Cryptanalysis
(암호분석)

Course Introduction

2020.3

강의 개요

- 과목명: 암호분석(Cryptanalysis)
  - 학수번호: 139580-01
  - 학점/시간: 3/3
- 수업시간/강의실
  - 금요일 2,3,4교시 (10:00~12:50)
  - 강의실: 과학관 310호
- 수강 대상
  - 정보보안암호수학과 3,4학년

수업 개요

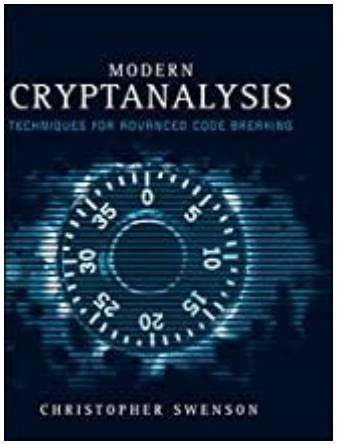
- 수업 개요
  - 현대 암호의 안전성 개념의 이해를 바탕으로 대칭키 암호의 분석 이론을 체계적으로 학습한다.
  - 분석 프로그램의 구현을 통해 이해를 명확히 하며 실질적인 공격 시나리오를 파악한다.
  - (HOT-TEAM Class) 양자 컴퓨팅 시대의 암호 공격기법과 이에 대비한 암호기술을 전망한다.

선수 학습

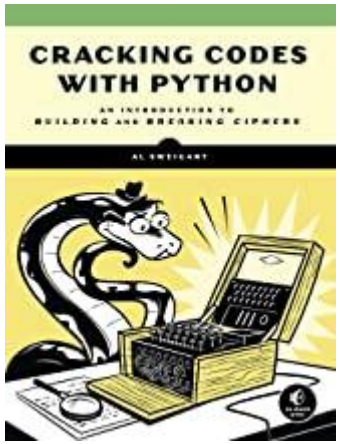
- 선수 과목
  - Calculus
  - 대칭키 암호

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

교재



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



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

담당교수/면담시간

염용진
(Yeom, Yongjin)

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

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

과제

- 과제
  - 교재 및 학습내용과 관련된 연습 문제
  - 프로그래밍 (C 또는 Python 중 선택)

- 주의/참고 사항
  - 명시된 제출 기한 엄수 (추가 제출 없음)
  - 과제의 일부는 시험문제로 활용
  - 반드시 혼자의 노력으로 풀 것

시험 및 보강

- 시험 일정
  - 중간고사 : 미정 (학사일정 조정으로)
  - 기말고사: 6월 26일 (금)

- 보강
  - 온라인 수업이 끝나고 중간고사 전후로 판단하여 보강이 필요하면 오/오프라인 수업으로 진행함

강의 일정

일정	내용
1주	Course introduction / Python Programming Basic
2주	Brief History of Cryptanalysis / Substitution Cipher
3주	Breaking Substitution Cipher
4주	Number theoretic ciphers and underlying mathematics
5주	Factoring and discrete logarithms
6주	Invited Lecture: Quantum computing and quantum secure ciphers
7주	Block cipher and security measures
8주	Brute-force attack and TMTO(Time Memory Trade Off)

* 학습 진도에 따라 강의 일정과 순서는 일부 변경될 수 있음

강의 일정

일정	내용
9주	DC(Differential Cryptanalysis) – Theory
10주	DC(Differential Cryptanalysis) – Implementation
11주	LC(Linear Cryptanalysis) – Theory
12주	LC(Linear Cryptanalysis) – Implementation
!3주	Integral, Higher-order DC
14주	Impossible DC, Boomerang attack
!5주	Mentoring (Quantum-Safe Cryptography) and wrap up
16주	Final exam

* 학습 진도에 따라 강의 일정과 순서는 일부 변경될 수 있음

성적

- 반영 비율
  - 중간고사: 40%
  - 기말고사: 40%
  - 과제:10%
  - 출석: 10%

- 주의 사항
  - 상대평가 비율 이내에서 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

HOT Team Class

- HOT(Hitting the Obvious Things)팀Class 란?
  - 현장의 전문가를 산학멘토로 위촉하여 수업에 참여하게 한다는 의미와 TEAM 교육방식을 구현한다는 의미에서「HOT팀 Class」로 명명
  - 산업계 전문가가 수업의 설계, 진행, 멘토링 등에 참여 하는 교육모델

- 암호분석 과목의 HOT팀 Class 적용 방법
  - Big Question: 양자 컴퓨팅(quantum computing) 시대에도 안전한 암호기술은 어떻게 확보하는가?
  - Post quantum cryptography 전문가 참여로 암호분석의 미래를 전망함

* HOT TEAM Class 개설은 확정되지 않음 (3월 중 결정 예정)

온라인 강의

- 개강 후 4주 동안
  - 가상대학을 이용한 온라인 강의로 진행
  - 주요 내용
    - Python을 이용한 치환암호 구현
    - 암호분석에 필요한 수학