Final Exam Review Sheet (CS-352 Spring 2024)

This review sheet is an outline of main topics covered in class.

Overview

- **Scope of the exam:**
  - Topics covered *Authentication Protocols, Classical Ciphers, Block Cipher Principles, DES, TwoFish, and AES.*
  - The exam ***does not*** cover any other material covered by the midterm exam **except** where the knowledge of the prior material is related to the new material.
- Be able to answer questions similar and related to the handouts, demos, assignments, quizzes and slides.
- The guidelines to the salient topics are provided below.

Classical Ciphers

- **Do not** need to know the history of cryptography.

- Understand the basic terminology: e.g. plaintext, ciphertext, cryptanalysis etc.

- How are the ciphers classified?

  - Substitution vs Transposition vs Product

  - Stream vs Block

  - Symmetric vs Public Key

- What is the difference between a monoalphabetic and a polyalphabetic cipher?

- Why are attackers more interested in compromising the encryption keys than discovering the content of the specific ciphertext?

- What are the basic building blocks of symmetric cryptography?

- What are the requirements for strong symmetric encryption?

- What is the difference between *unconditional* and *computational security*?

- Be able to encrypt and decrypt using all classical ciphers discussed in class e.g. Cesar, Playfair, Vigenère (with and without autokey), Railfence, etc.
  - **Example:** Encrypt plaintext `sssssdlfjh` using Playfair cipher and key `hello`.

  - **Example:** Decrypt ciphertext `dyucumyed` using Playfair cipher and key `hello`.

  - **Example:** Encrypt `yuiopvbnm` using the Vigenère cipher with autokey and key `midterm`.

Block Cipher Principles and DES

- What is the difference between stream and block ciphers?

- What are confusion and diffusion? Why are they important when designing a block cipher? Give an example.

  - **Example:** Consider a block cipher with a property where if one bit of the key changes, many bits of the ciphertext change. Is this example of confusion or diffusion? Explain.

- What primary techniques are used to achieve confusion and diffusion, respectively?

- What makes a block cipher reversible?

- Understand the ideal block cipher concepts.

  - **Example:** How many possible keys can I have in an ideal block cipher which encrypts 64-bit text blocks?

  - **Example:** What is the size of the key in a 64-bit ideal block cipher?

- How does Feistel cipher perform substitution and permutation?

- What are the advantages of the Feistel cipher network?

- Know and understand how to use all DES-related tables.

  - **Example:** Consider binary key string:
    `00110001101101110000001110011111011101111000010100111100101110100`.
    What will be the first five bits after running this key through PC-1 table?

  - **Example:** What will be the output of S-Box 8 given input 111011

- What important function do S-Boxes perform in DES encryption?

- **Do not** Do not need to know all of the S-Box design criteria but need to know at least a few and describe them.

- What is the important property of block cipher security achieved by swapping two halves of the text block after every round?

- What is the avalanche effect? Why is it important?

- Why not double DES? What is the method of breaking double DES?

- Understand why when using 3DES, it's better to use `EDE` instead of `EEE`.

- What is the difference between differential and linear cryptoanalysis?

Twofish

- What key sizes and block sizes does Twofish support?

- Know that Twofish is based upon a Fiestal cipher structure (as is DES).

- What is the distinguishing feature of Twofish S-Boxes? How do they compare with, say, DES S-Boxes.

- What is the distinguishing feature of Twofish key scheduling algorithm?

Advanced Encryption Standard (AES)

- Compare and contrast AES and DES in terms of security, key size, block size, structure, and the number of rounds.

- Is AES based on the Feistel cipher network?

- Be able to compare and contrast the Fiestal cipher framework to the Substitution Permutation framework.

- Know basic structure of the single AES round.

  - **Example:** What sequence of operations does the first AES round perform?

  - **Example:** How does the last round of AES differ from all other rounds?

  - **Example:** In DES, the number of rounds is fixed. Is the same true of AES?

- Know how to convert a given plaintext into an AES state.

- In the `SubBytes` step, know how to use the Rijnadel S-Box in order to perform substitutions.

  - **Example:** What is the result of substituting byte `AE` into the Rijnadel S-Box?

  - **Example:** What is the result of substituting byte `2F` into the Rijnadel S-Box?

- Understand how the `ShiftRows` step works.

  - **Example:** Suppose `12 34 56 78` is the third row of the state. How will the row be transformed in the `ShiftRows` step.

- Understand how the `MixColumns` step works.

  - **Example:** What is the rationale behind the `MixColumns` step?

  - Given the `MixColumns` matrix and the state, know how to multiply the matrix by the state.

  - Know how to E-table and L-table for performing $GF(2^8)$ multiplication.

    * **Example:** What is `AB` $\times$ `34` in $GF(2^8)$?

- Understand how the `AddRoundKey` step works.

  - **Example:** Given the initial round key `93 1E D7 36 D6 C2 1B D9 D2 01 86 98 EA 07 D2 F5`, write the key in the matrix form, convert the key into four 4-byte vectors W_0, W_1, and W_2, and W_3, and derive vectors W_4, W_5, and W_6, and W_7 for the next round.

Block Cipher Modes

- What are advantages and disadvantages of ECB, CBC, CFB, and CTR modes? Be able to analyse their security, efficiency, etc.

- Be able to prove correctness of given mode (similar to what we did in class).

  - **Example:** Show that CBC cipher mode is correct (e.g. Slide 14 of Block Cipher Modes of Operation Slideset).

- What is the importance of padding? When is it done?

Authentication Protocols (AuthenticationProtocols.pdf)

- What are main issues in authentication protocols (slide 3).

- Know and understand all types of replay attacks (slide 4).

- What are the main countermeasures against replay attacks (i.e. nonces and time stamps)?

- Explain the flow of logic in the Needham-Schroeder and Needham-Schroeder-Lowe protocols (slides 8 - 18).

- What is the vulnerability in the Needham-Schroeder protocol? Explain (slides 9-12).

- Why is it challenging to counter replay attacks with time stamps? (slide 12).

- Explain the flow logic in the Needham-Schroeder Public Key Protocol (15-18).

  - Is there a vulnerability?
  - How do we fix the vulnerability?

- How does one-way authentication work in order to protect email? Does it provide confidentiality? Does it protect against replay attacks?

- Explain why the information transferred through the Web vulnerable (slides 24-25)? Be able to give examples of attacks. How can we protect against such vulnerabilities?

- At what layer does SSL run?

- Know the protocols involved in SSL/TLS and their functions. Do not need to remember the details of the SSL/TLS handshake protocol.

- What services does the SSL/TLS protocol provide?

- Know that SSL fragments messages. Each fragment can be compressed (optionally).

- Does the Heartbleed vulnerability comprise a security flaw in the design of SSL? Explain.
- What are two fundamental ways of protecting passwords (slide 42)?

  - Access control.
  - One-way functions.
- What are hashing and salting?
- How is the password file protected in UNIX (as discussed in class)?