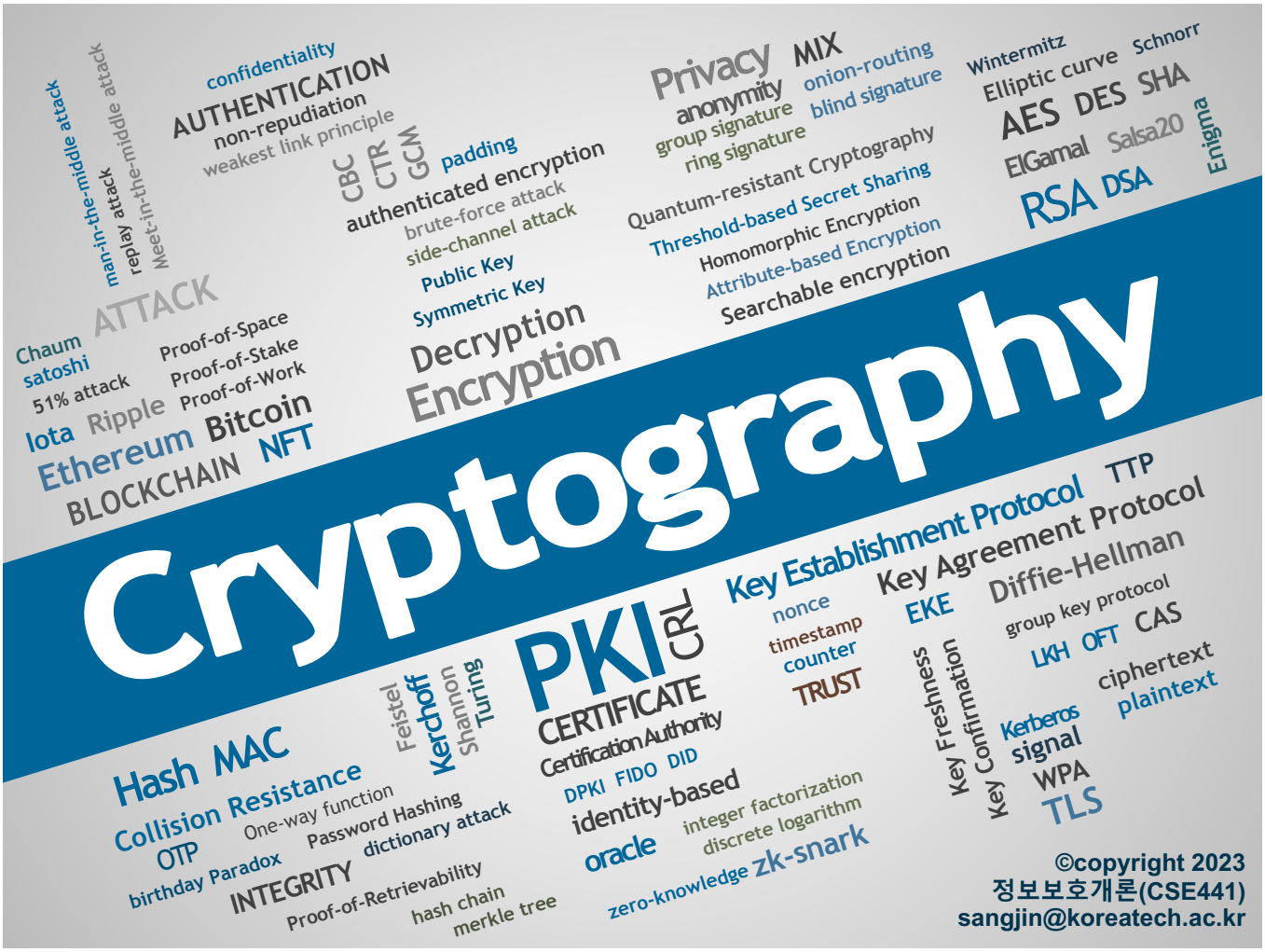
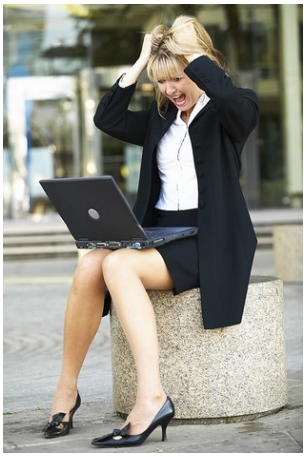


다음 용어들은 들어보셨나요???

- 바이러스
- 스파이웨어
- 백신: V3, 빗자루, 알약, avast
- 피싱
- 스팸 메일
- 해킹, 침입 탐지/예방
- DDoS(Distributed Denial-of-Service) 공격
- 방화벽(firewall)



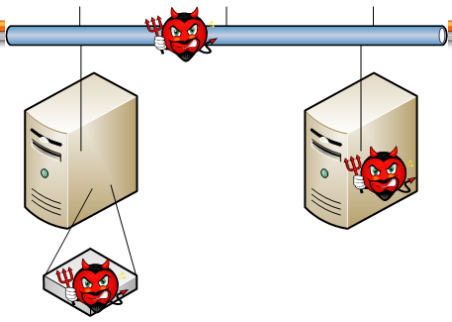
- HTTPS, WPA2
- 인증서, DID
- 전자서명, OTP
- 비트코인, 블록체인, NFT

이 용어들은?

- 제4차 산업혁명: 빅데이터/클라우드, 인공지능, IoT, 로봇
- 유비쿼터스(ubiquitous): invisible computer
  - 5A: 어디서나(any where), 언제나(any time), 어떤 장치(any device), 어떤 네트워크(any network), 어떤 서비스(any service)
  - 내재성(pervasive): 사물인터넷, 임베디드, 홈네트워크, 입는 컴퓨터
  - 지능화(intelligent): context-aware
- 융합(convergence)
  - 방송과 IT 기술의 융합: IPTV
  - 차량과 IT 기술의 융합: ITS(Intelligent Transportation System)
- All IP 시대: IPTV, OTT, VoIP → 초연결시대
- 정보화의 역기능
  - 보안 위협의 변화
  - 개인 프라이버시 침해
  - 공격의 용이성, 전파 속도와 파급 효과의 증가

공격의 경로가 더 이상 기존 컴퓨팅 장치로 제한되지 않고 있음

정보보호 분야



- 프로그램 보안
  - 공격자가 활용할 수 있는 허점이 없도록 소프트웨어를 구현하는 기술 (방어 프로그래밍, 안전 프로그래밍)
  - 기존 소프트웨어의 허점을 발견하는 기술
- 시스템 보안
  - 공격자가 활용할 수 있는 컴퓨터 시스템의 허점을 발견하는 기술
  - 컴퓨터 시스템에 공격자가 침입하였을 때 대응(탐지, 예방)하는 기술
- 네트워크 보안
  - 네트워크의 패킷을 분석하여 공격에 대응하는 기술
  - 통신 프로토콜의 보호
- 응용 보안
  - 응용의 보안 요구사항을 충족시키기 위해 사용되는 기술
- 기타: 컴퓨터 포렌식, 정보보호 정책, 정보보호 관련 법률, 정보보호 윤리, 정보보호 교육

4대 정보보호 서비스

- 비밀성(confidentiality): 인가된 사용자들만 데이터의 내용을 볼 수 있도록 해주는 서비스
- 무결성(integrity): 비인가된 데이터의 변경(삽입,삭제,교체)을 발견할 수 있도록 해주는 서비스
- 가용성(availability): 사용자가 요구하는 서비스가 항상 제공되도록 보장해주는 서비스
- 인증(authentication): 주장된 것을 검증할 수 있도록 해주는 서비스

- 이 중에 비밀성, 무결성, 인증은 보통 암호기술을 사용하여 제공함

강의 내용

- 이 교과는 정보보호 서비스를 제공하기 위해 사용하는 여러 기술 중 암호기술에 초점을 두는 교과임
- 암호기술을 이해하기 위해서는 다음을 학습하여야 함
  - 기본 도구인 각종 암호알고리즘의 특성과 사용법
  - 다양한 응용 서비스의 보안 요구사항을 충족하기 위해 사용하는 암호프로토콜을 설계하고 분석하는 방법
  - 암호알고리즘과 암호프로토콜의 특성을 이해하기 위한 수학 이론
- 이 강의는 개론 성격의 교과이므로 상세한 수준에서 위에 나열한 모든 내용을 다루지 않고 기본적인 개념을 충분히 이해할 수 있고, 흥미를 잃지 않도록 가능한 상위 수준에서 강의함
- 우리가 사용하는 각종 응용, 서비스에서 사용하는 암호기술 기반 정보보호 기술
  - WiFi: WPA2
  - Web: TLS, 패스워드 해싱
  - 인터넷 뱅킹: OTP, 인증서

강의 목표

- 암호기술을 바탕으로 정보보호 개념 이해
- 주어진 문제에 대한 보안 요구사항을 도출하는 능력
- 암호알고리즘에 대한 기본적 이해와 올바르게 활용할 수 있는 능력
- 주어진 보안 요구사항을 해결하기 위해 사용하고 있는 암호프로토콜 이해
  - 기초적인 암호프로토콜 설계 능력
  - 암호프로토콜에서 사용하고 있는 암호기술 이해
- 각 종 응용, 서비스에서 사용하는 암호기술 이해
- 암호기술의 안전성과 효율성을 분석하는 기초적인 능력
- 주어진 문제를 해결하는 다양한 방법 이해 및 응용 능력

개인 목표

- 정보보호 분야에서 일하고자 하는 학생들에게는 필수 교과
- 다른 컴퓨터공학 분야에 일하고자 하는 학생들에게는 유용한 전공 지식
  - 듣다 보니 관심이 생겨 새 목표를 가지게 될 수 있음
    - 정보보호 분야로 취업 또는 정보보호 분야에 대한 전문 지식 습득을 위한 진학
- 공통. 암호기술 분야에서 사용한 문제 해결 기법들을 여러 분이 앞으로 만나는 다양한 문제에 응용

강의정보 (1/3)

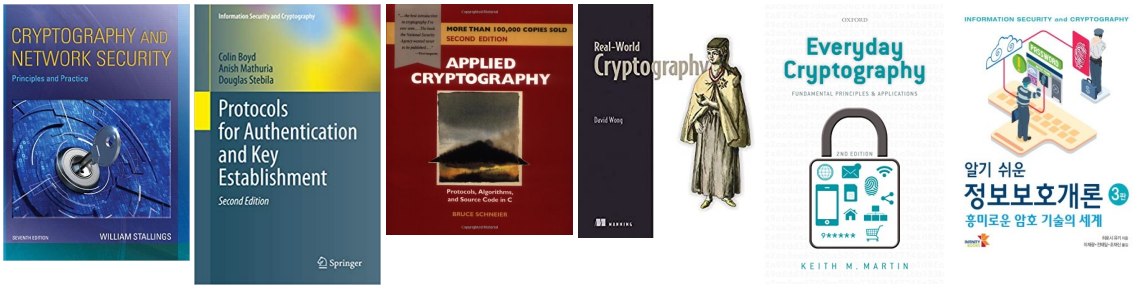
- 교수 정보
  - 연구실: 제2공학관 239호
  - 전화번호: 교내 1490 (041-560-1490)
  - 전자우편: sangjin@koreatech.ac.kr
  - 강의홈페이지: el.koreatech.ac.kr
  - 페이스북 페이지: www.facebook.com/koreatech.crypto
  - 유투브: youtube.com/c/SangjinKim
    - 강의녹화 업로드 (복습에 활용)
  - 교재: 주차별로 직접 제공함
  - Pre-requiste: 데이터통신, 컴퓨터네트워크

강의정보 (2/3)

- 강의 평가 방법
  - 출석: 5%, 퀴즈 5%, 질의응답 5%, 숙제: 10%, 중간: 35%, 기말: 35%
    - 참고. 바뀔 수 있음
- 출석은 전자출결
- 퀴즈: el을 통해 매주 3~5문제 제공 (4지선다 또는 단답형)
- 과제
  - 각 장이 끝날 때마다 교재에 있는 연습문제를 풀어 el로 제출
    - 연습문제 중 지정된 문제
  - 각 장의 내용과 연관된 최신 기술/이슈 관련 문제나 자료 조사
  - 매주 5명 정도를 랜덤으로 선택하여 제출 답안을 이용하여 과제 피드백 영상을 촬영하여 제공
- 중간, 기말: 8주, 15주
  - 9주에 중간시험 피드백 영상 제공

강의 정보 (3/3)

- 강의 부교재
  - W. Stalling, Cryptography and Network Security,7th Ed., 2016
  - Colin Boyd, Anish Mathuria, Douglas Stebila, Protocols for Authentication and Key Establishment, 2nd Ed., Springer, 2019
  - B. Schneier, Applied Cryptography, 2nd Ed., Wiley, 1996
  - David Wong, Real-World Cryptography, Manning, 2021
  - K. Martin, Everyday Cryptography, Oxford Univ. Press, 2017
  - 히로시 유키, 알기 쉬운 정보보호개론, 3판, 인피니티북스, 2017



강의계획

1	강의 소개, 암호기술 개요	9	해시함수의 활용
	암호알고리즘 개요 Part I 암호알고리즘 개요 Part II		
2		10	다자간 키 확립 프로토콜
3		11	고급 암호기술 1부: 비밀 공유 기법, 데이터 아웃소싱 보안
	암호프로토콜 개요		
4	암호프로토콜 기초 설계 기법 키 확립 프로토콜 개요	12	고급 암호기술 2부: 고급 전자서명 기술, 익명 인증 기술
			블록체인 Part I
5	암호프로토콜에 대한 공격	13	
	암호알고리즘 Part I 암호알고리즘 Part II 자바/파이썬 암호라이브러리		
6		14	블록체인 Part II
7		15	기타 응용 보안
	키 확립 프로토콜 대표 사례		
8	중간시험	16	기말시험

암호프로토콜의 예: 동전 던지기

- 원격에 있는 두 사용자 Alice와 Bob은 동전 던지기를 하고 싶다.
  - Alice가 동전을 던지고, Bob이 그 결과를 예측하기로 함
  - 그러나 Bob은 실제 동전 던지는 과정을 볼 수 없으므로 Alice를 믿기 힘듦
- 요구사항
  - Alice는 동전 던진 결과를 Bob에게 속일 수 없어야 함
- 주어진 도구
  - Magic function f:
    - 특성 1. 모든 정수 x에 대해 $f(x)$를 계산하는 것은 쉽지만 $f(x)$로부터 그것의 원상(pre-image)을 계산하는 것은 불가능함. 특히, 원상이 짝수인지 홀수인지 구분할 수 없음
    - 특성 2. $x \neq y$이지만 $f(x) = f(y)$인 정수쌍 $(x,\ y)$를 찾는 것은 불가능함 (충돌)

f를 이용한 동전 던지기 프로토콜

- 프로토콜
  - 단계 1. Alice는 매우 큰 정수 x를 선택하여 $f(x)$를 계산하고, $f(x)$ 값을 Bob에게 전달함
  - 단계 2. Bob은 $f(x)$의 원상 x가 짝수인지 홀수인지 추측하여 그 결과를 Alice에게 전달함
  - 단계 3. Alice는 x를 Bob에게 전달함
  - 단계 4. Bob은 x가 $f(x)$의 올바른 원상인지 확인함

- 분석
  - f 함수의 특성 2 때문에 Alice는 $f(x)$를 Bob에게 전달한 후에 실제 사용한 원상 x 대신에 다른 x를 찾을 수 없음
  - f 함수의 특성 1 때문에 Bob은 $f(x)$를 통해 원상 x에 대한 어떤 정보도 얻을 수 없음
    - 맞출 확률이 50% 이상이 되도록 해주는 추가 정보를 얻을 수 없음