CRYPTOGRAPHY AND DATA SECURITY
Overview of panel discussion

Michael Willett, session chairman
Department of Mathematics
University of North Carolina at Greensboro

Cryptography is the science of secret writing. It has been used since the dawn of writing itself to conceal messages from an adversary. Throughout history, the use of cryptography has been largely confined to diplomatic and military communications. But in the last 10 years the tremendous advances in communication technology have created a serious need for cryptographic protection of private sector communications. Electronic funds transfer systems and satellite voice/digital networks are particularly vulnerable to compromise, without the use of cryptography. Recognizing the need for data protection apart from national security concerns, the National Bureau of Standards issued a call for a data encryption algorithm in 1973. During the subsequent discussions and debates, the mathematicians and computer scientists involved realized that cryptography was not an established science in the unclassified literature. They began the task of creating the foundations for this young discipline. In 1977, the NBS published the Data Encryption Standard (DES). Its use is required to protect sensitive governmental information not related to national security. Several national and international standards organizations have also adopted the DES.

The DES is a classical scheme (even though it is designed to encrypt computerized (binary) data) in the sense that the two communicants must first exchange a secret quantity called the key, by other means, before a secure communication link can be established. This key exchange is typically done manually or at the time the encryption equipment is manufactured.

In 1976, a radically different approach to cryptography, called public key, was introduced by Diffie and Hellman at Stanford University. No prior, secret exchange of a key is needed. Instead, a specially designed encryption function (one for each communicant) is publically distributed to everyone, thereby allowing instantaneous use of this function without the exchange of a secret key. The encryption function is designed so that calculating its inverse is an intractible problem. The function designer possesses secret design information (called trapdoor information) which makes the inversion (decryption) problem easy. Of course, this design information is not distributed.

The distinquished panelists for this session will discuss the past, present, and future of cryptography in the private sector. These panelists are David Kahn, author of THE work on the history of cryptography (Codebreakers), Miles Smid, developer of cryptography-related standards at NBS, and Stephen Kent, consultant to government and private industry in the area of cryptography.