MH4311 Cryptography

Revision

The final exam covers

- Lecture 1 to 19
  - All the contents except those marked with ‘*’
- Tutorial 1 to 12
  - All the tutorial questions except those optional questions
- Assignment 3 and 4

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

1. Classical ciphers

- 1.1 Caesar cipher
- 1.2 Substitution cipher, frequency cryptanalysis
- 1.3 Vigenere cipher
- 1.4 Playfair cipher
- 1.5 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)
  - 2.2.2 Advanced Encryption Standard (AES)
  - 2.2.3 Modes of operation
  - 2.2.4 Attacks on block ciphers
- ~~2.3 Stream ciphers~~

One time pad & Information theory

- One-Time Pad
  - Perfect secrecy
- Information theory
  - Entropy
  - ~~Entropy & redundancy of a language~~
  - ~~Unicity distance~~

Block Cipher Introduction

- Information-theoretical security & computational security
- Practical symmetric key ciphers
  - Computationally secure
  - Kerckhoffs' principle
  - Resist known-plaintext attack & …
- Block Cipher
  - Iterated structure
    - Round function & round key
    - Key schedule

DES

- DES
  - 56-bit key, 64-bit block, 16 rounds
  - Feistel network
    - Always invertible
    - The same network for encryption and decryption
      - The order of the round keys are reversed
- Double DES, Triple DES
  - Their security
  - Should use three-key-triple-DES

AES

- Mathematical preliminaries
  - $GF(2^8)$
    - You do not need to know the polynomial being used in $GF(2^8)$ in AES
    - You need to know how to compute the addition, multiplication, and multiplicative inverse in this finite field
  - Polynomial ring with coefficients in $GF(2^8)$
    - You need to know how to compute the addition and multiplication in this polynomial ring

AES

- AES
  - 128-bit key, 10 rounds, 11 round keys
  - 192-bit key, 12 rounds, 13 round keys
  - 256-bit key, 14 rounds, 15 round keys
  - Encryption
    - Substitution-Permutation Network
    - Round function
      - You should know the four operations in each AES round

Modes of Operation

- Modes of operations
  - ECB: not strong
    - Parallel computation of the message blocks
  - CBC: for the same key, the IV needs to be different & unpredictable
    - Reasonably strong when the same IV is reused
    - the most commonly used
    - Parallel decryption
  - CFB: for the same key, the IVs must be different
  - OFB: for the same key, the IVs must be different
  - CTR: for the same key, the IVs must be different
    - Parallel computation is possible
- You need to know how each mode works

Modes of Operation

- Ciphertext stealing for encrypting the partial block
  - ECB
  - CBC
  - Partial block is not a problem for CFB, OFB & CTR
- Message padding for partial block for block cipher in OpenSSL

Attacks on Block Cipher

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

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

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

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)

3.3 Message Authentication Code

3.2.1 CBC-MAC & CMAC

3.2.2 HMAC

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
- Hash function standards
  - SHA-1 (insecure)
  - SHA-2
    - SHA-224,SHA-256, SHA-384, SHA-512
  - ~~SHA-3~~
  - You do not need to know the details of SHA-1 and SHA-2, but you need to know the overall structure, the compression function structure, message block size, message digest size of SHA-1 and SHA-2.

Message Authentication Code

- Message Authentication Code
  - Compress a secret key and a message into an fixed-length authentication tag
  - MAC based on block cipher
    - CBC-MAC (insecure)
    - CMAC (NIST recommendation)
  - MAC based on hash function
    - HMAC (NIST standard)
- You need to know the specifications of the above three MACs.
- You need to know how to attack the CBC-MAC

4. Public key encryption

4.1 RSA encryption

4.2 ElGamal encryption

RSA Encryption

- Public key encryption
  - Allows two parties to communicate secretly without sharing a secret key before communication
- RSA
  - Specification
  - 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

OAEP

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

RSA Blinding

- RSA decryption vulnerable to timing attack
- RSA blinding is needed in applications
  - A one-time secret number is used in decryption

ElGamal Encryption

- Specification
- Implementation
  - Find a generator of a multiplicative cyclic group
- 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 or 3072-bit
  - Do not re-use the per-message secret k

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

5.3.3 ECDSA

- Digital Signature
  - Authentication
    - Everyone can verify; non-repudiation
  - Schemes
    - RSA signature scheme
      - padding is needed for message digest
    - ElGamal signature scheme
    - Digital Signature Standards
      - Digital Signature Algorithm (DSA)
      - RSA digital signature algorithm
      - ECDSA (ECDSA will be given later)
- In ElGamal signature and DSA, one-time secret number is needed
- Application
  - Authenticate digital documents (public key, e-passport …)
  - Signing contract …
- You need to know the details of the above digital signature algorithms
- You need to know how to launch the man-in-the middle attack when the public key is not authenticated

6. Key establishment and management

6.1 Key generation

~~6.2 Key establishment with symmetric key cryptography~~

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

6.4.2 Threshold public key cryptosystem

- Key generation
  - Good entropy source is needed
    - Avoid using the function “random( )” to generate key
  - Try to use the random number generated by the operating system
- Key establishment
  - ~~Key establishment using symmetric key~~ cryptography
    - ~~Kerberos~~
    - ~~Bellare-Rogaway key establishment scheme~~
  - Key establishment using public key cryptography
    - Public key encryption
    - Diffie-Hellman key exchange

- SSH
- TLS/SSL
  - PKI, public key certificate: authenticate public keys
  - You need to know how to read a ciphersuite
  - You need to know how DHE (Ephemeral Diffie-Hellman key exchange) works in TLS
- You need to know how to use RSA or DHE for key exchange in 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~~

7. Elliptic Curve Public Key Cryptosystem

7.1 Elliptic curve over a finite field
7.2 Elliptic curve Diffie-Hellman key exchange (ECDH)
7.3 Elliptic curve digital signature algorithm (ECDSA)

You need to know how to compute the addition in the Elliptic curve group over a finite field.

You need to know the specifications of ECDH and ECDSA.

~~8. Introduction to other topics~~

~~8.1 Post-Quantum cryptography~~

~~8.2 Side-channel attacks~~

Consultation before the exam:

23 Nov, Friday, 2pm to 5pm

30 Nov, Friday, 2pm to 5pm

3 Dec, Monday, 2pm to 5pm

4 Dec, Tuesday, 2pm to 5pm