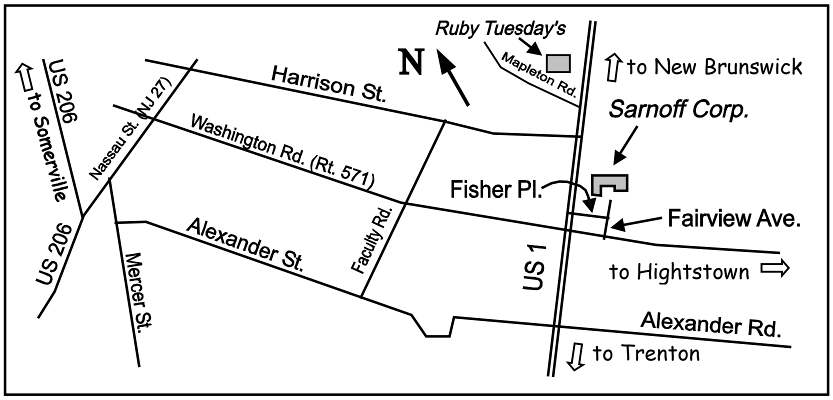
Jonathan Low

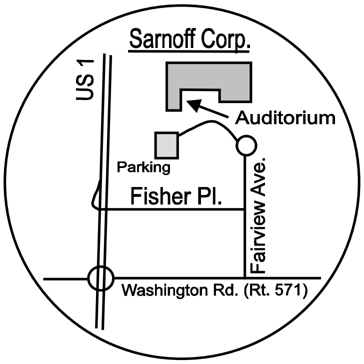
This talk will be an overview of secure communication protocols, including the following topics:

- Zero knowledge proof protocols using graph theory.
  - ➠ How does Alice prove to Bob that she is in fact Alice, without giving Bob enough information to allow Bob to prove to Carol that Bob is in fact Alice?
- Key creation protocol using exponentiation in a finite field and the difficulty of calculating discrete logarithms in finite fields.
  - ➠ How do Alice and Bob establish a cryptologic key over an unsecure channel, without giving Eve, the eavesdropper, enough information to allow Eve to figure out the key?
- Secure communication without a shared crypto key using the difficulty of factoring large composite numbers having two large prime factors.
  - ➠ How do Alice and Bob establish secure communication over an unsecure channel, without a shared crypto key and without public key cryptosystem infrastructure?
- Digital signatures.
  - ➠ How to sign an electronic document such that a court of law can determine that the signature is authentic, not forgeable, not reuseable, cannot be repudiated, and that the document has not been altered?
- Message digests and message authentication codes using one-way hash functions.
  - ➠ How do you make sure a file has not been altered?
- Secure communication without a shared crypto key using the difficulty of factoring large composite numbers having two large prime factors.
  - ➠ How does the RSA public key cryptosystem work?
- Probabilistic encryption.
  - ➠ How to defeat the cryptanalyst's chosen plain text attack on a public key cryptosystem.

Jonathan Low is a Principal Engineer for BAE Systems.

Date: Thursday, December 15, 2005, 8:00 pm (Refreshments at 7:30 pm)
Place: Sarnoff Corp., Routes 1 and 571, Princeton, NJ
Information: Rebecca Mercuri (609) 895-1375, Dennis Mancl (908) 582-7086
On-line info: `http://www.acm.org/chapters/princetonacm`





All ACM / IEEE-CS meetings are open to the public. Students and their parents are welcome. There is no admission charge, and refreshments are served.

A pre-meeting dinner with the speaker is held at 6:00 p.m. at Ruby Tuesday's Restaurant on US 1. Please send email to **princetonacm@acm.org** in advance if you plan to attend the dinner.