Cryptography

Final Exam Review

Arkady Yerukhimovich

December 9, 2024

Outline

Practical Block Ciphers

- Objectives:
  - Confusion-diffusion paradigm
  - Avalanche effect

Practical Block Ciphers

- Objectives:
  - Confusion-diffusion paradigm
  - Avalanche effect
- Substitution-Permutation Networks (AES as an example)
  - Construction – know the main steps (key-mixing, substitution, permutation)
  - Intuition on why steps are necessary

Practical Block Ciphers

- Objectives:
  - Confusion-diffusion paradigm
  - Avalanche effect
- Substitution-Permutation Networks (AES as an example)
  - Construction – know the main steps (key-mixing, substitution, permutation)
  - Intuition on why steps are necessary
- Feistel Network (DES as an example)
  - Be able to simulate by hand
  - Be able to explain how to invert
  - Why we don't need invertible round function?

Practical Block Ciphers

- Objectives:
  - Confusion-diffusion paradigm
  - Avalanche effect
- Substitution-Permutation Networks (AES as an example)
  - Construction – know the main steps (key-mixing, substitution, permutation)
  - Intuition on why steps are necessary
- Feistel Network (DES as an example)
  - Be able to simulate by hand
  - Be able to explain how to invert
  - Why we don't need invertible round function?
- Key-length extension
  - Meet-in-the-middle attack
  - Why 2DES fails to add security
  - 3DES construction and its security

Outline

1. Constructing Block Ciphers

2. Public-Key Crypto
   - Number Theory and Group Theory
   - Key Exchange and Encryption
   - Digital Signatures

Number Theory and Group Theory

- Modular Arithmetic
- Euclidean algorithm, gcd, Euler ϕ function
- Chinese Remainder Theorem
- Groups: $\mathbb{Z}_p^*, \mathbb{Z}_N^*$, Quadratic residues mod p
  - Definition of a group
  - modular arithmetic in base (mod N) and exponent (mod $\phi(N)$)
  - cyclic groups, order (of elements and groups)
- Be able to do simple number theory by hand

Cryptographic Hardness Assumptions

- Hard Problems
  - Factoring
  - RSA
  - Discrete LOG (DLOG)
  - CDH, DDH
  - Understand relationships between these hard problems

Cryptographic Hardness Assumptions

- Hard Problems
  - Factoring
  - RSA
  - Discrete LOG (DLOG)
  - CDH, DDH
  - Understand relationships between these hard problems
- Private-key crypto from these assumptions
  - PRG, PRF from DDH
  - CRHF from DLOG

Public-Key Revolution

- The limitations of private-key crypto
- Key distribution center (KDC)
- Goals of public-key crypto

Public-Key Revolution

- The limitations of private-key crypto
- Key distribution center (KDC)
- Goals of public-key crypto
- Key Exchange
  - Security definition
  - Diffie-Hellman key exchange
    - Construction
    - Why it's secure

Public-Key Encryption

- Security definitions (CPA, CCA), difference from private-key definitions
- El Gamal Encryption
  - Construction – be able to simulate by hand
  - Relationship to DH-KE
  - Why is it secure

Public-Key Encryption

- Security definitions (CPA, CCA), difference from private-key definitions
- El Gamal Encryption
  - Construction – be able to simulate by hand
  - Relationship to DH-KE
  - Why is it secure
- Plain RSA encryption
  - Construction – be able to simulate by hand
  - Why it is not secure
  - Padded-RSA – be able to explain how this avoids above attacks

Public-Key Encryption

- Security definitions (CPA, CCA), difference from private-key definitions
- El Gamal Encryption
  - Construction – be able to simulate by hand
  - Relationship to DH-KE
  - Why is it secure
- Plain RSA encryption
  - Construction – be able to simulate by hand
  - Why it is not secure
  - Padded-RSA – be able to explain how this avoids above attacks
- Hybrid encryption

Digital Signatures

- Objectives – how they are different from MACs
- Security definition
- Applications

Digital Signatures

- Objectives – how they are different from MACs
- Security definition
- Applications
- Plain RSA signatures
  - Construction – be able to simulate by hand
  - Understand attacks on this
  - RSA-FDH
    - Understand construction
    - Don't need to understand proof of security

Hash-based signatures

- Definition of one-way function
- Lamport one-time signature scheme
  - Construction
  - Proof of security

Hash-based signatures

- Definition of one-way function
- Lamport one-time signature scheme
  - Construction
  - Proof of security
- Chain-based signatures
- Tree-based signatures
- How to make this stateless (and what this means)

Exam Procedures

- Exam on Mon., Dec. 16, 12:40-2:40 PM in the classroom
- You may bring 2 pieces of 8.5 x 11 inch paper (back and front) with notes
- No computers, phones, or calculators during exam – bring pens or pencils

Exam format

The exam will contain the following:

1. 10 True/False questions – no partial credit
2. 2-3 compute by hand problems – Number theory, RSA, El Gamal, Feistel
3. 2 long answer questions – definitions, reductions, Encryption, Signatures
4. 1 challenge problem
5. Questions may have multiple parts, complete as much as you can.