BILKENT UNIVERSITY
Department of Computer Technology and Information Systems
2012 - 2013 Fall Semester
CTIS 496 Data Security in Computing

Course Code	**CTIS 496**	
Course Name	**Data Security in Computing**	
Course Credit	3 (3 hour lectures in class)	
Instructor	Dr. Hamdi Murat Yıldırım	http://www.bilkent.edu.tr/~hmurat hmurat@bilkent.edu.tr Office E118 / Phone: x5072
Course Description	The course covers theory and practice of computer security, focusing in particular on the security aspects of the computing systems. It surveys classical cryptography and cryptographic tools used to provide security, such as shared key encryption (DES, 3DES, AES, RC4 etc.); cipher block modes of operation, cryptographic hash functions, public key encryption, key exchange, and digital signature (Diffie-Hellmann, RSA, DSS, etc.) Besides, it then briefly reviews how these tools are utilized in Public Key Infrastructure (PKI), Transport-Level Security, Wireless Network Security, Electronic Mail Security and IP Security.	
Text Book	**Network Security Essentials** by William Stallings, Fourth Edition, 2011 **Cryptography Theory and Practice (Chapter1)** by Douglas R. Stinson	
Other References	**Course materials of the Online Cryptography Course titled "Introduction to Cryptography", Stanford University, https://class.coursera.org/crypto-preview/class/index** **Cryptography and Network Security: Principles and Practice** by William Stallings, Fifth Edition, 2011 **Network Security** (Private Communication in a Public World) by Charlie Kaufman, Second Edition, 2002. **Reference books and references available on web sites.**	
Grading (Tentative)	Quiz 1 (Week 5) %8 Midterm Exam (Week 8) %30 Quiz 2 (Week 11) %8 Homeworks & Project %12 Final Exam %35 Performance, moodle and in-class participation and attendance %7	

Overview

For the security of the operating systems, software, communication hardware, embedded systems, devices and software, cryptographic algorithms are required (considering algorithms, protocols and implementations).

Some reasons to take this course:

- You should be familiar with modern cryptographic algorithms, techniques, protocols, network and computer security related concepts (at least introductory level). When you are involved in a software project, you can use them to enhance the security of the software.
- Certainly it gives additional skills to find more (good) jobs.

Throughout this course, we will use some software such as

* Main reference, strongly recommended: http://www.cryptool.org/ ("Cryptool 1" e-learning application – you may look at its nice documentation)

* (Well known, widely used) http://www.openssl.org (toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library)

* GnuPG is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC4880 (http://www.gnupg.org/)

Attendance Policy

You are expected to attend all lectures. Participation in this course is very important. Learning course topics will be enhanced by regular attendance. Moreover, regular attendance will improve your grade in the course.

- **At least 50% of attendance is required. Students who fail to satisfy this requirement will automatically get an FX grade**.
- **Students who do not attend/submit more than 55% of assessments/exams: fail the course (FX).**
- **If a student earns an FX grade, (s)he can attend the rest of the lectures but cannot attend any exams.**

Class participation will contribute to your final grade:

%60-%69: 1 pt. / %70-%79: 2 pts. / %80-%89: 3 pts. %90 +: 4 pts.

Grading Policy

Passing grades range from A to D; F is a fail. A student is required to obtain at least 45% in total to pass this course.

Changes

- The Information and Schedules contained in this course Syllabus are subject to change.
- Students will be informed of any changes either in the class and/or by e-mail and/or publishing at the course moodle web site.
- It is each students' responsibility to regularly check this website and their e-mail accounts to learn of course changes.

Course Overview

- Introduction (1 week) --Security Goals (Confidentiality, Integrity and Availability), X800 International standard: X.800 Security Architecture: Security attacks, services and mechanisms

- Cryptography (with theory /applications -9 week-)

– Classical Cryptography --2,5 weeks--: Some Simple Cryptosystems (Ceaser, Affine, Substitution and Permutation ciphers etc.) and Their Cryptanalysis

– Symmetric Encryption Algorithms (Block Ciphers and Stream Ciphers) – 2 weeks--

– Cipher Block Modes of Operation, Hash functions, MAC and HMAC –1,5 week--

– Asymmetric (Public Key) Encryption Algorithms (RSA, DSS, Elliptic Curve Cryptography

etc.), Digital Signatures, Key Management / Distribution and Some Applications –1,5 weeks--

– Public Key Infrastructure (PKI) and some related applications –1,5 week--

- Network Security Applications (4 weeks)

– Electronic Mail Security (Introduction to PGP & S/MIME)

– Transport-Level Security (SSL & TLS, HTTPS)

- Wireless Network Security

- IP Security

TENTATIVE COURSE OUTLINE

WEEKS	CONTENTS	REFERENCES
Week 1 (Sep 17 – 21)	* **Course Overview** ** **Introduction**	* **Readings:** http://en.wikipedia.org/wiki/Computer_Security http://en.wikipedia.org/wiki/Cryptography http://www.ibm.com/developerworks/library/s-pain.html ** Chp 1 (Stallings)
Week 2 (Sep 24– 28)	**Classical Cryptography** (Some Simple Cryptosystems)	Chp 1 (Stinson) / Cryptool 1 (http://www.cryptool.org)
Week 3 (Oct 1 – 5)	**Classical Cryptography** (Some Simple Cryptosystems) **Classical Cryptography** (Cryptanalysis)	Chp 1 (Stinson) / Cryptool 1
Week 4 (Oct 8 – 12)	**Classical Cryptography** (Cryptanalysis) **Cryptography:** Symmetric Encryption and Message Confidentiality: Symmetric Encryption Principles/Algorithms -Block Ciphers	Chp 1(Stinson), Cryptool 1 Chp 2 (Stallings) / Cryptool 1
Week 5 (Oct 15 – 19, Oct 22-23)	**Cryptography:** Symmetric Encryption and Message Confidentiality: Symmetric Encryption Principles/Algorithms -Block Ciphers	Chp 1 (Stinson) / Chp 2 (Stallings) / Cryptool 1
Week 6 (Oct 30 – Nov 2)	**Cryptography:** Symmetric Encryption and Message Confidentiality: Symmetric Encryption Principles/Algorithms -Block Ciphers -Stream Ciphers	Chp 2 (Stallings) / Cryptool 1/ Openssl

Week 7 (Nov 5 - 9)	**Cryptography:** Symmetric Encryption and Message Confidentiality: -Cipher Block Modes of Operation **Cryptography:** Public-Key Cryptography and Message Authentication : -Message Authentication	Chp 2 (Stallings) / Cryptool 1/ Openssl
Week 8 (Nov 12 - 16)	**Cryptography:** Public-Key Cryptography and Message Authentication : – Secure Hash Functions and HMAC – Digital Signatures	Chp 3 (Stallings) / Cryptool 1/ Openssl
Week 9 (Nov 19 - 23)	**Cryptography**: Public-Key Cryptography and Message Authentication: Public-Key Cryptography Algorithms) – Key Management and Some Applications **Cryptography**: Authentication Applications: -X.509 Authentication Service and Public-Key Infrastructure	Chp 3 (Stallings) / Cryptool 1
Week 10 (Nov 26 -30)	**Cryptography:** Authentication Applications: X.509 Authentication Service and Public-Key Infrastructure	Chp 4 (Stallings) / Cryptool 1
Week 11 (Dec 3 - 7)	**Electronic Mail Security** (PGP and S/MIME)	Chp 7 (Stallings) / Cryptool 1 / GnuPG
Week 12 (Dec 10 - 14)	**Transport-Level Security** (Web Security Considerations, SSL & TLS)	Chp 5 (Stallings) / Cryptool 1/ Openssl
Week 13 (Dec 17 - 21)	**Wireless Network Security** (Wireless Transport Layer Security)	Chp 6 (Stallings)
Week 14 (Dec 24 - 28)	**IP Security**	Chp 8 (Stallings)
Week 15 & 16 (Jan 2 - 11)	**Final Examination**	