MAS 433: Cryptography

Revision

Contents

- Classical ciphers
- Symmetric key encryption
- Hash function and Message Authentication Code
- Public key encryption
- Digital signature
- Key establishment and management
- ~~Introduction to other cryptographic topics~~

1. Classical ciphers

1.1 Caesar cipher

1.2 Substitution cipher, frequency cryptanalysis

1.3 Vigenere cipher

1.4 Transposition (permutation) cipher

2. Symmetric key encryption

- 2.1 One time pad, Shannon's information theory
- 2.2 Block ciphers
  - 2.2.1 Data Encryption Standard (DES), Double DES, Triple DES
  - 2.2.2 Advanced Encryption Standard (AES)
  - 2.2.3 Modes of operation:
  - 2.2.4 Attacks on block ciphers:
    security of Double DES,
    ~~differential and linear cryptanalysis~~
- 2.3 Stream ciphers
  - 2.3.1 Block cipher based stream ciphers
  - 2.3.2 LFSR based stream ciphers
  - 2.3.3 NLFSR based stream ciphers

Block Cipher Introduction

- Information-theoretical security & computational security
- Practical symmetric key ciphers
  - Computational security
  - Kerckhoffs' principle
  - Known-plaintext attack & …
- Block Cipher
  - Iterated structure
    - Round function & round key
    - Key schedule
  - Round function
    - Design strategy: Confusion & diffusion
    - Methods:
      - Substitution-permutation network
      - Feistel network

DES

- DES
  - Feistel Network
    - Always invertible
    - The same network for encryption and decryption
      - The order of the round keys are reversed
  - Key schedule
    - Linear
- Double DES, Triple DES
  - Their security

AES

- Mathematical preliminaries
  - GF(2^8)
  - Polynomials with coefficients in GF(2^8)
- AES
  - Encryption
    - Substitution-Permutation Network
    - Round function
      - different round numbers for different key sizes
    - Key schedule
      - different for different key sizes
  - Two equivalent decryption algorithms
    - One is straight forward inverse
    - Another with modified key schedule

Modes of Operation

- Modes of operations
  - ECB: not strong
    - Parallel computation is possible
  - CBC: strong, the most commonly used
  - CFB
  - OFB: for the same key, all the IVs must be different
  - CTR: for the same key, all the IVs must be different
    - Parallel computation is possible
- Ciphertext stealing for encrypting the partial block
  - ECB
  - CBC
  - Not a problem for CFB, OFB & CTR

Attacks on Block Cipher

- Meet-in-the-middle attack on double DES

- Attacks on block cipher
  - Solving algebraic equations
  - ~~Statistical approach~~
    - *Differential cryptanalysis
    - *Linear cryptanalysis
    - ……..

Important for block cipher design: Sbox (confusion), diffusion

Stream Cipher

- One-time pad → stream cipher
- Two types of stream ciphers
  - Synchronous stream cipher (more popular)
  - Asynchronous stream cipher
- Three main constructions
  - Block cipher based stream cipher
    - CFB, OFB, CTR
  - LFSR based stream cipher
  - NLFSR based stream cipher (now dominative)
- Two widely used stream ciphers
  - A5/1
  - RC4

3. Hash function and Message Authentication Code

- 3.1 Birthday paradox, birthday attack
- 3.2 Cryptographic hash function
  - 3.2.1 Hash function structures
  - 3.2.2 Secure Hash Algorithm (SHA-1, SHA-2)
  - ~~3.2.3 Recent developments on hash function~~
- 3.3 Message Authentication Code
  - 3.2.1 CBC-MAC & CMAC
  - 3.2.2 HMAC
- 3.4 Unconditionally secure MACs

Birthday Attack

- Birthday problem
  - The probability that at least two elements of *n* random elements are the same
- Birthday attack
  - Find a collision of a function *f*
    - Function *f* is non-injective
  - Methods:
    - Direct birthday attack
      - computational & memory complexity $1.17\sqrt{M}$
    - Rho method
      - Reduce the memory complexity

Hash Function

- Cryptographic hash function
  - Aim: Each message digest represents only one message (computationally)
  - Three security requirements
    - Preimage resistance
    - Second-preimage resistance
    - Collision resistance
- Structure
  - Iterated Structure
    - Merkle-Damgard
  - Compression function structure
    - MMO
    - Davies-Meyer
- SHA-1
- SHA-2
  - SHA-224,SHA-256, SHA-384, SHA-512
- ~~SHA-3~~
  - ~~ongoing~~

Message Authentication Code

- Message Authentication Code
  - Compresses a secret key and a message into an authentication tag with fixed length
  - MAC based on block cipher
    - CBC-MAC
    - CMAC (NIST recommendation)
  - MAC based on hash function
    - HMAC (NIST standard)
- Unconditionally secure MAC
  - Each key is used only once

4. Public key encryption

4.1 RSA encryption

4.1.1 RSA algorithm

4.1.2 RSA Implementation:

Primality testing; fast modular exponentiation

4.1.3 Security of RSA:

Integer factorization; other attacks on RSA

4.2 ElGamal encryption

4.2.1 ElGamal algorithm

4.2.2 Algorithms for the discrete logarithm problem

4.3 Message padding:

Optimal asymmetric encryption padding (OAEP)

RSA Encryption

- Public key encryption
  - Allows two parties to communicate secretly without sharing a secret key before communication
- RSA
  - Specifications
  - Implementation
    - Primality testing: Fermat's primality test, Miller-Rabin primality test
    - Extended Euclidean algorithm
    - Fast modular exponentiation
  - Security
    - Integer factorization
      - Dixon's Random Squares algorithm
    - Other attacks
      - Short message
      - Shared public key
      - Small public key
      - Small private key

ElGamal Encryption

- Specification
- Implementation
- Security
  - Discrete logarithm algorithms
    - Shank’s baby-step giant-step algorithm
    - Pollard’s Rho algorithm
    - Pohlig-Hellig algorithm
      - *p*-1 should have a large prime factor
    - Index calculus algorithm
      - Large *p*: 2048-bit *p* for 128-bit security
  - Do not re-use the per-message secret *k*

OAEP

- “Textbook” RSA encryption
  - Deterministic & public encryption algorithm
  - Do not use it practice
- Padding is needed
  - Use the strong OAEP
    - Introduce the randomness into the encryption process

5. Digital Signature

- 5.1 RSA signature scheme
- 5.2 ElGamal signature scheme
- 5.3 Digital Signature Standard (DSS)
  - 5.3.1 Digital Signature Algorithm (DSA)
  - ~~5.3.2 RSA Digital Signature Algorithm~~

- Digital Signature
  - Authentication
    - Everyone can verify
  - Schemes
    - RSA signature scheme
      - padding is needed for message digest
    - ElGamal signature scheme
    - Digital Signature Standards
      - Digital Signature Algorithm
      - ~~RSA digital signature algorithm~~
- Use different keys for digital signature and public key encryption
  - RSA
  - ElGamal
- Application
  - Authenticate digital documents (public key, e-passport …)
  - Signing contract …

6. Key establishment and management

6.1 Key generation

~~6.2 Key establishment with symmetric key cryptography~~

~~6.2.1 Kerberos~~

6.3 Key establishment with public key cryptography

6.3.1 Public key infrastructure (PKI)

6.3.2 Applications: SSL/TLS

6.4 Secret Sharing

6.4.1 Shamir's Threshold Scheme

- Key generation
  - Good entropy source is needed
    - Avoid using the function “random( )” to generate key
  - Apply randomness extractor to enhance randomness
- Key establishment
  - ~~Key establishment using symmetric key cryptography~~
    - ~~Kerberos~~
    - ~~Bellare-Rogaway key establishment scheme~~
  - Key establishment using public key cryptography
    - SSH
    - PKI, public key certificate: authenticate public keys
      - TLS/SSL
- Secret sharing
  - (*n*, *n*) secret sharing
  - Shamir’s secret sharing scheme
  - Threshold public key cryptosystem
    - (*n*, *n*) threshold public key cryptosystem
    - (*t*, *n*) threshold public key cryptosystem
    - ~~(*t*, *n*) threshold ElGamal encryption scheme based on Shamir’s secret sharing scheme~~