**İ.Y.T.E**

**MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ**

**LİSANSÜSTÜ PROGRAMLARINDA YENİ AÇILACAK**

**DERSLER İÇİN TANITIM FORMU**

**Gönderen : Bilgisayar Mühendisliği Anabilim Dalı**

**Bilgisayar Bilimleri ve Mühendisliği Ortak Doktora Programı**

**Gönderilen : Mühendislik ve Fen Bilimleri Enstitü Müdürlüğü**

| | | |
|---|---|---|
| Dersin Kodu ve Kredisi | | : CENG661 (3+0) 3 |
| Dersin Adı | (İngilizce) | : Advanced Asymmetrical Cryptosystems |
| | (Türkçe) | : İleri Asimetrik Kriptosistemler |
| Dersin Amacı | (İngilizce) | : At the end of the course, the students will be analyzed the open research topics of asymmetrical cryptography and its security functions. They will learn the recent solution protocols, related standards and their already exist vulnerabilities. The students will have the ability to do risk analysis and assessment for asymmetrical cryptographic solution mechanisms. |
| | (Türkçe) | : Dersi alan öğrenciler için hedef; Asimetrik kripto sistemlerin çözüm olarak kullanıldığı açık problemleri analiz edebilmek, olası çözüm protokollerini öğrenmek, doğru çözüm aracını belirleyebiliyor ve risk analizini yapabiliyor olmak. |
| Dersin İçeriği | (İngilizce) | : This course follows on from the introductory cryptography course. In that course cryptographic algorithms were introduced according to the properties they possessed and how they might fit into larger security architecture. In this unit, the most popular and widely deployed algorithms are studied and highlighted design and cryptanalytic trends over the past twenty years. This course is, by necessity, somewhat mathematical and some basic mathematical techniques will be used. However, despite this reliance on mathematical techniques, the emphasis of the module is on understanding the more practical aspects of the performance and security of some of the most widely used cryptographic algorithms. |
| | (Türkçe) | : Asimetrik kripto sistemlere ilişkin temel matematik konuları ve uygulama koşul ve prensipleri değerlendirilecektir. Dönem sonunda öğrencilerin güvenlik problemini analiz ederek, en uygun protokolü seçme ve uygulayabilme yeterliliğinde olması için çalışmalar kuramsal ve uygulamalı olarak yürütülecektir. |

Dersin Taslağı (İngilizce) :

1. General introduction
2. Mathematics: The integer factorization problem, The RSA problem, the quadratic residuosity problem, Computing square roots in Zn, The discrete logarithm problem, The Diffie-Hellman problem.
3. Mathematics: Composite mod, Computing individual bits, The subset sum problem, Factoring polynomials over finite fields, Notes and further references, Probabilistic primality tests, (True) Primality tests, Prime number generation.
4. Mathematics: Irreducible polynomials over Zp, Generators and elements of high order, Notes and further references, Random bit generation, Pseudorandom bit generation, Statistical tests, Cryptographically secure pseudorandom bit generation.
5. Public Key: Rabin Public-Key Algorithm, ElGamal Public-Key Algorithms.
6. Public Key: Knapsack Public-key Encryption, Merkle-Hellman Knapsack Algorithm, Goldwasser-Micali Probabilistic Algorithm.
7. Public Key: Elliptic Curve Algorithm.
8. Digital Signature: Public-key cryptography standards (PKCS #1) Formatting; PKCS #1 Data Formatting, Signature Process for PKCS #1, Verification Process for PKCS #1, The ElGamal Signature Algorithm, The Digital Signature Algorithm (DSA), Fiat-Shamir Algorithm.
9. Digital Signature: The Schnorr Signature Algorithm, The ElGamal Signature Algorithm with Plaintext Recovery, Nyberg-Rueppel Algorithm, One-Time Digital Signatures, The Rabin One-Time Signature Algorithm, The Merkle One-Time Signature Algorithm, Other Signature Algorithms, Arbitrated Digital Signatures, ESIGN, Blind Signature Algorithms.
10. Hash Function: Unkeyed hash functions (MDCs) Cryptography Hash functions based on block ciphers Cryptography Hash functions based on modular arithmetic (MASH) Other Cryptography Hash Functions MD Family (MD2, MD4 and MD5) SHA Family (1, 256,384 and 512) RIPEMD Family (160, 128, 256) Keyed hash functions (MACs) The Keyed Hash MAC Code (HMAC) MACs Based on Block Ciphers Constructing MACs from MDCs Customized MACs The Use of the Hash Functions (Message Authentication) Definitions and types Comparison of Non-malicious and malicious threats to data integrity Data integrity using a MAC alone Data integrity

using an MDC and an authentic channel Data integrity combined with encryption.

11. Authentication: Zero-Knowledge Interactive Proof Systems and Zero-Knowledge Protocols Remarks on Zero-Knowledge.
12. Authentication: Other Asymmetric Protocols General structure of zero-knowledge protocols Feige-Fiat-Shamir identification protocol Guillou-Quisquater identification protocol Schnorr identification protocol.
13. Key Managements: Key generation, distribution and management protocols.
14. Cryptography Algorithms Applications: More on Cryptography Algorithms Applications.

(Türkçe) :

1. Genel giriş
2. Ilgili matematik altyapıları; "The integer factorization problem, The RSA problem, the quadratic residuosity problem, Computing square roots in Zn, The discrete logarithm problem, The Diffie-Hellman problem".
3. Ilgili matematik altyapıları; "Composite mod, Computing individual bits, The subset sum problem, Factoring polynomials over finite fields, Notes and further references, Probabilistic primality tests, (True) Primality tests, Prime number generation".
4. Ilgili matematik altyapıları; "Irreducible polynomials over Zp, Generators and elements of high order, Notes and further references, Random bit generation, Pseudorandom bit generation, Statistical tests, Cryptographically secure pseudorandom bit generation".
5. Açık anahtar yapıları; "Rabin Public-Key Algorithm, ElGamal Public-Key Algorithms".
6. Açık anahtar yapıları; "Knapsack Public-key Encryption, Merkle-Hellman Knapsack Algorithm, Goldwasser-Micali Probabilistic Algorithm".
7. Açık anahtar yapıları; "Elliptic Curve Algorithm"
8. Sayısal İmza; "Public-key cryptography standards (PKCS #1) Formatting; PKCS #1 Data Formatting, Signature Process for PKCS #1, Verification Process for PKCS #1, The ElGamal Signature Algorithm, The Digital Signature Algorithm (DSA), Fiat-Shamir Algorithm."
9. Sayısal İmza; "The Schnorr Signature Algorithm, The ElGamal Signature Algorithm with Plaintext Recovery, Nyberg-Rueppel Algorithm, One-Time Digital Signatures,

The Rabin One-Time Signature Algorithm, The Merkle One-Time Signature Algorithm, Other Signature Algorithms, Arbitrated Digital Signatures, ESIGN, Blind Signature Algorithms".

10. Hash Fonksiyonları
11. Kimlik denetimi; "Zero-Knowledge Interactive Proof Systems and Zero-Knowledge Protocols Remarks on Zero-Knowledge".
12. Kimlik denetimi; "Other Asymmetric Protocols General structure of zero-knowledge protocols Feige-Fiat-Shamir identification protocol Guillou-Quisquater identification protocol Schnorr identification protocol".
13. Anahtar yönertimi; anahtar üretimi, dağıtımı ve yönetimi.
14. Kriptografik algoritma uygulamaları.

Kullanılacak Materyal-Kitap ve Referanslar :


Introduction to Cryptography with Coding Theory 2nd Ed., W. Trappe, L.Washington, 2006.

Handbook of Applied Cryptography, A.Menezes, P.van orschot, S.Vanstone, 1996.

Complexity and Cryptography an Introduction, J. Talbot, D. Welsh, 2006.

Basics of Contemporary Cryptography for IT Practitioners, Ryabko, B. Fionov, Andrey, 2005, (from ebrary).

Innovative Cryptography 2nd Ed., M. Alex, M. Nick, 2007, (from ebrary).

User's Guide to Cryptography and Standards, D. Alex, M.Chris, 2004, (from ebrary).

"Applied Cryptography, Schneier B., John Wiley and Son, Inc. 1996

Cryptography and Network security: Principles and Practices, William Stallings, Third ed. Prentice Hall 2003 ISBN: 0-13-091429-0

XML Hacks, Michael Fitzgerald, O'Reilly's Hacks Series 2004 ISBN: 0-596-00711-6


Değerlendirme Yöntemi :

| | |
|---|---|
| Ara Sınav | %25 |
| Dönem Projesi | %30 |
| Proje Yayını | %45 |

Dersi Verecek Olan Öğretim Üyesi : Yrd. Doç. Dr. Serap ATAY