Cryptanalysis
(암호분석)

Course Introduction

2022.3

강의 개요

- 과목명: 암호분석(Cryptanalysis)
  - 학수번호: 1395800
  - 학점/시간: 3/3

- 수업시간/강의실
  - 수요일 1,2,3교시 (9:00~11:50)
  - 강의실: 과학관 310호
  - 수업방법: 대면/비대면 혼합(1주차 온라인 실시간으로 수업방식 논의)

- 수강 대상
  - 정보보안암호수학과 3,4학년

수업 개요

- 수업 개요
  - 현대 암호의 안전성 개념을 이해하고 대칭키 암호의 분석 이론을 체계적으로 학습한다.
  - 분석 프로그램의 구현을 통해 공격의 개념을 명확히 하며 실질적인 공격 시나리오를 파악한다.

  - 암호의 안전성을 정량적으로 정의하기 위해, 수학 및 확률론을 기반으로 다양한 공격자 모델에 대한 안전성 개념을 다룬다.
  - 블록암호의 주요 분석법인 차분분석(DC)과 선형분석(LC)을 이해하고, 이를 확장한 분석기술에 대하여 살펴본다.

수업 목표/주제

- 수업 목표
  - 암호 알고리즘의 공격과 안전성 분석에 사용되는 주요 이론을 이해하고 공격 알고리즘의 구현 능력을 확보한다.

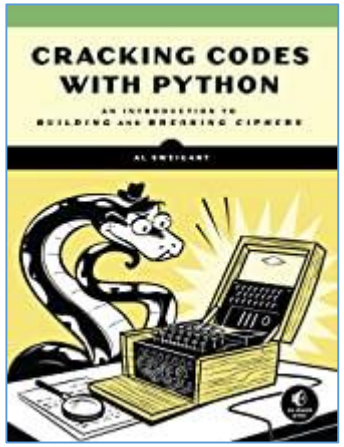
- 수업 주제(주요 분석기법)
  - Brute-Force Attack (Exhaustive key search)
  - Generic attack - TMTO(Time Memory Trade Off) and Slide attack
  - DC(Differential Cryptanalysis)
  - LC(Linear Cryptanalysis)
  - Integral attack, Higher-Order DC
  - Impossible Differential attack

선수 학습

- 선수 과목
  - 수리전산(Python)
  - 대칭키 암호

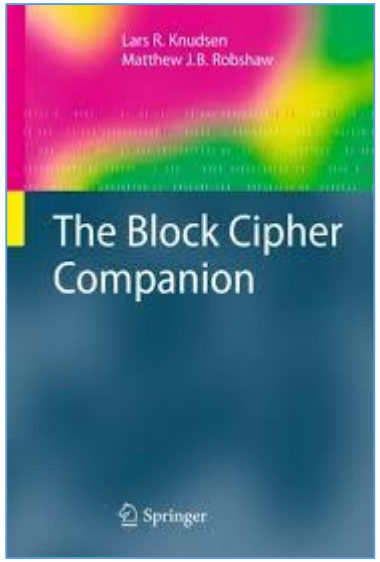
- 프로그래밍 능력
  - 수학적 알고리즘을 구현할 수 있는 수준 이상
  - 언어: C, C++, 또는 Python 중 적어도 하나 이상

교재

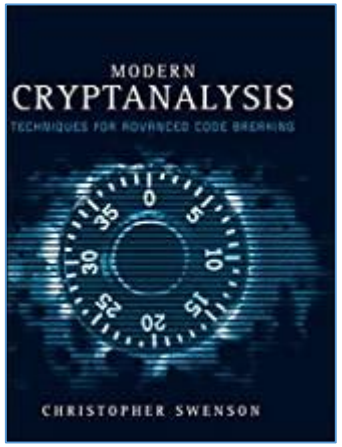


- Cracking codes with Python: An Introduction to Building and Breaking Ciphers
  - Author: Al Sweigart
  - Publisher(Year): No Starch Press (2018)
  - ISBN: 978-1593278229

- The Block Cipher Companion
  - Author: L. Knudsen, M. Robshaw
  - Publisher(Year): Springer (2011)
  - ISBN: 978-3642173417

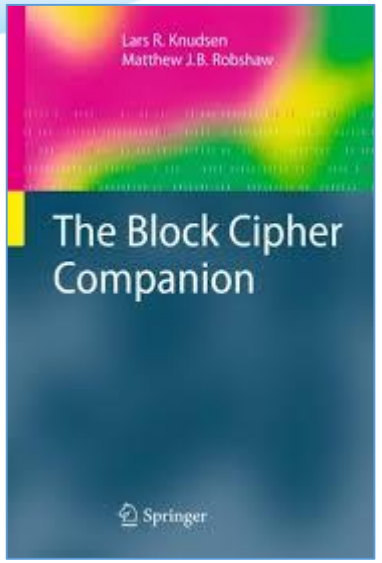


참고도서



- Modern Cryptanalysis: Techniques for Advanced Code Breaking
  - Author: Christopher Swenson
  - Publisher(Year): Wiley (2008)
  - ISBN:978-0470135938

주 교재 목차



1. Introduction
2. DES
3. AES
4. Using Block Ciphers (Modes of Operation)
5. **Brute Force Attacks**
6. **Differential Cryptanalysis**
7. **Linear Cryptanalysis**
8. **Advanced Topics**

담당교수/면담시간

- 담당 교수: 염용진
  - 연구실: 휘랑관 (생활관D동/E4) 710호
  - 이메일: salt@kookmin.ac.kr
  - 전화: 02-910-5749
  - 연구팀: 난수성 분석 및 안전성 평가 연구실 (http://randanalysis.kookmin.ac.kr/wordpress/)

염용진
(Yeom, Yongjin)

- 면담방법
  - 면담시간(Office Hour): 월요일 9:00~12:00
  - 면담방법: 이메일을 통한 사전 예약 (시간변경 가능)

과제

- 과제
  - 공격 알고리즘의 구현 및 결과 분석
  - 학습한 이론에 대한 이해도를 확인하기 위한 문제

- 주의/참고 사항
  - 제출 기한 엄수할 것 (추가 제출 불가)
  - 과제의 일부는 시험문제로 활용됨
  - 반드시 혼자의 노력으로 풀 것

시험

- 시험 일정
  - 중간고사 : 4월 20일 (수)
  - 기말고사 : 6월 8일 (수)

- 시험방법
  - 학교의 규정과 방침에 따름

강의 일정

일정	내용
1주	Course introduction
2주	암호분석의 역사/치환암호의 구현
3주	치환암호의 공격기법
4주	안전성 개념과 블록암호의 공격모델
5주	공격 실습을 위한 Toy Cipher 구현
6주	키 전수조사 공격법과 TMTO(Time Memory Trade Off)
7주	차분공격 기법(DC, Differential Cryptanalysis)
8주	중간고사

* 학습 진도에 따라 강의 일정과 순서는 일부 변경될 수 있음

강의 일정

일정	내용
9주	차분공격의 구현
10주	차분분석의 응용: TDC(Truncated DC), IDC(Impossible DC)
11주	Integral cryptanalysis and HO-DC(Higher Order DC)
12주	선형공격 기법(LC, Linear Cryptanalysis)
13주	Generic attack - Slide attack
14주	공격기법의 결합: 연관키(related key) 공격, Boomerang 공격
15주	기말고사
16주	Wrap up

* 학습 진도에 따라 강의 일정과 순서는 일부 변경될 수 있음

성적

- 반영 비율
  - 중간고사: 30%
  - 기말고사: 40%
  - 과제:20%
  - 출석 및 참여도: 10%

- 주의 사항
  - **절대평가로 학습목표 달성도에 따라 학점을 부여함**
  - 평균점수와 개인성적은 통보하나 등수를 공개하지 않음
  - 과제, 시험 결과에 대한 문의는 가능하나
    점수확정 후 학점의 상향/하향 조정은 절대 불가함