

CS 389 Final Review

Chapter 1: Introduction

- Three goals of security
 - Confidentiality
 - It is probably the most common aspect of information security.
 - It is to protect the confidential information and to guard against those malicious actions that endanger the confidentiality of the information.
 - Integrity
 - Information needs to be changed constantly.
 - Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.
 - Availability
 - The information created and stored by an organization needs to be available to authorized entities.
 - Information needs to be constantly changed, which means it must be accessible to authorized entities.
- Attacks
 - The three goals of security^{3/4}confidentiality, integrity, and availability^{3/4}can be threatened by security attacks.
 - Attacks Threatening Confidentiality
 - Snooping refers to unauthorized access to or interception of data.
 - Traffic analysis refers to obtaining some other type of information by monitoring online traffic.
 - Attacks Threatening Integrity
 - Modification means that the attacker intercepts the message and changes it.
 - Masquerading or spoofing happens when the attacker impersonates somebody else.
 - Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.
 - Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.
 - Attacks Threatening Availability
 - Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.
 - Passive versus Active Attacks
- Cryptography is the science and art of transforming messages to make them secure and immune to attacks.
- Steganography means “secret writing.”

Chapter 2: Mathematics of Cryptography

- Set of integers, binary operations on integers.
- Divisibility
- Common divisors of two integers
- Greatest Common Divisor
 - The greatest common divisor of two positive integers is the largest integer that can divide both integers.
 - When $\gcd(a, b) = 1$, we say that a and b are relatively prime.
- Euclidean Algorithm
 - Fact 1: $\gcd(a, 0) = a$.
 - Fact 2: $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b .
- Extended Euclidean Algorithm
 - Given two integers a and b , we often need to find other two integers, s and t , such that

$$s \times a + t \times b = \gcd(a, b)$$

- The extended Euclidean algorithm can calculate the $\gcd(a, b)$ and at the same time calculate the value of s and t .
 - Linear Diophantine Equation
 - A linear Diophantine equation of two variables is $ax + by = c$.
 - Modular Arithmetic
 - The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n , or Z_n .
 - To show that two integers are congruent, we use the congruence operator (\equiv).
 - Operation in Z_n, Z_n^*
 - Additive Inverse
 - In modular arithmetic, each integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo n .
 - Multiplicative Inverse
 - In Z_n , two numbers a and b are the multiplicative inverse of each other if
- $$a \times b \equiv 1 \pmod{n}$$
- In modular arithmetic, an integer may or may not have a multiplicative inverse.
 - When it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo n .
 - Multiplicative inverses are only defined for square matrices.
- Matrices
 - Additions and Multiplications

- Multiplications are not commutative.
- Determinant
 - The determinant of a square matrix A of size $m \times m$ denoted as $\det(A)$ is a scalar.
 - The determinant is defined only for a square matrix.
- Single-Variable Linear Equations
 - Equations of the form $ax \equiv b \pmod{n}$ might have no solution or a limited number of solutions.
 - We can also solve a set of linear equations with the same modulus if the matrix formed from the coefficients of the variables is invertible.

Chapter 3: Traditional Symmetric-Key Ciphers

- In a symmetric-key cipher, both the encryption algorithm and the decryption algorithm share the same secret key.
- Kerckhoff's principle
 - One should always assume that the adversary, Eve, knows the encryption/decryption algorithm.
 - The resistance of the cipher to attack must be based only on the secrecy of the key.
- Cryptography and cryptanalysis
 - Cryptography is the science and art of creating secret codes, and cryptanalysis is the science and art of breaking those codes.
 - Ciphertext-Only Attack
 - Known-Plaintext Attack
 - Chosen-Plaintext Attack
 - Chosen-Ciphertext Attack
- Substitution Cipher
 - A substitution cipher replaces one symbol with another.
 - Monoalphabetic ciphers
 - The relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.
 - Polyalphabetic ciphers
 - Each occurrence of a character may have a different substitute.
 - The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.
 - Additive Ciphers
 - This cipher is sometimes called a shift cipher or a Caesar cipher.
 - Multiplicative Ciphers
 - The plaintext and ciphertext are integers in Z_{26} ; the key is an integer in Z_{26}^* .
 - Affine Ciphers

- The set is the set of all permutations, and the operation is composition: applying one permutation after another.
 - Using two permutations one after another cannot strengthen the security of a cipher, because we can always find a permutation that can do the same job because of the closure property.
 - Finite Group
 - A group is called a finite group if the set has a finite number of elements. Otherwise, the group is an infinite group.
 - Subgroups
 - Cyclic Subgroups
 - If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.
 - Cyclic Groups
 - A cyclic group is a group that is its own cyclic subgroup.
 - Order of a Group
 - The order of an element is the order of the cyclic group it generates.
 - Equivalently, the order of an element is the smallest power that generates the identity e .
 - Lagrange's Theorem
 - Assume that G is a group, and H is a subgroup of G . If the order of G and H are $|G|$ and $|H|$, respectively, then, based on this theorem, $|H|$ divides $|G|$.
- Rings
 - A ring, $R = \langle \{...\}, \oplus, \otimes \rangle$, is an algebraic structure with two operations.
 - Distribution of \otimes over \oplus .
 -
- Fields
 - A field $F = \langle \{...\}, \oplus, \otimes \rangle$ is a commutative ring in which the second operation satisfies all five properties defined for the first operation except that the identity of the first operation has no inverse.
 - Finite Fields
 - Galois showed that for a field to be finite, the number of elements should be p^n , where p is a prime and n is a positive integer.
 - A Galois field, $GF(p^n)$, is a finite field with p^n elements.

Chapter 5: Introduction to Modern Symmetric-key Ciphers

- A symmetric-key modern block cipher encrypts an n -bit block of plaintext or decrypts an n -bit block of ciphertext. The encryption or decryption algorithm uses a k -bit key.
- To be resistant to exhaustive-search attack, a modern block cipher needs to be designed as a substitution cipher.

- In a full-size key transposition cipher, $n!$ possible keys are needed. So, the key should have $\log_2(n!)$ bits.
- In a full-size key substitution cipher, $(2^n)!$ possible keys are needed. So, the key is $\log_2(2^n)!$ bits long.
- Modern block ciphers normally are keyed substitution ciphers in which the key allows only partial mappings from the possible inputs to the possible outputs.
- P-box (permutation box)
 - A P-box transposes bits.
 - Straight P-Boxes
 - A straight P-box is a P-box with n inputs and n outputs.
 - Compression P-Boxes
 - A compression P-box is a P-box with n inputs and m outputs where $m < n$.
 - Expansion P-Boxes
 - An expansion P-box is a P-box with n inputs and m outputs where $m > n$.
 - A straight P-box is invertible, but compression and expansion P-boxes are not.
- S-Box (substitution box)
 - An S-box is an $m \times n$ substitution unit, where m and n are not necessarily the same.
 - Linear and nonlinear S-boxes.
 - An S-box may or may not be invertible. In an invertible S-box, the number of input bits should be the same as the number of output bits.
- Product cipher
 - A product cipher is a complex cipher combining substitution, permutation, and other components discussed in previous sections.
- Diffusion
 - Diffusion hides the relationship between the ciphertext and the plaintext.
- Confusion
 - Confusion hides the relationship between the ciphertext and the key.
- Diffusion and confusion can be achieved using iterated product ciphers where each iteration is a combination of S-boxes, P-boxes, and other components.
- Feistel Ciphers and non-Feistel Ciphers.
- Non-Feistel Ciphers
 - A non-Feistel cipher uses only invertible components. A component in the encryption cipher has the corresponding component in the decryption cipher.
- Differential Cryptanalysis
 - Differential cryptanalysis is a chosen-plaintext attack.
 - Differential cryptanalysis is based on a nonuniform differential distribution table of the S-boxes in a block cipher.

- Modern Stream Cipher
 - In a modern stream cipher, each r-bit word in the plaintext stream is enciphered using an r-bit word in the key stream to create the corresponding r-bit word in the ciphertext stream.
 - Synchronous Stream Ciphers
 - In a synchronous stream cipher the key is independent of the plaintext or ciphertext.
 - Nonsynchronous Stream Ciphers
 - In a nonsynchronous stream cipher, the key depends on either the plaintext or ciphertext.

Chapter 6: Data Encryption Standard (DES)

- The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).
- The encryption process is made of two permutations (P-boxes), which we call initial and final permutations, and sixteen Feistel rounds.
- The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.
- Key Generation: The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.
- DES Analysis
 - Two desired properties of a block cipher are the avalanche effect and the completeness.
 - Completeness effect means that each bit of the ciphertext needs to depend on many bits on the plaintext.
 - S-Boxes provide confusion and diffusion of bits from each round to the next.
 - P-Boxes provide diffusion of bits.
 - DES uses sixteen rounds of Feistel ciphers. The ciphertext is thoroughly a random function of plaintext and ciphertext.
 - Weaknesses in Cipher Design
 - Weaknesses in S-boxes
 - Weaknesses in P-boxes
 - Weaknesses in Key
 - Weak Keys
 - Semi-weak keys
 - Double DES
 - Using a known-plaintext attack called meet-in-the-middle attack, it proves that double DES improves this vulnerability slightly (to 2^{57} tests), but not tremendously (to 2^{112}).

Chapter 7: Advanced Encryption Standard (AES)

- AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds.
- General design of AES encryption cipher.
- AES was designed after DES. Most of the known attacks on DES were already tested on AES.
 - Brute-Force Attack: AES is definitely more secure than DES due to the larger-size key.
 - Statistical Attacks: Numerous tests have failed to do statistical analysis of the ciphertext.
 - Differential and Linear Attacks: There are no differential and linear attacks on AES as yet.
- AES can be implemented in software, hardware, and firmware. The implementation can use table lookup process or routines that use a well-defined algebraic structure.

The algorithms used in AES are so simple that they can be easily implemented using cheap processors

Chapter 8: Encipherment Using Modern Symmetric-Key Ciphers

- Block Ciphers
 - Modes of Operations
 - Electronic Codebook (ECB) Mode
 - Cipher Block Chaining (CBC) Mode
 - Cipher Feedback (CFB) Mode
 - Output Feedback (OFB) Mode
 - Counter (CTR) Mode
- Stream Ciphers
 - RC4
 - A5/1

Chapter 9: Mathematics of Cryptography (*Part III: Primes and Related Congruence Equations*)

- Primes
 - A prime is divisible only by itself and 1.
 - There is an infinite number of primes.
 - Checking for Primeness.
 - Sieve of Eratosthenes
 - Euler's Phi-Function
 - Euler's phi-function $f(n)$ denotes the number of integers that are both smaller than n and relatively prime to n .
 - Properties:

1. $\phi(1) = 0$.
 2. $\phi(p) = p - 1$ if p is a prime.
 3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
 4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.
 - The difficulty of finding $f(n)$ depends on the difficulty of finding the factorization of n .
- Fermat's Little Theorem
 - p is a prime, a is an integer such that p does not divide a .
 - $a^{p-1} \equiv 1 \pmod{p}$
 - $a^p \equiv a \pmod{p}$
 - Multiplicative Inverses
 - $a^{-1} \pmod{p} = a^{p-2} \pmod{p}$
 - Euler's Theorem
 - If a and n are co-prime (relatively prime)
 - First Version
 - $a^{f(n)} \equiv 1 \pmod{n}$
 - Second Version
 - $a^{k \times f(n) + 1} \equiv a \pmod{n}$
 - Multiplicative Inverses
 - Euler's theorem can be used to find multiplicative inverses modulo a composite
 - $a^{-1} \pmod{n} = a^{f(n)-1} \pmod{n}$
 - Generating Primes
 - Mersenne Primes:
 - A number in the form $M_p = 2^p - 1$ is called a Mersenne number and may or may not be a prime.
 - Fermat Primes
 - Primality Testing
 - Finding an algorithm to correctly and efficiently test a very large integer and output a prime or a composite has always been a challenge in number theory.
 - Divisibility Algorithm
 - The bit-operation complexity of the divisibility test is exponential.
 - Fermat Test
 - If n is a prime, $a^{n-1} \equiv 1 \pmod{n}$
 - If n is a composite, it is possible that $a^{n-1} \equiv 1 \pmod{n}$
 - Square Root Test
 - Factorization
 - Greatest Common Divisor
 - Least Common Multiplier
 - Trial Division Method

- Fermat Method
- Chinese remainder theorem
 - The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable, but different moduli.
 - Solution To Chinese Remainder Theorem
 - Find $M = m_1 \times m_2 \times \dots \times m_k$. This is the common modulus.
 - Find $M_1 = M/m_1, M_2 = M/m_2, \dots, M_k = M/m_k$.
 - Find the multiplicative inverse of M_1, M_2, \dots, M_k using the corresponding moduli (m_1, m_2, \dots, m_k) . Call the inverses $M_1^{-1}, M_2^{-1}, \dots, M_k^{-1}$.
 - The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \dots + a_k \times M_k \times M_k^{-1}) \bmod M$$

- Exponentiation and Logarithm
- Fast Exponentiation
- Logarithm
 - Order of the Group
 - Order of an Element
 - Primitive Roots In the group $G = \langle Z_n^*, \times \rangle$, when the order of an element is the same as $f(n)$, that element is called the primitive root of the group.
 - The group $G = \langle Z_n^*, \times \rangle$ has primitive roots only if n is 2, 4, p^t , or $2p^t$.
 - If the group $G = \langle Z_n^*, \times \rangle$ has any primitive root, the number of primitive roots is $f(f(n))$.
 - Cyclic Group If g is a primitive root in the group, we can generate the set Z_n^* as $Z_n^* = \{g^1, g^2, g^3, \dots, g^{f(n)}\}$
 - The idea of Discrete Logarithm
 - Properties of $G = \langle Z_p^*, \times \rangle$:
 1. Its elements include all integers from 1 to $p - 1$.
 2. It always has primitive roots.
 3. It is cyclic. The elements can be created using g^x where x is an integer from 1 to $f(p) = p - 1$.
 4. The primitive roots can be thought as the base of logarithm.
 - The discrete logarithm problem has the same complexity as the factorization problem.

Chapter 10: Asymmetric-Key Cryptography

- Symmetric-key cryptography is based on sharing secrecy;
- Asymmetric-key cryptography is based on personal secrecy.
- Asymmetric key cryptography uses two separate keys: one private and one public.

- Plaintext/Ciphertext
 - Unlike in symmetric-key cryptography, plaintext and ciphertext are treated as integers in asymmetric-key cryptography.
- Encryption/Decryption
 - $C = f(K_{public}, P)$, $P = g(K_{private}, C)$
- Trapdoor One-Way Function
 - The main idea behind asymmetric-key cryptography is the concept of the trapdoor one-way function.
 - One-Way Function (OWF)
 - f is easy to compute.
 - f^{-1} is difficult to compute.
 - Trapdoor One-Way Function (TOWF)
 - f is an One-Way Function
 - Given y and a trapdoor, x can be computed easily.
- Knapsack Cryptosystem
 - Definition
 - $a = [a_1, a_2, \dots, a_k]$ and $x = [x_1, x_2, \dots, x_k]$.
 - Given a and x , it is easy to calculate the knapsack sum s .
 - However, given s and a it is difficult to find x .
 - Super-increasing Tuple
 - $a_i \geq a_1 + a_2 + \dots + a_{i-1}$
 - Secret Communication with Knapsacks
- RSA cryptosystem
 - Key Generation
 - Encryption
 - Decryption

Chapter 11: Message Integrity and Message Authentication

- Message and Message Digest
 - The message digest needs to be safe from change.
- Cryptographic Hash Function Criteria
 - A cryptographic hash function must satisfy three criteria:
 - preimage resistance,
 - Second preimage resistance, and
 - Collision resistance.
 - Random Oracle Mode
 - The hash function based on the random oracle model behaves as follows:
 1. When a new message of any length is given, then oracle creates and gives a fixed-length message digest that is a random string of 0's and 1's. The oracle records the message and the message digest.
 2. When a message is given for which a digest exists, the oracle simply gives the digest in the record.

3. The digest for a new message needs to be chosen independently from all previous digests. This implies that the oracle cannot use a formula or an algorithm to calculate the digest.
 - Pigeonhole Principle
 - If n pigeonholes are occupied by $n + 1$ pigeons, then at least one pigeonhole is occupied by two pigeons.
 - The generalized version of the pigeonhole principle is that if n pigeonholes are occupied by $kn + 1$ pigeons, then at least one pigeonhole is occupied by $k + 1$ pigeons.
 - Four Versions of the Birthday Problems
 - Their descriptions, solutions, and comparison.
 - Attacks on Random Oracle Model
 - Preimage Attack
 - Second Preimage Attack
 - Collision Attack
 - Alternate Collision Attack
 - Message Authentication
 - Modification Detection Code (MDC)
 - Message Authentication Code (MAC)
 - The security of a MAC depends on the security of the underlying hash algorithm.

Chapter 12 is ignored and will not be covered in the exam.

Chapter 13: Digital Signature

- A digital signature needs a public-key system. The signer signs with her private key; the verifier verifies with the signer's public key.
- A cryptosystem uses the private and public keys of the receiver: a digital signature uses the private and public keys of the sender.
- A digital signature provides message authentication.
- Nonrepudiation: Nonrepudiation can be provided using a trusted party.
- Confidentiality: A digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied.

Chapter 14 is ignored and will not be covered in the exam.

Chapter 15: Key Management

- Key-Distribution Center: KDC
 - Flat Multiple KDCs.
 - Hierarchical Multiple KDCs
- Session Keys

- A KDC creates a secret key for each member. This secret key can be used only between the member and the KDC, not between two members.
- A session symmetric key between two parties is used only once.
- Kerberos
 - Kerberos is an authentication protocol, and at the same time a KDC.
 - Authentication Server (AS)
 - The authentication server is the KDC in the Kerberos protocol.
 - Ticket-Granting Server (TGS)
 - The ticket-granting server (TGS) issues a ticket for the real server.
 - Real Server
 - The real server provides services for the user.

Chapter 16: *Security at the Application Layer: PGP and S/MIME*

- Pretty Good Privacy (PGP) can be used to create a secure e-mail message or to store a file securely for future retrieval.
 - Confidentiality with One-Time Session Key.

Chapter 17 is ignored and will not be covered in the exam.

Chapter 18 is ignored and will not be covered in the exam.