Final Exam Review

CS 458: Information Security
Kevin Jin

Final Exam

- Date/Time
  - Dec 2nd , Wednesday, 2:00-3:15 pm
- Content
  - All lecture/lab materials
- Type of Questions
  - Multiple choice questions
  - Multiple answer questions
  - Short answer/working problems
- Exam platform
  - Blackboard with a randomized question order
- Past year sample exam
  - https://www.dropbox.com/s/90w5t9yobt6xtqk/Final_exam_example.pdf?dl=0

On the exam day

- Before the class
  - Join blackboard, open “CS458 Final Exam” in the Assignment
  - You can also join the classroom session, TA and I will be there
- During the class: TA and I are available to answer questions via
  - Live chat on blackboard session
  - Email Kevin dong.jin@iit.edu and/or
    TA Xiaoliang at xwu64@hawk.iit.edu
- Click “submit” button to submit your exam
  - Before submission, you can navigate questions and change answers as much as you want
  - Only submit once
  - Exam ends at 3:15 pm, no late submission

Comprehensive – Topics

- Introductory Definitions
- Historical Cryptography
- Symmetric Cryptography
- Public or Asymmetric Cryptography
- Crypto Hash
- Identity and Key management
- Authentication
- SSL/IPSec
- Access Control
- RBAC
- Mandatory Access Controls
- Malicious Code
- Database Security
- Buffer Overflow
- Network Security
- Intrusion Detection
- Firewalls
- Software Reverse Engineering

Historical Ciphers

- Transposition
  - N-columnar transposition
- Substitution
  - Caesar, Vigenere, one-time pad
- General crypto analysis assumptions
  - Ciphertext only, known plaintext, chosen plaintext
- No Attacks/Statistical Cryptanalysis

Sample Exam Q

You are given a section of cipher text. You know nothing about the encrypting algorithm. You compute the character frequencies in the message. The character frequencies are close to the standard character frequencies you would expect to see in a segment of English text. Based on this information, you believe that the type of encryption algorithm is:

a. Polyalphabetic b. Substitution

c. Transposition d. Product

Sample Exam Q

You are given a section of cipher text. You know nothing about the encrypting algorithm. You compute the character frequencies in the message. The character frequencies are close to the standard character frequencies you would expect to see in a segment of English text. Based on this information, you believe that the type of encryption algorithm is:

a. Polyalphabetic

b. Substitution

c. **Transposition**

d. Product

Symmetric Encryption

- Block vs stream ciphers
- DES
  - 56 bit key and 64 bit block
- AES
  - Multiple key sizes: 128, 192, 256
  - Block size: 128

Sample Exam Q

What is the block size for AES-192 encryption algorithm?

a. 64
b. 128
c. 192
d. 256

Sample Exam Q

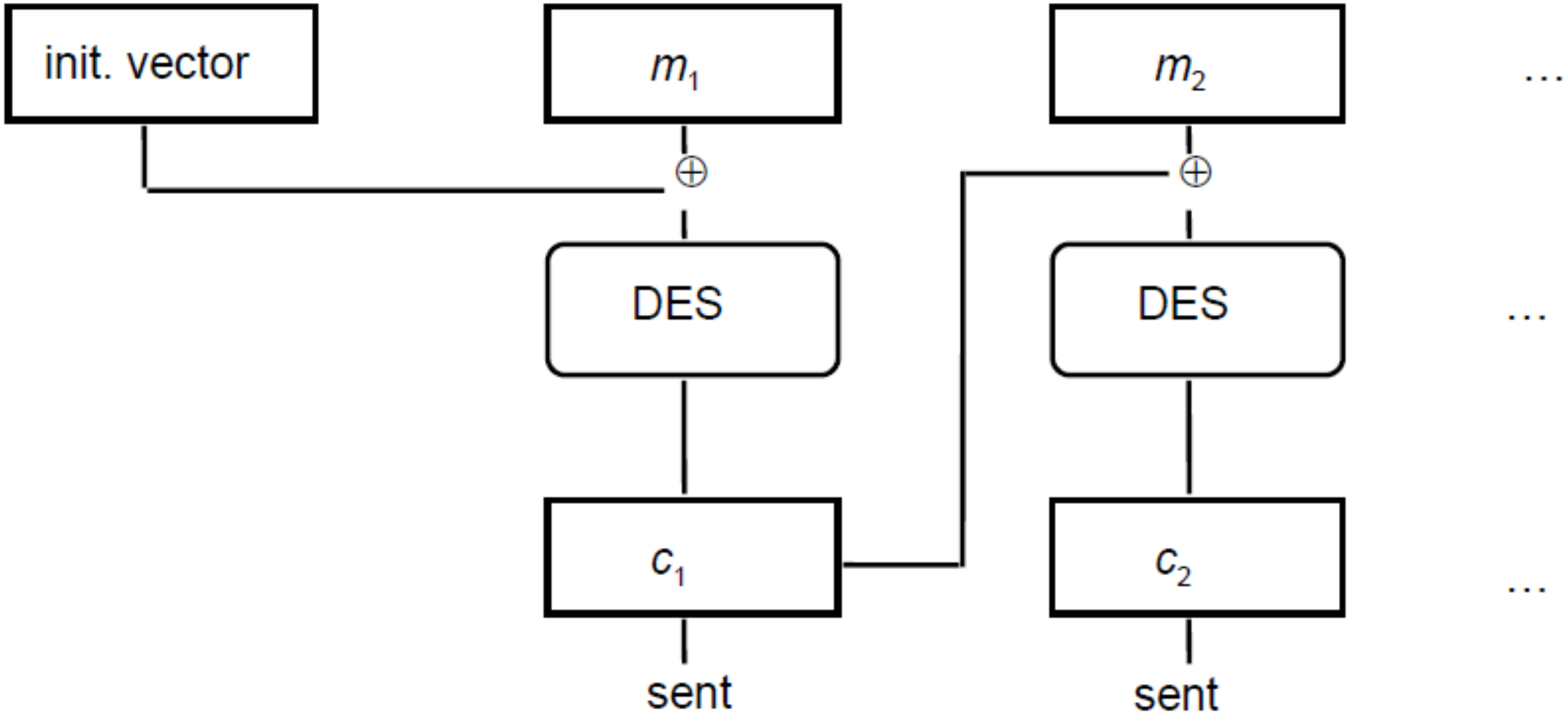
What is the block size for AES-192 encryption algorithm?

a. 64
b. **128**
c. 192
d. 256

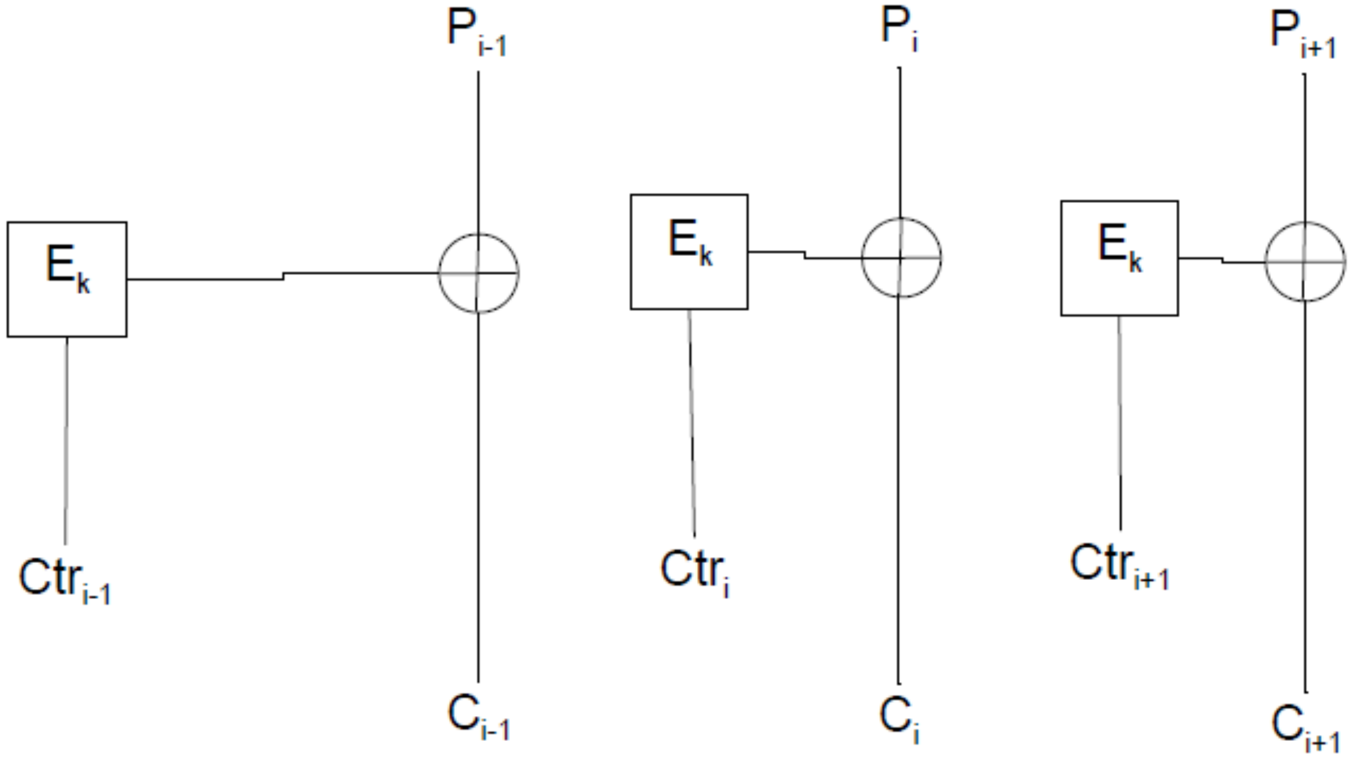
Block Encryption Modes

- Chapter 20 (Section 5) of the text
  - 7.2.2 of the Handbook of Applied Cryptography
  - http://www.cacr.math.uwaterloo.ca/hac/about/chap7.pdf
- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Counter Mode

What Mode?



What Mode?



Multiple Encryptions

- Double Encryption does not gain much
  - Meet-in-the-middle
    - Both decrypt and encrypt with test key
    - Save both and check against the other for middle values as you check new keys

Public/Asymmetric Encryption

- Two keys
  - One key public, eases some bootstrap issues
- Based on “hard problems”
  - RSA – factoring composites of large primes
  - Diffie Hellman – computing discrete logarithms
- Know equations for RSA and DH
  - What values are public and what are private

Public Encryption

- Assume an RSA scenario with Alice and Bob
  - Alice public values = e_A and n_A. Private value d_A
  - Bob public values = e_B and n_B. Private value d_B
- What does it mean for Alice to sign m?
- What does it mean for Bob to send m to Alice privately?
- What key is used for what purpose/property?

Sample Exam Q

If Alice wants to send a private message to Bob using asymmetric-key crypto what should she do?

a. Encipher it with her private key

b. Encipher it with Bob’s private key

c. Encipher it with her public key

d. Encipher it with Bob’s public key

Sample Exam Q

If Alice wants to send a private message to Bob using asymmetric-key crypto what should she do?

a. Encipher it with her private key

b. Encipher it with Bob’s private key

c. Encipher it with her public key

d. Encipher it with Bob’s public key

Public Encryption

- In text and slides we provided computation examples with very small values.
  - Not strong for small values. Hard problems do not hold.

7^5 mod 11 =?

= (7 mod 11) x (7^2 mod 11) x (7^2 mod 11) mod 11

= 7 x 5 x 5 mod 11 = 175 mod 11 = 10

Cryptographic hashes

- Difference from regular checksums
- Keyed (MAC) and keyless
  - When is each appropriate
- Brute force attack
  - Find another message with the same hash value
- Birthday attack and Pigeonhole Principle
- Standard algorithms
  - SHA, MD5, block ciphers in CBC mode
- HMAC to make keyless hash keyed

Sample Exam Q

Which hash algorithm would be most appropriate for generating hash of a software package posted on the main corporate web site? In this scenario, customers may be downloading the software package from mirror sites or other locations not directly under the corporation's control.

a. MD5
b. HMAC-MD5
c. CRC
d. RSA

Sample Exam Q

Which hash algorithm would be most appropriate for generating hash of a software package posted on the main corporate web site? In this scenario, customers may be downloading the software package from mirror sites or other locations not directly under the corporation's control.

a. MD5
b. **HMAC-MD5**
c. CRC
d. RSA

Crypto Strengths

- Brute-force Key Search (symmetric algorithms)
  - Attack strength is O(size of key space)
  - e.g., strength of AES-192 is O(2^{192})
  - Some special cases, e.g. double encryption and meet in the middle
- Attack hard problem (asymmetric algorithms)
  - Know the hard problems underlying RSA and DH
  - Know how an easy solution to the hard algorithm breaks the cipher

Sample Exam Q

The numbers of steps in a brute force attack on a system that is using DES with two keys to double encrypt the plaintext is:

a. 2^{56}

b. 2^{57}

c. 2^{112}

d. 2^{128}

Sample Exam Q

The numbers of steps in a brute force attack on a system that is using DES with two keys to double encrypt the plaintext is:

a. 2^{56}

b. $\mathbf{2^{57}}$

c. 2^{112}

d. 2^{128}

Crypto Strengths

- Crypto Hash
  - Weak-Collision Resistance
    - Attacker wants to find malicious message that has same hash as original message
    - Attack steps needed ~ O(2^n); n bit hash; assuming algorithm hasn’t been “broken”
    - Example – SHA-256 has 256 output bits so attack steps needed are ~ O(2^{256})
  - Strong-Collision Resistance
    - Attacker wants to find two messages that have the same hash
    - Attack steps needed ~ O($2^{n/2}$); n bit hash; birthday attack

Key Management

- Digital signatures
- Long lived vs. session keys
- Randomness and pseudo random
- Key/identity distribution
  - Trusted third party, public key
  - Needham-Schroeder
  - Kerberos at a high level
  - Certificate frameworks
    - Hierarchical and web of trust

Sample Exam Q

The introduction of a nonce into a key exchange algorithm thwarts which attack?

a. Replay attack
b. Key cracking
c. The man-in-the-middle attack
d. The meet-in-the-middle attack

Sample Exam Q

The introduction of a nonce into a key exchange algorithm thwarts which attack?

a. Replay attack
b. Key cracking
c. The man-in-the-middle attack

d. The meet-in-the-middle attack

User Authentication

- Establish ID
  - What you know
  - What you have
  - What you are
    - Static and dynamic
- Spent a lot of time on passwords
  - Online vs. offline attacks
  - Salt
- Challenge Response
- Biometrics

SSL/IPSec (22.3 – 22.5)

- SSL vs. IPSec
  - Network layer, Transparency
- Handshake protocol
  - Use of Diffie-Hellman/RSA
  - Certificates for authentication
- Handshake properties
- IPSec
  - Modes – Tunnel vs. Transport
  - AH vs. ESP

Access control

- AAA
  - Authentication, Authorization, Audit
- DAC/MAC/RBAC
- Access Matrix
  - Model to capture protection state
  - Rules for change
- Access Control Lists
  - Access Matrix by column
- Capabilities
  - Access Matrix by row

Role Based Access Control (RBAC)

- Add intermediate role layer
  - Map users to roles
  - Map roles to permissions
  - Users take on one or more roles during sessions
- Different models
  - RBAC0 = base model
  - RBAC1 = RBAC0 + hierarchy
- RBAC2 = RBAC0 + constraints
- RBAC3 = everything in RBAC1 and RBAC2
- NIST Standard
  - Core
  - Hierarchical - limited
  - Constraints – SSD, DSD

Mandatory Access Controls

- Bell-LaPadula Confidentiality Model
  - security levels
  - security labels (level + category)
  - simple security property
    - No-read-up
  - *-property
    - No-write-down

- Biba Integrity Model
  - simple security
    - No-read-down
  - *-property
    - No-write-up
- Chinese Wall Model
  - Conflict-of-interest
  - security properties

Database Security

- Access control model
  - No single owner of all data/privilege
  - Revocation model
- Statistical databases
  - Attacker attempts to infer information from multiple queries
  - Deny results over too small set
  - Perturb inputs, queries, outputs
- SQL injection attack

Malicious Code

- Types of malicious code
  - Trojan programs
  - Rootkits
    - types and defenses
  - Virus
    - Detection and virus evasion
  - Worms
    - Propagation techniques
  - Botnets
- Propagation techniques vs. hiding techniques
- Defenses

Buffer Overflow

- Stack Overflow
  - Stack smashing
- Shell Code
  - NOP sled
- Defenses
  - Compile Time
  - Run-time

- Compile Time
  - Language
  - Safe Coding
  - Safe libraries
  - Stack protection
- Run-time
  - No-execute
  - Address space randomization

Network Security

- Denial of Service attacks
  - Resource exhaustion/Flooding
- Address spoofing
- ARP cache poisoning
- Smurf – an amplification/reflection attack
- Open Relay DNS – DoS amplification attack
- DNS Cache Poisoning
- TCP-based Attacks
  - SYN Spoofing, Reset, Session Hijacking
- Defenses against Distributed Denial of Service

Intrusion detection system

- Intruders
- IDS
  - Principles and Requirements
  - False Negatives and Positives
  - How IDS actively respond to an attack
- IDS Types
  - Host-based vs. Network-based
  - Anomaly vs. Signatures based

Firewalls

- Different types of firewalls
  - Packet filtering, rules
  - Stateful Inspection
  - Application Proxy
- Deployment Level
  - Network
  - Host
  - Personal

Software Reverse Engineering

- Tools: Disassembler, Debugger, Hex Editor…
- SRE Attack Mitigation
  - Anti-disassembly techniques
  - Anti-debugging techniques
  - Tamper-resistance
  - Code obfuscation

CS458 Information Security