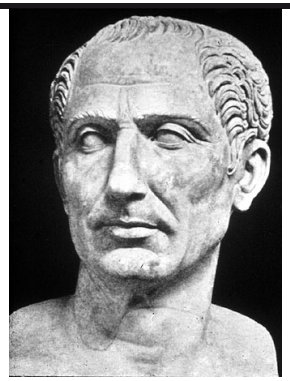
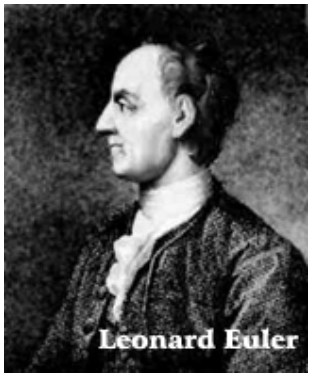
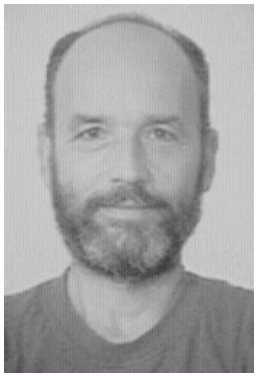
EE817/IS 893
Cryptography Engineering and Cryptocurrency

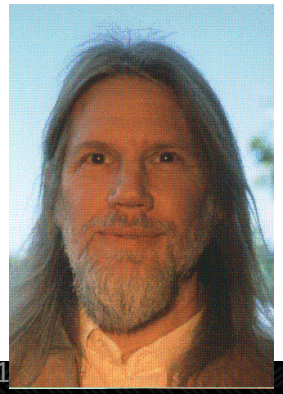
Yongdae Kim
한국과학기술원

Who's who?



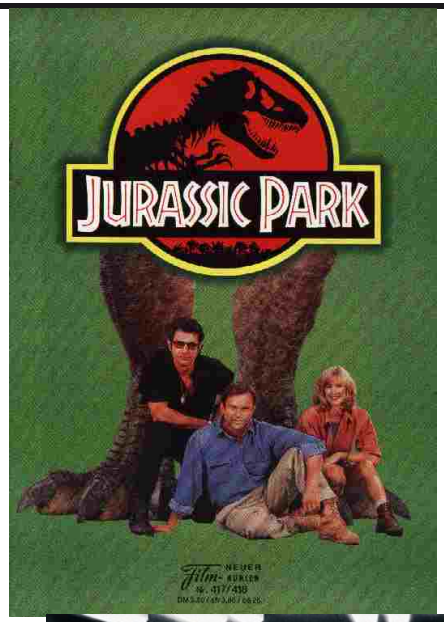



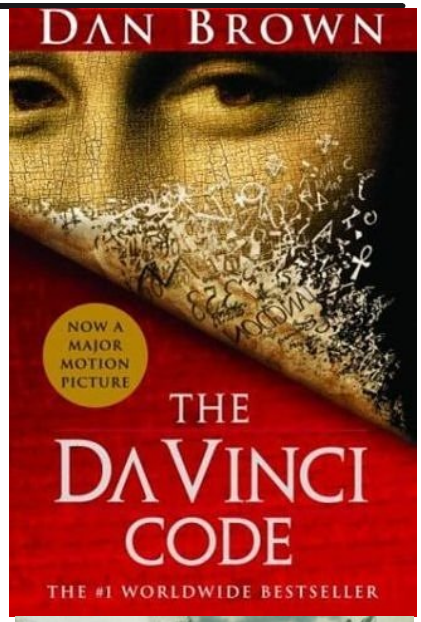


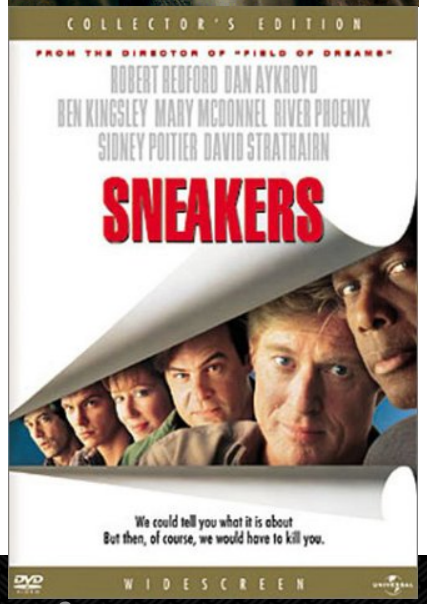
Some movies


RUSSELL CROWE
A BEAUTIFUL MIND


ENIGMA
DAS GEHEIMNIS
SENATOR
UNIVERSAL


JURASSIC PARK


DAN BROWN
NOW A MAJOR MOTION PICTURE
THE DA VINCI CODE
THE #1 WORLDWIDE BESTSELLER


COLLECTOR'S EDITION
FROM THE DIRECTOR OF "FIELD OF DREAMS"
ROBERT REDFORD DAN AYKROYD
BEN KINGSLEY MARY MCDONNEL RIVER PHOENIX
SIDNEY POITIER DAVID STRATHAIRN
SNEAKERS
We could tell you what it is about
But then, of course, we would have to kill you.
WIDESCREEN


Meet James Bond,
secret agent 007
His new incredible women...
His new incredible enemies...
His new incredible adventures...
IAN FLEMING'S
FROM RUSSIA WITH LOVE
SEAN CONNERY AS JAMES BOND
DANIELA BIANCHI
JOHN BARRY
TERENCE YOUNG
TECHNICOLOR
UNITED ARTISTS


JOHN TRAVOLTA
HUGH JACKMAN
HALLE BERRY
DON CHEADLE
Log on.
Hack in.
Go anywhere.
Steal everything.
SWORD FISH
PASSWORD ACCEPTED


U-571

Introduction

- Class Information
  - Title: Cryptography Engineering and Cryptocurrency
  - Course Number: EE817/IS 893
  - Lectures: MW 10:30Am - 11:45Am, N1 111

- Has been experimental and challenging to teach this course…
  - Trying to learn how to teach this course well

Instructor, TA, Office Hours

- Instructor
  - Yongdae Kim
    - » 1st time teaching EE817/IS 893 in KAIST
    - » Taught 10 times in Minnesota
  - Email: yongdaek (at) kaist. ac. kr, yongdaek (at) gmail. com
    - » Please include ee817 or is893 in the subject of your mail
  - Office: N26 201
  - Office Hours: TBD
- TA
  - EE TA: Yujin Kwon, dbwls8724 (at) kaist.ac.kr, Dohyun Kim, dohyunjk (at) kaist.ac.kr
  - GSIS TA: Yunjong Jeong, yunjong (at) kaist.ac.kr
  - Office hours:

Class web page, e-mail

- http://syssec.kaist.ac.kr/~yongdaek/courses/is893/
  - Read the page carefully and regularly!
  - Read the Syllabus carefully.
  - Check calendar.

- E-mail policy
  - Include [ee817] or [is893] in the subject of your e-mail

Textbook

- Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone (Editor), CRC Press, ISBN 0849385237, (October 16, 1996) Available on-line at http://www.cacr.math.uwaterloo.ca/hac/
- Some research papers

Prerequisite

- Recommended
  - Discrete Mathematics, Data Structure or Algorithm and some math

- Quiz Today
  - To understand your mathematical knowledge
  - Nothing to do with your grade
  - 30 minutes will be given

Course Objectives

- To learn
  - mathematical background for cryptographic techniques
  - basic cryptographic techniques for computer and network security
  - how secure these techniques are
  - **how to use these techniques securely**
  - **how to apply these techniques**

Student Expectations

- Keep up with material
  - complete relevant readings before class
  - browse lecture slides
    - » Slides will be on-line the same day, after class
- Attend lectures
  - Understanding lecture is as important as reading before class.
- Feedback!!!!
- Read your email regularly. No excuses!
- Quizzes, Exams and homework:
  - Write your own answer
  - Violators will be prosecuted
  - An F in the course is guaranteed

Class Information

- Lecture format
  - Slides (will try to post before class, but not guaranteed)
- Browse the course Web site often
  - http://syssec.kaist.ac.kr/~yongdaek/courses/is893/
  - check it regularly
  - news and lecture notes (in PDF, PPT) will all be there
- Please read your email!

Grading

- Distribution
  - Midterm: 18%
  - Final: 28%. (In-class)
  - 6 biweekly assignments: 12 %. (6 x 3 %) Hard
  - 6 biweekly quizzes: 30 %. (6 x 6 % each) Easy
- Policy
  - 90.0% or above yields an A, 87.0% an A-, 83% = B+, 80% = B, 75% = B-, 70% = C+, 65% = C, 60% = C-, 55% = D, and less than 50% yields an F.
  - You can fail (<50%) quiz at most once (Twice or more fails = F)

Assignment

- Submission instruction
  - Type up your homework by text/pdf file. Send me (CC TA) as either mail body or attachment.
    - » No html email, doc, …
  - Check Calendar.
    - » First homework due: On the week of Mar 16
    - » First quiz: On the week of Mar 16
  - No grading for late Homework/missing quizzes
    - » If you cannot submit/take it, let me know in advance.
    - » Provide evidence.

Course Topic - tentative

- Mathematics! Mathematics! Mathematics!
- Symmetric Ciphers
- Hash Functions and Integrity
- Public Key Encryption
- Digital Signatures
- Identification and Authentication
- Key Establishment and Management
- Cryptocurrency
  - Bitcoin, Etherium, Alt-coins, Consensus Algorithms

You may not be able to…

- Become expert (needs time…)
- Learn everything
- Break well-known encryption algorithm
- Wireless security, P2P security, …

- You may be able to (I hope)
  - be interested in security
  - be very strong in mathematics (number theory, …)
  - Know technologies behind cryptocurrency

Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google "Yongdae Kim"