Exam 1 review

Bo Luo
bluo@ku.edu

Bo Luo

Exam 1

- Time: Thursday March 21 4:00 – 5:15pm

- Closed book, closed notes
- No electronic devices!
- You can bring a calculator.

- One-page cheat sheet allowed. Letter size, double sided.

- 30% of the final grade

Bo Luo

Exam 1

- Format
  - Multiple choice
  - T/F **with justification**
  - Short answers: Encryption/decryption, security analysis, etc.

False reason —> may be too many F

- Coverage
  - Introduction (approximately 5%) 2
  - Cryptography (approximately 55%) 63
  - Authentication (approximately 25%) 17
  - Database security (approximately 15%) 12

Introduction

- Concepts, principles, etc.
  - Principle of Easiest Penetration
    - Identify easiest penetration in real world scenarios
  - Threats, vulnerabilities, controls
  - Kinds of threats: interception, interruption, modification, fabrication
  - MOM: method, opportunity, motive
  - Meaning of computer security: CIA – confidentiality, integrity, availability
  - Hardware, software, and data
  - Defense: prevent, deter, deflect, detect, recover
  - Principle of Effectiveness, Principle of Weakest link

Cryptography

没考

- Terminology and concepts:
  - S: sender (Alice); R: recipient (Bob); O: outsider or intruder
    - Chuck; Eve: eavesdropper; Mallory: malicious attacker
    - O might try to: block intercept modify fabricate
  - Cryptographic algorithm take a key and convert plaintext to ciphertext and back
  - Key, plaintext, and ciphertext
  - Cryptosystem cryptosystem algorithm set of all possible keys,plaintext,and ciphertext
  - Mathematic representation of cryptosystems

Cryptography

- Cryptology: Cryptography + Cryptanalysis
  - Good cryptosystems
  - Kerckhoffs's principle

we use key, key generated != random

- Unconditional secure vs. computational secure
- Brute-Force Attack: how many keys (on average)?

尝试每一种可能性去破译，强行破解

考了一道计算

Average time to break DES
try all possible keys

- Secret key cryptography
- Public key cryptography two keys: secret and public keys
- Cryptographic hash functions

Cryptography

- Cryptosystems
  - Substitution ciphers
  - Shift cipher (Caesar cipher): encryption, decryption, formal definition
  - Monoalphabetic ciphers
  - Polyalphabetic ciphers: Vigenere Cipher
  - Homophonic Ciphers
  - Polygram Ciphers: Playfair
  - Attacks

monoalphabetic 单线破解

Caesar cipher ==》 shift 3

考了Vigenere Cipher

26*26对应表

一个plaintext 对应多个 ciphertext
disadvantage：Inefficient

加密：两个字母在同一行向右看，同一列向下，不同列和行 看对角线

Monoalphabetic ciphers and Homophonic ciphers
– Substitute one character for another character
• Polygram ciphers
– substitute a group of characters for another group of characters
– Goal: make it difficult for frequency analysis

Substitutionciphers
– Monoalphabetic cipher – Polyalphabetic ciphers – Homophonic ciphers
– Polygram ciphers
– “classical ciphers”

Still vulnerable to various attacks
– Brute force attack —>when key space is small – How to generate a large keyspace?

Cryptography

- Cryptosystems
  - One-time pad
  - Rotor machines
  - Transposition Ciphers
  - Combinations of approaches
  - Shannon Secrecy: the probability model
  - Confusion vs. diffusion
  - Substitution-permutation (S-P) networks
  - Stream ciphers vs. block ciphers

very long key； XOR bit-wise 使用bit来加密和解密

rearrage the plaintext to get ciphertext
横着写，竖着读，反之亦然
period：一行或一竖行写几个

考了Confusion and diffusion

AES and DES

P (M = m I E(K, m) = c) = P (M = m)
•
Probabilityofguessingtheplaint extknowingthe ciphertext = probability of guessing plaintext without knowing ciphertext.
P (E(K, m) = c) = P (E(K, m') = c)
• Probability of any message giving a ciphertext is the same

Confusion: make the relationship between the plaintext and the ciphertext (or the ciphertext and the key) as complex as possible.
• Use the key in a very complex way.
– Diffusion: dissipate the statistical structure of the plaintext in the long range statistics of the ciphertext.
• Have many plaintext characters (bits) affect each ciphertext character (bit)

Streamciphers
– Advantages: fast; low error propagation
– Disadvantages: low diffusion; vulnerable to insertions and modifications
• Block ciphers
– Advantages: high diffusion; more immunity to insertion
– Disadvantages: slower; error propagation

Cryptography

考了一大题

- Modern Cryptosystems
  - DES
    - Block size, key length
    - The algorithm: initial permutation, 16 rounds of encryption, final permutation. Operations in each round. Key schedule.
    - Strength of DES
    - Not in the exam: modes of operation

Cryptography

考了short answer

- Modern Cryptosystems
  - AES
    - Block size, key length, state array, etc.
    - In each round: SubBytes, ShiftRows, MixColumns, AddRoundKey
  - Diffie-Hellman key agreement 考了5分
    - Key agreement: motivation
    - The protocol
    - Man-in-the-middle attack
    - ~~ACM Turing Award!!~~

Cryptography

- Modern Cryptosystems
  - RSA 考了4分
    - Public key cryptography: encryption vs. digital signatures
    - RSA: Key generation, encryption, decryption
    - Why RSA is secure?
    - Public key + session key. Why? speed
    - Not in the exam: attacks on RSA
  - MAC
    - MAC, Cryptographic hash, Hash for authentication
    - Not in the exam: collision resistance

Authentication

- Basic concepts
  - Why authenticate? How?
- Public-Key Infrastructure (PKI)
  - Certificate
  - CA hierarchy
- Password authentication
  - Use of strong password, why?
  - Password storage, attacks, rainbow table, salt

Authentication

- Distributed authentication
  - Basic concepts
- Kerberos
  - Scenario, design goals
  - Architecture
  - The protocol, ticket, session key, authenticator
  - Short-term credentials
  - Kerberos Single Sign-On (SSO)
- Real world use cases of Kerberos

Why do we kerberos expensive?

DB Security

- Basic concepts: CIA
- Access control
  - Policy vs. enforcement mechanism
  - Access control models: MAC, DAC, RBAC
  - MLS schema, special handling of insert and update
  - DAC: subjects and privileges, GRANT/REVOKE
  - RBAC

DB Security

- Database encryption
  - Application level encryption vs. database encryption
- Inference attacks
  - Tracker attack
  - Possible controls