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

CRYPTOGRAPHIC CONCEPTS

<table>
<thead>
<tr>
<th>Set up</th>
<th>Security concept</th>
<th>encryption</th>
<th>authentication</th>
<th>identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret key</td>
<td>Information theory</td>
<td>Vernam’s One-time-pad</td>
<td>Wegman-Carter’s One-time-authen.</td>
<td>One-time-identification</td>
</tr>
<tr>
<td></td>
<td>Complexity theory</td>
<td>PRBG, PRΦG, DES, AES,…</td>
<td>PRBG, PRΦG, DES, AES,…</td>
<td>PRBG, PRΦG, DES, AES,…</td>
</tr>
<tr>
<td>Public key</td>
<td>PKC : RSA, BG, ElGamal</td>
<td>Signature : RSA, ElGamal, DSS</td>
<td>Signature : RSA, ElGamal, DSS</td>
<td>GQ, Schnorr, ZK: RSA, ElGamal</td>
</tr>
</tbody>
</table>
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
SECRET-KEY CONCEPTS
COMPLEXITY THEORETICAL SECURITY

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 ElGamal 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 ?