İçerik

Ders Kodu	Dersin Adı	Yarıyıl	Teori	Uygulama	Lab	Kredisi	AKTS
INF441	Şifrelemeye Giriş	8	3	0	0	3	4

Ön Koşul	INF315
Derse Kabul Koşulları	INF315

Dersin Dili	Türkçe
Türü	Seçmeli
Dersin Düzeyi	Lisans
Dersin Amacı	Kriptografi çok eski bir bilim dalı olsa da son zamanlarda gerçek bir devrim geçirmiştir. Aritmetikten gelen teknikler, tek yönlü olarak adlandırılan özellikleri oluşturmakta yardımcı olmuştur. Örneğin açık anahtarı bilen herkes için şifrelemek çok kolay olurken, özel anahtarı bilmeyenler için şifreyi çözmek imkansız bir hale gelmiştir. Modern şifreleme bilgisayarlara, e-ticaret sistemlerine, banka işlemlerine erişimi güvence altına almak için, hatta dijital bir belgeyi tasdik etmek ya da elektronik oy için de kullanılmaktadır. Bu bağlamda, bu dersin amaçları şu şekilde sıralanabilir: - Açık anahtar şifreleme sistemlerinde kullanılan başlıca algoritmaların öğretimi: "açgözlü" (greedy) algoritmalar, Euclid algoritması ve modülo n kuvvetinde hızlı hesaplama algoritmaları - Açık anahtar sistemlerinde kullanılan başlıca aritmetik teoremlerin ispatlanması - Teoremlerin Merkle-Hellman, RSA ve El Gamal şifreleme sistemlerine uygulanması - Sistemlerin güvenliğine dayalı özelliklerinin açıklanması - Şifreleme sistemlerinin ayrıca kimlik doğrulama sistemlerinde nasıl kullanıldığının gösterilmesi - Eski (Ceaser, Vigenère, ...) ve Modern (tek kullanımlı şifre, Hill şifreleme) gizli anahtar şifreleme sistemlerinin öğrenciye tanıtılması - Farklı blok şifreleme sistemlerini sunulması.
İçerik	1. Hafta Glouton algoritması, şifreleme biliminde uygulamalar 2. Hafta Euclide algoritması ve mod n uygulaması 3. Hafta Lagrange ve Fermat teoremleri, hızlı ve modüler hesaplama uygulamaları 4. Hafta RSA şifreleme sistemi 5. Hafta Blok RSA şifreleme 6. Hafta Ayrık logaritma problemi 7. Hafta Diffie-Hellman anahtar değişim yöntemi 8. Hafta Ara Sınav 9. Hafta El Gamal şifreleme sistemi 10. Hafta Elektronik imza, imza ve hash fonksiyonları 11. Hafta César, Vigénère, vb. gibi klasik şifreleme yöntemleri 12. Hafta Hill şifreleme 13. Hafta Blok şifreleme yöntemlerinin prensipleri ve çalışma mekanizmaları 14. Hafta Feistel şeması
Kaynaklar	1.Ders Notları: http://uni.gsu.edu.tr/moodle/course/view.php?id=53 2. Cours de cryptographie, Gilles Zémor, Cassini. ISBN 2-84225-020-6

Teori Konu Başlıkları

Hafta	Konu Başlıkları
1	Glouton algoritması, şifreleme biliminde uygulamalar
2	Euclide algoritması ve mod n uygulaması

Hafta	Konu Başlıkları
3	Lagrange ve Fermat teoremleri, hızlı ve modüler hesaplama uygulamaları
4	RSA şifreleme sistemi
5	Blok RSA şifreleme
6	Ayrık logaritma problemi
7	Diffie-Hellman anahtar değişim yöntemi
8	Ara Sınav
9	El Gamal şifreleme sistemi
10	Elektronik imza, imza ve hash fonksiyonları
11	César, Vigénère, vb. gibi klasik şifreleme yöntemleri
12	Hill şifreleme
13	Blok şifreleme yöntemlerinin prensipleri ve çalışma mekanizmaları
14	Feistel şeması