CSCE 4013/5013 Applied Cryptography

Midterm Exam Study Guide

Module 1 – Overview

- What is confidentiality? What is integrity, including data integrity and origin integrity (or authenticity)?

Module 2 – Basic Crypto

- Understand the statistical attack against substitution cipher
- The elements of encryption and decryption process
- Understand the principle of publishing cipher algorithm and keeping keys secret for security
- Understand how key size affects security level: same key for encryption and decryption
- The main feature of symmetric key cryptography: different keys for encryption and decryption
- Be able to list a few well-known algorithms for symmetric key crypto (DES, AES, 3DES)
- The main feature of public key crypto
- Be able to list a few well-known algorithms for public key crypto (RSA, ECC)
- Understand <public key, private key> pair and which is kept secret and is released to public.
- In public key crypto, know which keys to use for providing confidentiality (via encrypting/decrypting)
- Know how one-time pad works
- Understand the tradeoff between security and performance

Module 3 – Secret Key Cryptography

- Basic properties of block cipher: constant key size, constant size input/output, random permutation
- How 3DES works
- Meet-in-the-middle attack
- Be able to analyze the security and cost of simple constructions over DES or a block cipher in general.
- Understand the usage of padding and know how to judge whether a padding method is good or not.
- For CBC mode, know whether IV can be a constant.
- Understand the key advantage of Counter mode over CBC mode
- Be able to list a recommended block cipher
- Be able to describe message content using notations such as m, c, E(), D(), and k.

Module 4 – Public Key Cryptography

- Understand requirement for the size of RSA key
- Know that public key component e can be small but private key component d cannot be small
- Understand the pitfalls when having small e and when encrypting low-entropy messages
- List an encoding standard name for RSA encryption/decryption

- Know the size of message directly encrypted (or directly signed) by RSA cannot exceed the size of modulus n
- Be able to write down the RSA encryption and decryption formula given notations m, c, e, d, n.
- Understand who generates public and private key pair for a user
- Be able to describe message content using notations such as m, c, E(), D(), e, d, and n.
- Comparison between symmetric key crypto and public key crypto

Module 5 – Message Authentication

- Define MAC
- Understand the notations MAC(k,m) and $MAC_k(m)$ which mean the MAC generated using key k over message m
- Basic properties of cryptographic hash: arbitrary size input, constant size output, output is random
- Understand the notation H(m) which is the hash of message m
- List a few well-known hash algorithms: MD5, SHA
- Know the one-way property and the collision resistance property of hash
- Know how to judge whether a given hash algorithm is good or not
- Understand why hash itself cannot be used as the MAC function
- Know how to compute HMAC
- Know how authentication with MAC works
- Know how the RSA signature generation and verification works, under notations m, s, e, d, n.
- Know how digital signature works for message authentication, signing on the hash of a message instead of the message itself and how to verify it
- Combining the knowledge of hash, HMAC, digital signature to judge whether a given authentication algorithm is good or not
- The message formats when achieving different security properties using symmetric key crypto and public key crypto and both

Module 6 – Key Distribution

- Know how to distribute a shared secret key between two parties using public key based encryption and decryption
- Know how D-H protocol works
- Know perfect forward secrecy
- Understand the advantage of using D-H protocol to exchange a session key, and the problem of RSA-based session key distribution
- Recommended size of p for D-H protocol
- Know the role of CA, the main content of certificate, and how CA-based public key distribution works
- Know the security issue with storing a list of trusted CAs in web browsers

Module 7 – Password-Based Security

- Describe why and how to use salt in password storage
- Describe then how password is verified during user login when salted passwords are stored
- Describe dictionary attacks in offline password guessing
- Understand why Salt helps defend against dictionary attacks
- Define PBKDF and why to use an iteration count in the function
- In the password (or master key derived from password) based challenge-response protocol, understand why nonce is used

Module 8 – TLS

- Know the end-to-End security property provided by TLS
- Know that only the server is authenticated and understand why
- Given the process of TLS (except the SYN, SYN ACK, and ACK), understand what each step does
- Know the two ways of distributing the "premaster key"
- Limitations of TLS

Module 9 – Broadcast Authentication

- Know how to use MAC to do broadcast authentication and analyze the tradeoffs between communication and computation/storage cost
- Know how to construct Merkle hash tree
- Know how to use Merkle hash tree to do broadcast authentication