



# THE 1997 RSA DATA SECURITY CONFERENCE

## SPEAKER BIOGRAPHY

### CRYPTOGRAPHERS' TRACK

Symmetric Cipher Design and Implementation

Speaker: **Michael Wiener**

Cryptographic Advisor

Entrust Technologies Thomas Public Relations

1270 6th Avenue

New York, NY 10020

Phone: 212-332-7800

Fax: 212-332-7801

Email: [jennifer@nythomaspr.com](mailto:jennifer@nythomaspr.com)

### Company Background:

Nortel Secure networks supplies Entrust, a unique security solution scalable to any size network with fast software-based encryption and digital signature services, on Windows, Macintosh and UNIX systems. A high-level API allows easy integration into applications such as E-mail. Entrust provides fully automated key management allowing a common security architecture across applications. Entrust Technologies develops the Entrust family of software security products for encryption and digital signature with fully automated key management. A high-level API allows easy integration into applications such as e-mail, electronic funds transfers, and database transactions. Entrust also works on any size client/server networks and on Windows, Macintosh or UNIX platforms.

### Presentation Overview:

This presentation will address the fundamentals principles of symmetric block cipher design and implementation, including a survey on encryption algorithms and a discussion on CAST program.

### Speaker Background:

Since graduating from the University of Waterloo with a Bachelor of Applied Science in Electrical Engineering in 1986, Michael Wiener has worked for Bell-Northern Research in Ottawa. His research and practical work in cryptology includes cryptanalysis of block ciphers and public-key cryptosystems, design of secure cryptographic protocols, design of practical public-key infrastructures and key management systems, and fast implementations of public-key cryptosystems.

**PRESENTATION**