CIS 6930/4930 Computer and Network Security

Midterm review

About the Test

- This is an open book and open note exam.
  - You are allowed to read your textbook and notes during the exam;
  - However, you are not allowed to exchange anything with or talk to each other unless you get permission from the instructor.
  - You may bring your laptop to the exam **but you are not allowed to access to internet during the exam.**

Covered Topics

- Lectures 1 - 9
    - Basic Security Concepts
    - Introduction to Cryptography
    - DES
    - Modes of Block Cipher Operations
    - Double DES and Triple DES
    - Number Theory
    - Public Key Cryptography

Type of Questions

- Multiple choices (25%)
- Simple calculation (25%)
- Open-ended questions (50%)

Introduction to Cryptography

- Basic Security Concepts
  - Confidentiality, integrity, availability
- Introduction to Cryptography
  - Secret key cryptography
    - Sender and receiver share the same key
    - Applications
      - Communication over insecure channel, Secure storage, Authentication, Integrity check

Introduction to Cryptography

- Introduction to Cryptography
  - Public key cryptography
    - Public key: publicly known
    - Private key: kept secret by owner
    - Encryption/decryption mode
      - How the keys are used?
    - Digital signature mode
      - How the keys are used?
    - Application: Secure communication, secure storage, authentication, digital signature, key exchange

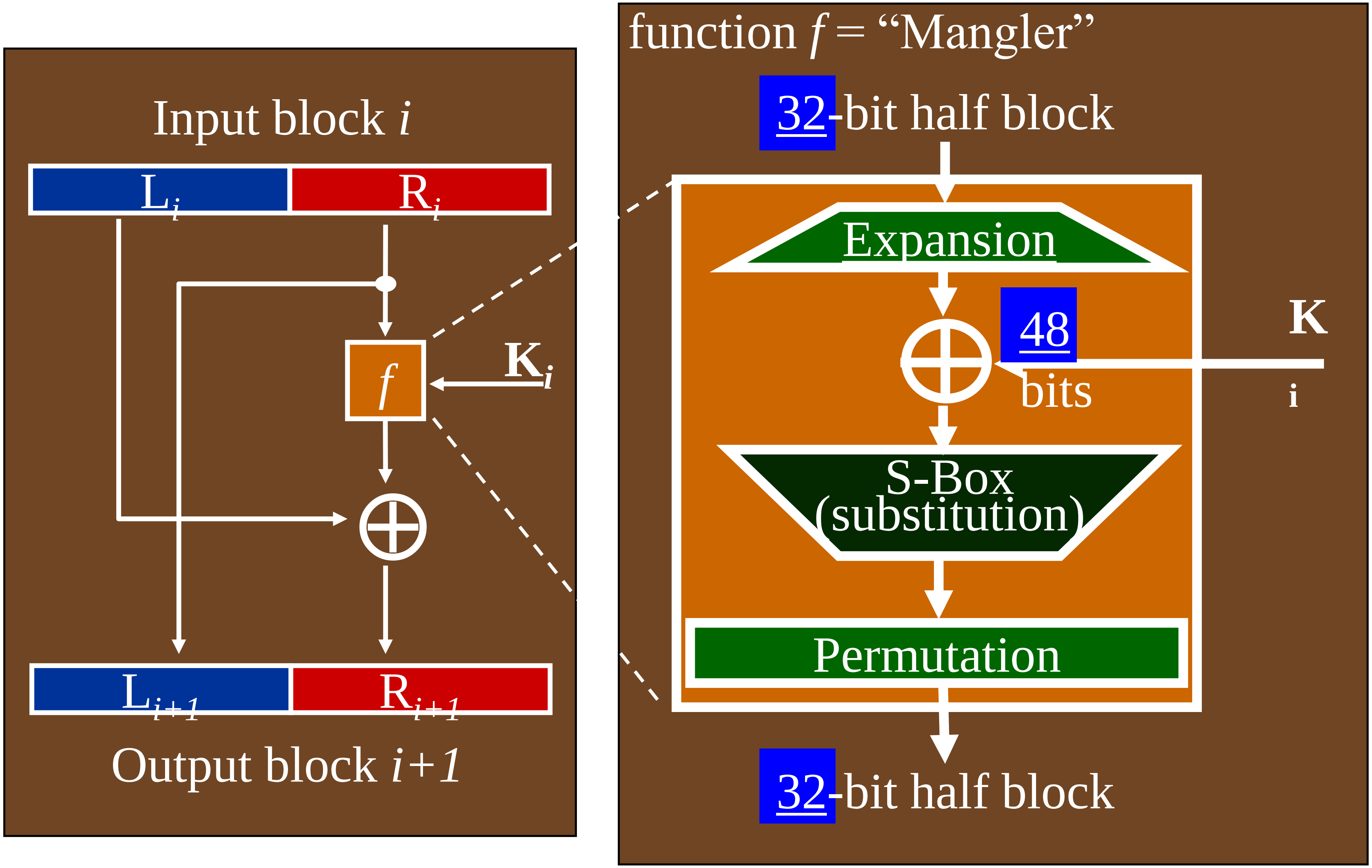
Introduction to Cryptography

- Introduction to Cryptography
  - Hash function
    - Map a message of arbitrary length to a fixed-length short message
  - Desirable properties
    - Performance, one-way, weak collision free, strong collision free

DES

- DES
  - Parameters
    - Block size (input/output 64 bits)
    - key size (56 bits)
    - number of rounds (16 rounds)
    - subkey generalization algorithm
    - round function

DES Round: *f* (Mangler) Function



Modes of Block Cipher Operations

- ECB (Electronic Code Book)
- CBC (Cipher Block Chaining Mode)
- OFB (Output Feedback Mode)
- CFB (Cipher Feedback Mode)

Modes of Block Cipher Operations

- Properties of Each Mode
  - Chaining dependencies
  - Error propagation
  - Error recovery

Double DES and Triple DES

- You need to understand how double and triple DES works
  - Double DES C=Ek2(Ek1(P))
  - Triple DES C = Ek1(Dk2(Ek1(P))
  - Meet-in-the-middle attacks
  - Operation modes using Triple DES

Number Theory Summary

- Fermat: If p is prime and a is positive integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Example: 11 is prime, 3 not divisible by 11, so $3^{11-1} = 59049 \equiv 1 \pmod{11}$

Euler: For every a and n that are relatively prime, then $a^{\phi(n)} \equiv 1 \bmod n$

Example: For a = 3, n = 10, which relatively prime: $\phi(10) = 4$, $3^{\phi(10)} = 3^4 = 81 \equiv 1 \bmod 10$

Variant: for all a in $\mathcal{Z}_n^*$, and all non-negative k, $a^{k\phi(n)+1} \equiv a \bmod n$

Example: for n = 20, a = 7, $\phi(n) = 8$, and k = 3: $7^{3*8+1} \equiv 7 \bmod 20$

Generalized Euler's Theorem: for $n = pq$ (p and q are distinct primes), all a in $\mathcal{Z}_n$, and all non-negative k, $a^{k\phi(n)+1} \equiv a \bmod n$

Example: for n = 15, a = 6, $\phi(n) = 8$, and k = 3: $6^{3*8+1} \equiv 6 \bmod 15$

$x^y \bmod n = x^{y \bmod \phi(n)} \bmod n$ (foundation for RSA public key cryptographic)

Example: x = 5, y = 7, n = 6, $\phi(6) = 2$, $5^7 \bmod 6 = 5^{7 \bmod 2} \bmod 6 = 5 \bmod 6$

Multiplicative Inverses

- Don't always exist!
  - Ex.: there is no *z* such that $6 \times z = 1 \bmod 8$ (m =6 and n=8)

z	0	1	2	3	4	5	6	7
6×z	0	6	12	18	24	30	36	42
6×z mod 8	0	6	4	2	0	6	4	2

…

- An positive integer $m \in Z_n$ has a multiplicative inverse m^{-1} **mod** n **iff** $\gcd(m, n) = 1$, i.e., *m* and *n* are **relatively prime**

  $\Rightarrow$ If *n* is a prime number, then all positive elements in Z_n have multiplicative inverses

Finding the Multiplicative Inverse

- Given m and n, how do you find m^{-1} mod n?

– Extended Euclid's Algorithm
`exteuclid(m,n)`:
$m^{-1} \bmod n = \mathbf{v_{n-1}}$
  – if $\gcd(m,n) \neq 1$ there is no multiplicative inverse m^{-1} mod n

Example

x	q_x	r_x	u_x	v_x
0	-	35	1	0
1	-	12	0	1
2	2	11	1	-2
3	1	1	-1	$\boxed{3}$
4	11	0	12	-35

gcd(35,12) = 1 = -1*35 + 3*12

12^{-1} mod 35 = **3** (i.e., 12*3 mod 35 = 1)

Discrete Logarithms

- For a primitive root *a* of a number *p,* where a^i mod $p = b$, for some $0 \leq i \leq p$-1
  - the exponent *i* is referred to as the *discrete logarithm of b to the base a, mod p*
  - Given *a*, *i*, and *p*, computing b = a^i mod *p* is straightforward
  - Given *a*, *p*, and *b*, computing the discrete logarithm *i* is hard. The common method is the brute force method.

i	1	2	3	4	5	6	7	8	9
3^i *mod 7*	3	2	6	4	5	1	3	2	6

Public Key Cryptography

- RSA Algorithm
  - Basis: factorization of large numbers is hard
  - Variable key length (1024 bits or greater)
  - Variable plaintext block size
    - plaintext block size must be smaller than key size
    - ciphertext block size is same as key size

Generating a Public/Private Key Pair

- Find large primes p and q
- Let $n = p*q$
  - do not disclose p and q!
  - $\phi(n) = (p-1)*(q-1)$
- Choose an e that is relatively prime to $\phi(n)$
  - **public** key = $<e,n>$
- Find d = multiplicative inverse of e mod $\phi(n)$ (i.e., $e*d = 1 \bmod \phi(n)$)
  - **private** key = $<d,n>$

RSA Operations

- For plaintext message ***m*** and ciphertext ***c***

Encryption: $\boldsymbol{c = m^{e} \bmod n}$, $m < n$

Decryption: $\boldsymbol{m = c^{d} \bmod n}$

Signing: $\boldsymbol{s = m^{d} \bmod n}$, $m < n$

Verification: $\boldsymbol{m = s^{e} \bmod n}$