Bilgisayar Güvenliği ve Kriptografi
BLM5101

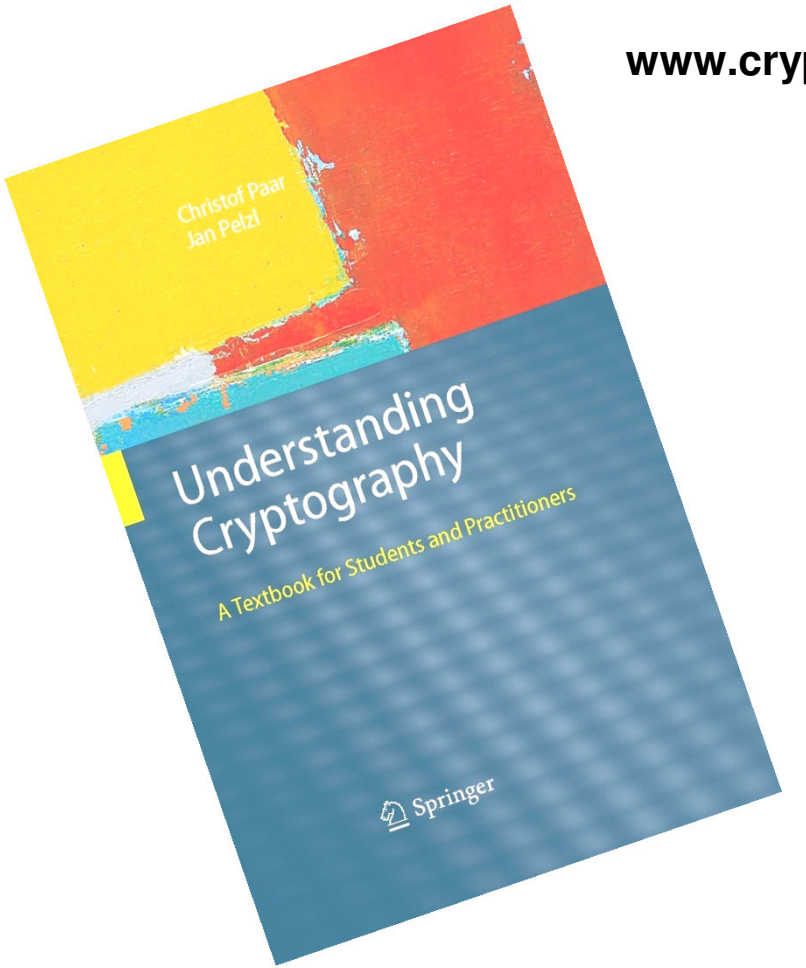
Doç. Dr. Sırma Yavuz

sirmayavuz@gmail.com

sirma@ce.yildiz.edu.tr

Understanding Cryptography – A Textbook for Students and Practitioners

by Christof Paar and Jan Pelzl



www.crypto-textbook.com

Bilgisayar Güvenliği ve Kriptografi BLM5101 - Gr 1			
Hafta	**Tarih**	**Konular**	
1	18.Şub.16	Giriş	Introduction to Cryptography
2	25.Şub.16	Kriptografi-Bilgi Güvenliği Temeller	Introduction to Cryptography
3	03.Mar.16	Ders Yok	No Class
4	10.Mar.16	Akan Şifreleme	Stream Ciphers
5	17.Mar.16	DES	DES - Data Encryption Standard
6	24.Mar.16	AES	AES - Advanced Encryption Standard
7	31.Mar.16	Modes of Operation Ch5	Block Cipher Mode Implementation
8	07.Nis.16	Ara Sınav	Midterm Exam
9	14.Nis.16	Blok Şifreleme - Public key kripto Intro - number theory Ch 6	Introduction to Public-Key Cryptography
10	21.Nis.16	RSA	The RSA Cryptosystem
11	28.Nis.16	Diskrit Logaritma Tabanlı Public-Key Kriptografi	Public-Key Cryptosystems Based on the DLP
12	05.May.16	Eliptic Curve Kriptografi/Dijital İmza	Elliptic Curve Cryptosystems/Digital Signatures
13	12.May.16	Sınav Haftası – Son Rapor Teslimi-Sunumlar	Midterm Week-FinalReport Submission
14	19.May.16	Sunumlar	Presentations
15	26.May.16	Sunumlar	Presentations

- Dersle ilgili duyuruları takip etmek için:

Yıldız Kriptografi grubuna üye olmanız gerekmektedir (Subscribe to the group)

https://groups.google.com/forum/#!forum/kripto2016

Ders Projesi ve Sunum %30

- Ara Sınav %30
- **Proje konunuzu 3 Mart tarihine kadar e-mail ile bildirmeniz gerekiyor**
- Final - % 40

Proje Konuları