Computer Science 308-547A
Cryptography and Data Security

NUMBER THEORETICAL CONCEPTS

- The Euclidean Algorithm : computing GCDs
- Computing multiplicative inverses mod n
- Exponentiation mod n
- Probabilistic Primality Testing
- Notion and determination of a generator (primitive element) mod p
- Quadratic Residues and non-residues mod p and mod n
- Legendre and Jacobi symbols
- Extracting square roots mod p
- The Chinese Remainder Theorem
- Extracting square roots mod n

SECRET-KEY CONCEPTS

SECRET-KEY ENCRYPTION

Classical Cryptography
- Shift Cipher
- Substitution Cipher
- One-time-pad and stream ciphers
- Enigma : how it works, what's good and bad about it ?

The Data Encryption Standard
- Description of DES : understanding the structure and tables
- DES Modes of Operation : what are they good and bad for ?
- Advanced Encryption Standard (AES)

Shannon's Information Theory
- Perfect Secrecy
- Entropy
- Spurious Keys and Unicity Distance

Secret Sharing Schemes
- Shamir's Threshold Scheme

Key Exchange
- Goal
- Diffie-Hellman Public Key Exchange
- The Discrete log problem/assumption
- The Diffie-Hellman assumption

Pseudo-random Generation
- Pseudo-random Bit Generation : Definition and Examples
- Indistinguishable Probability Distributions
- The Blum-Blum-Shub Generator (x^2 mod N)
- The Blum-Micali Generator (g^x mod p)
- Stream cipher from PRBG
- Pseudo-random function generators : definition and construction
- Bloc cipher from PRΦG

SECRET-KEY AUTHENTICATION

Message Authentication Codes
- Introduction and definitions : MACs
- Example from DES' CBC mode
- Universal Hashing Functions
- Perfect or nearly perfect MACs

SECRET-KEY IDENTIFICATION

- Identification procotol from PRΦG

PUBLIC-KEY CONCEPTS

PUBLIC-KEY ENCRYPTION

The RSA System and Factoring

- Introduction and definitions : Public-key Cryptography
- The RSA Cryptosystem
- Implementing RSA
- Factoring Problem/assumption
- RSA assumption
- Attacks On RSA
  - $\Phi(n)$
  - The Decryption Exponent
  - Partial Information Concerning Plaintext Bits
- The Rabin Cryptosystem

The ElGamal Cryptosystem and Discrete Logs

- The ElGamal Cryptosystem
- The Discrete log problem/assumption
- The Diffie-Hellman assumption

Probabilistic Encryption

- Goldwasser-Micali system : the Quadratic Residuosity Problem
- Blum-Goldwasser cryptosystem from BBS Pseudo-random Bit Generator

PUBLIC-KEY AUTHENTICATION

Signature Schemes

- Introduction and definitions : digital signature schemes
- The RSA Signature Scheme
  - forging random messages
- The ElGamal Signature Scheme
  - the "El Gammal" assumption
  - forging random messages
  - attacks on secret exponent
- The Digital Signature Standard
  - the "DSS" assumption
- Undeniable Signatures : how are they diferent ?

Hash Functions

- Signatures and Hash Functions
- Collision-free Hash Functions
- The Birthday Attack
- A Discrete Log Hash Function
- Extending Hash Functions
- MD4 / MD5 / SHS

PUBLIC-KEY IDENTIFICATION

Identification Schemes

- General framework
- The Schnorr Identification Scheme based on Discrete Logs
- The GQ Identification Scheme based on RSA
- what is good and bad about these ID schemes ?