Distinguished Seminar ACM and Comp. Sci.

Cryptography: From Enigma to Elliptical Curve Cryptography

Dr. Donald Costello

University of Nebraska

September 16, Tuesday, 12:30 to 1:30pm

Room: CS 209

Abstract - The history of cryptography can be likened to a reawaking history of mathematics and computer science. The story of cryptography goes back 4000 years and some of the mathematics employed goes back as long. This talk will address the history of cryptography beginning with the Enigma used by the Germans in WWII and broken by world famous Mathematician/ Computer Scientist Alan Turing. It will continue down to today's advanced crypto systems such as RSA, PGP and Elliptic Curve cryptography. The lecture will point out the key role that cryptography plays in the future of e-commerce and the new products and ways of doing business that results when secure communications through cryptography is available.

Brief Bio - Don Costello has had a mixed career splitting his time between Universities and Business. He helped start three Computer Science Departments and three University Information Technology facilities (University of Nebraska, University of Wisconsin – Oshkosh and Madison and Colorado State University). He has taught undergraduate and graduate courses and has done work in research areas of Statistical Computing, Performance Modeling, Standards for Learning Objects and Managing Intellectual Property. He is a 40-year member of ACM and is a fellow of the British Computing Society. He has lectured all over the United States as well as in England, Ireland, Austria, Germany, India and Sri Lanka. He also held a four-year Carnegie Foundation grant to investigate how IP is managed in Universities around the World. In business career he has managed IT facilities, founded and sold two firms and consulted with over 100 firms throughout the world. His recent consulting includes five years consulting on ERP systems, SAP, as well as being a Technical Consultant on .com and e-Learning projects.

Don currently holds a position as a Senior Lecturer and NCITE scholar at the University of Nebraska and is working on the importance of standards in modeling the large systems needed to support e-learning environments.