



## **IEEE Southern Minnesota Section Meeting**

**Speaker:** Jeff Remfert  
IBM Corp.

**Topic:** Cryptography

**Date:** Monday, May 12

**Time:** 6:30 pm -- *pizza*  
7:00 pm -- *presentation*

**Place:** Mann Hall  
Mayo Medical Sciences Building  
321 3rd Avenue SW  
Rochester, Minnesota

## **Cryptography: Basics & Applications**

*By Jeff Remfert*

Today businesses are replacing paper documents (or forms) and manual document exchange processes with digital documents and online transactions. Business benefits of computer networks include increased operating efficiency and wider, easier contact with customers, business partners, and suppliers. Computer networking has also entered the home in the form of online banking and online shopping.

Performing business transactions and transmitting information over networks present issues related to document control and security. How are business and personal identities authenticated? How is the integrity of digital information maintained? How is transmitted information kept private? How do you prevent a transaction from being refuted? The common denominator in the solutions to these problems is cryptography.

It is useful to contrast how document control and security issues are handled in the paper world versus how they will be (or are being) solved in the digital world. Paper documents, along with the postal system, solve document control and security issues in the following way: authentication is done via company letter head, written signature, and postmark; integrity is ensured by use of physical seals; privacy is ensured by using a sealed envelope and/or secure courier delivery; and, finally, preventing a transaction from being refuted (i.e., non-repudiation) is accomplished via written signatures and/or registered mail.

Digital documents can provide similar document control and security characteristics with the use of cryptographic techniques: for a digital document, authentication is performed via public key cryptography;

integrity is ensured via modification detection codes or message digests; privacy is ensured via encryption; and non-repudiation is accomplished with digital signatures and time-stamps.

Basic cryptographic algorithms employed are: secret key (or symmetric) encryption, public key (or asymmetric) encryption, and secure hash (or message digest). Secret key encryption requires each communicating party to share the same key. Public key encryption requires each party to generate a key-pair: a private key and associated public key. Private keys are kept secret, but public keys can be widely distributed. A secure hash is a one-way function that takes an arbitrary-length message and produces a fixed length hash value (or message digest). A secure hash is used to ensure the integrity of a message (or document). Secure hash and public key encryption operations can be used together to generate and verify digital signatures.

Associated with public keys are certificates (or digital IDs). A public key certificate is a digital document which associates a public key with its owner. The certificate contains a public key, the name of its owner, the owner's organization and address, the name of the certificate issuer, a serial number, and validity period. The issuer is a trusted party called a certification authority (CA). To "bind" the certificate contents, the certificate is digitally signed by the CA. The most visible certification authority today is VeriSign ([www.verisign.com](http://www.verisign.com)). The U.S. Postal Service has expressed intent to become a CA. Also, individual companies will have the capability to establish their own intra-company CAs.

Cryptography is being integrated into software application products such as groupware and secure e-mail, as well as Web servers and browsers. A secure communication protocol that uses cryptography is Secure Sockets Layer (SSL). Next will be applications integrating secure payment protocols such as Secure Electronic Transaction (SET) -- the VISA and MasterCard joint specification for secure bankcard transactions.

Export of products containing data encryption capability is restricted by the U.S. Government. Many countries restrict importation of such products. Developers of products containing data encryption capability should be aware of government restrictions and export license requirements that apply to their products.

**Jeff Remfert** is an Advisory Engineer with IBM Corp. Since 1990 he has worked in the area of cryptography -- first integrating a hardware-based implementation of cryptography into the AS/400, and more recently integrating a software-based implementation of cryptography. Remfert has a B.S. in Electrical Engineering from the University of North Dakota.

## IEEE Southern Minnesota Section Officers

Chair:	Ron Jensen	253-3887	ron@rchvmw2.vnet.ibm.com
Vice Chair:	Jeff Brown	253-6020	jd_brown@vnet.ibm.com
Secretary:	Bill Gorder	253-1409	w.gorder@ieee.org
Treasurer:	Steve Kerchberger	253-4047	s.kerschberger@ieee.org
Computer Society:	Duane Wenzel	253-1035	d.j.wenzel@ieee.org
	Matt Graham	284-9551	mgraham@mayo.edu
Newsletter:	Chris Kimble	253-7571	c.kimble@ieee.org
Membership:	Tim Wolf	455-4304	t.wolf@ieee.org
PACE:	Dick Hall	282-7085	dick.hall@ieee.org
Student Activities:	Noelle Sesta	253-8058	nsesta@vnet.ibm.com

**The Institute of Electrical  
and Electronics Engineers, Inc.  
Southern Minnesota Section**

**Dated Material -- Please Deliver Immediately**

**Non-Profit**  
U.S. Postage Paid  
Permit #511  
Rochester, MN

## Section Election -- Proxy

Officers of the Southern Minnesota section of the IEEE will be elected at our May meeting. The following candidates have been nominated:

		<i>Write-In Candidate</i>
<input type="checkbox"/>	Chair: Ron Jensen	_____
<input type="checkbox"/>	Vice Chair: Rob Harveland	_____
<input type="checkbox"/>	Secretary: Bill Gorder	_____
<input type="checkbox"/>	Treasurer: Steve Kerchberger	_____

You may attend the May meeting to vote for these candidates, or for any eligible write-in candidate. You may also vote by completing the above form, and returning the entire newsletter to Bill Gorder (6751 Country Club Road SW, Rochester, MN 55902) before May 10. Check a box to vote for the nominated candidate, or write in the name of any eligible member. **Sign your name** below the mailing label. Your ballot is confidential.