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

- Prime fields $\mathbf{F}_p$
- Primitive elements over $\mathbf{F}_p$
- Probabilistic Primitive elements finding
- (Irreducible) Polynomials over $\mathbf{F}_p[x]$
- Probabilistic Irreducible Polynomial finding
- General finite fields $\mathbf{F}_q$ with $q=p^n$

CRYPTOGRAPHIC CONCEPTS

Set up	Security \ concept	encryption	authentication	identification
Secret key	Information theory	Vernam's One-time-pad	Wegman-Carter's One-time-authen.	One-time-identification
	Complexity theory	PRBG, PRΦG, DES, AES,…	PRBG, PRΦG, DES, AES,…	PRBG, PRΦG, DES, AES,…
Public key		PKC : RSA, BG, ElGamal	Signature : RSA, ElGamal, DSS	GQ, Schnorr, ZK: RSA, ElGamal

SECRET-KEY CONCEPTS
INFORMATION THEORETICAL SECURITY

SECRET-KEY ENCRYPTION

Classical Cryptography

- Shift Cipher
- Substitution Cipher
- One-time-pad and stream ciphers

Shannon's Information Theory

- Perfect Secrecy
- Entropy
- Spurious Keys and Unicity Distance

SECRET-KEY AUTHENTICATION

Message Authentication Codes

- Introduction and definitions : MACs
- Universal Hashing Functions (Wegman-Carter)
- Perfect or nearly perfect MACs

SECRET-KEY *IDENTIFICATION*

- One-time-identification protocol

<u>SECRET-KEY CONCEPTS</u>
<u>COMPLEXITY THEORETICAL SECURITY</u>

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)
- Pseudo-random function generators : definition and construction

SECRET-KEY ENCRYPTION

- Stream cipher from PRBG
- Randomized bloc cipher from PRΦG

SECRET-KEY AUTHENTICATION

- Stream authentication from PRBG
- Random authentication from PRΦG

***SECRET-KEY** IDENTIFICATION*

- Stream identification from PRBG
- Random Identification from PRΦG

Block ciphers' modes of Operation

- ECB, CBC, OFB, CFB
- Relation to pseudorandomness
- what are these modes good and bad for ?

The Data Encryption Standard

- Description of DES : understanding the structure and tables
- Sizes and resistance to cryptanalysis
- encryption-decryption
- MAC from DES’ CBC mode
- Identification from DES

The Advanced Encryption Standard (AES)

- Description of AES : understanding the structure and functions
- Sizes and resistance to cryptanalysis
- encryption-decryption

Key Exchange

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

PUBLIC-KEY CONCEPTS
COMPLEXITY THEORETICAL SECURITY

PUBLIC-KEY ENCRYPTION

Introduction and definitions : Public-key Cryptography

The RSA System

- The RSA encryption/decryption methods
- Factoring Problem/assumption, RSA assumption
- Attacks On RSA
    - $\Phi(n)$
    - The Decryption Exponent
    - Partial Information Concerning Plaintext Bits
- The Rabin Cryptosystem

Probabilistic Encryption

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

The ElGamal Cryptosystem

- The ElGamal encryption/decryption methods
- Breaking ElGamal PKC = breaking Diffie-Hellman assumption

PUBLIC-KEY AUTHENTICATION

Introduction and definitions : digital signature schemes

The RSA Signature Scheme

- signing and verifying methods
- forging random messages

The ElGamal Signature Scheme

- signing and verifying methods
- the “El Gammal” assumption
- attacks on secret exponent
- forging random messages

The Digital Signature Standard

- signing and verifying methods
- the DSS assumption

Hash Functions

- Signatures and Hash Functions
- Weak and Strong Collision-free Hash Functions

PUBLIC-KEY IDENTIFICATION

Identification Schemes

- proving knowledge of a plaintext
- proving knowledge of a signature
- proving knowledge of private information

Zero-Knowledge Interactive Proofs

- ZK proof for Graph isomorphism
- ZK proving knowledge of RSA plaintext
- ZK proving knowledge of ElGammal plaintext

Identification Schemes

- Public Identification: 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 ?