King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering

ICS 555 Data Security and Encryption (3-0-3)

Instructor: Dr. Marwan Abu-Amara
Office: 22-145
Phone: 1632
E-mail: marwan@kfupm.edu.sa
Term: 162 (2nd term 2016–2017)
Day & Time: MW 05:00 PM – 06:15 PM
Location: 22-119
Prerequisite: Consent of Instructor (ICS 454 taken is highly recommended)
Textbook: *A Course in Number Theory and Cryptography*, N. Koblitz, Springer-Verlag, 2nd Edition, 1994.
Office Hours: UTR 11:00 AM – 11:55 AM or by appointment
Web Site: http://faculty.kfupm.edu.sa/COE/marwan

Catalog Description:

Mathematical principles of cryptography and data security. A detailed study of conventional and modern cryptosystems. Zero knowledge protocols. Information theory, Number theory, complexity theory concepts and their applications to cryptography.

Tentative Grading Policy:

- Homeworks **20%**
- Research Project* **25%**
- Midterm Exam ..... **25%** (Week 10 – Monday April 17, 2017 during class time)
- Final Exam ..... **30%** (Sunday May 28, 2017, 9:00 PM)

* *A separate handout will be distributed describing the offered projects and the respective deadlines*

IMPORTANT NOTES:

- Use of cell phones, smart phones, and tablets during class period and during exams is absolutely **prohibited**.
- All KFUPM regulations and standards will be enforced. Attendance will be checked each class. The KFUPM rule pertaining to a DN grade will be strictly enforced (i.e. **> 6 absences** will result in a DN grade).
- Only university approved excuses will be accepted, and should be presented **no later than 1 week** after returning to classes.
- Homeworks are to be submitted **in class** on the due date. Late homeworks will **NOT be accepted**.
- You have up to the next class period to object to the grade of a homework or the midterm exam from the end of the class period in which the graded papers have been distributed back.
- **NO make ups for homeworks or exams**. ALL homeworks will be counted towards your grade.
- Final exam is **comprehensive**.

TENTATIVE Weekly Course Schedule

Week	Topic
1	Introduction to Data Security and Cryptography
2 – 3	Introduction to Number Theory, Modular Arithmetic, Complexity Theory, Group Theory
4 – 5	Symmetric-Key Cryptography
6 – 7	Public-Key Cryptography
8 – 10	Message Authentication, Secure Hashing, Digital Signatures
11 – 12	Zero-Knowledge Proofs and Oblivious Transfer
13 – 14	Elliptic-Curve Cryptography
15	Presentation of Projects