İçerik

Ders Kodu	Dersin Adı	Yarıyıl	Teori	Uygulama	Lab	Kredisi	AKTS
INF 524	Açık Anahtarlama ile Kriptografi	2	3	0	0	3	6

Ön Koşul	
Derse Kabul Koşulları	

Dersin Dili	İngilizce
Türü	Seçmeli
Dersin Düzeyi	Yüksek Lisans
Dersin Amacı	Bu ders modern şifreleme (asimetrik şifreleme yani açık anahtarlama ile şifreleme) tekniklerini, onların kriptoanalizini ve kullanımını anlatmaktadır. Derste ödevler yolu ile bu şifreleme tekniklerine ait bilgisayar programları yazılmakta ve ders kapsamındaki önemli makaleler incelenmektedir.
İçerik	1. Hafta: Sayı teorisine giriş. 2. Hafta: Bölünebilme özellikleri ve ilişkili teoremler. 3. Hafta: Sayı teorisine ait teoremler. 4. Hafta: Sayı teorisine ait teoremler. 5. Hafta: Sayı teorisine ait teoremler. 6. Hafta: Sayı teorisine ait teoremler. 7. Hafta: Diffie-Helman'ın makalesi (1976). 8. Hafta: RSA'nın makalesi (1978). 9. Hafta: RSA algoritmasına ait teoremler. 10. Hafta: RSA algoritmasının uygulanması. 11. Hafta: RSA algoritmasının uygulanması. 12. Hafta: Daha hızlı RSA algoritmaları üzerine makaleler. 13. Hafta: PGP (Pretty Good Privacy) 14. Hafta: Açık anahtarlı kriptografi üzerine uygulamalar (SSL).
Kaynaklar	1. Ders kapsamındaki orijinal makaleler. 2. Singh, S., "Kod Kitabı", Klan Yayınları, 2004.

Teori Konu Başlıkları

Hafta	Konu Başlıkları
1	Sayı teorisine giriş
2	Bölünebilme özellikleri ve ilişkili teoremler
3	Sayı teorisine ait teoremler I
4	Sayı teorisine ait teoremler II
5	Sayı teorisine ait teoremler III
6	Sayı teorisine ait teoremler IV
7	Diffie-Helman'ın makalesi (1976)
8	RSA'nın makalesi (1978)
9	RSA algoritmasına ait teoremler
10	RSA algoritmasının uygulanması I
11	RSA algoritmasının uygulanması II
12	Daha hızlı RSA algoritmaları üzerine makaleler
13	PGP (Pretty Good Privacy)
14	Açık anahtarlı kriptografi üzerine uygulamalar (SSL)