Emerging Applications of Cryptography

Çetin Kaya Koç
Oregon State University

Cryptography: The art/science of designing and breaking ciphers.

Traditionally, (secret-key) cryptography was used by the military and diplomatic services for providing secure communication.

In 1976, public-key cryptography was invented, providing techniques for signing and authenticating digital data.

As information super-highways are developed, cryptographic techniques are needed for privacy and authentication of digital data.

Outline

secure mail
secure communications
network authentication
electronic voting
electronic notary
digital money (digital wallet)
data distribution

Secure Communication

security for real-time electronic links
local area networks
link encryption
cellular (and ordinary) phones and faxes

Goals

message privacy
sender and recipient authentication
nonrepudiation

Tools

key-agreement protocols
secret-key cryptosystems
public-key cryptosystems
digital signatures
certificates
Electronic Voting
- general elections
- shareholders meetings
- secure distributed computation

Goals
- anonymity
- fairness
- accountability

Tools
- RSA-based mathematics
- blind signatures
- sender untraceability protocols

Digital Money (Digital Wallet)
- replacement for paper money
- more flexible than credit cards

Goals
- anonymity
- untraceability
- fairness
- dividability
- transferability
- off-line (from bank) operations
- universality

Tools
- more RSA-based mathematics
- zero-knowledge protocols
- secure hardware tokens

Data Distribution
- conditional access TV
- software distribution via CD-ROM
- information bulletin boards

Goals
- broadcast operation (TV, CD-ROM)
- message privacy
- selective reception

Tools
- secret-key cryptography
- public-key cryptography
- secure hardware

Research Interests in Cryptography
- Design of cryptographic algorithms
- Analysis of cryptographic algorithms
- Design of cryptographic protocols
- Hardware and software implementations
- Applications of cryptography