Cryptographic Hash Workshop
October 31 – November 1, 2005

Don B. Johnson, *Entrust CygnaCom*
djohnson@cygnacom.com

BIOGRAPHY: Don B. Johnson has over 18 years of experience in cryptographic standards and cryptosystem design, analysis, and review. He has presented ideas on cryptography and future resiliency at the Public Key Solutions and AES conferences. He represents Entrust at the ANSI X9F1 Cryptographic Tools working group. He is the editor of Draft ANSI X9.82 Part 1 Random Numbers – Overview and Basic Principles. Previously, he was an editor of the NIST Key Establishment Schemes Draft 2.0. He was the Certicom and the IBM representative to the ANSI X9F1 and X9F3 working groups and has made technical contributions to many standards including IEEE P1363 and the X/Open Crypto API. Don was the editor of ANS X9.62 ECDSA and the final editor of ISO/IEC 15946-3 Elliptic Curve Key Establishment.

Don was a co-author with Alfred Menezes and Scott Vanstone of "ECDSA: The elliptic curve digital signature algorithm," author of "ECC, Future Resiliency and High Security Systems," presented at Public Key Solutions 1999 and "AES and Future Resiliency: Further Thoughts" presented at the Third AES Conference, 2000. He was the lead author of two articles on the Common Cryptographic Architecture published in the IBM Systems Journal Volume 30, Number 2, 1991; a co-author of an article on Public Key Extensions to the Common Cryptographic Architecture published in the IBM Systems Journal Volume 32, Number 3, 1993; and the lead author of an article on the Commercial Data Masking Facility algorithm, which was published in the March 1994 issue of the IBM Journal of Research and Development.

Don has worked on methods for Public Key Validation, improvements to key agreement methods, the Commercial Data Masking Facility (CDMF) algorithm, the RACF Passticket algorithm and the Reverse Signature concept. He was the author of IBM Common Cryptographic Architecture API. He was a major contributor to the hardware and software cryptographic architectures of the IBM Transaction Security System. He helped design the IBM CD-ROM Showcase security subsystem.

Don has an M.S. in Computer Science from Union College, Schenectady, New York and a B.A. in Mathematics from Oakland University, Rochester, Michigan. He is a member of the IACR (International Association for Cryptologic Research). He has received a Certicom Innovation award, an eighth plateau IBM Invention Achievement award, a third plateau IBM Manassas Author Recognition program, an IBM President's Patent Award for two patents of strategic significance to IBM and an IBM Outstanding Innovation Award for the Common Cryptographic Architecture API