

İçerik

Ders Kodu	Dersin Adı	Yarıyıl	Teori	Uygulama	Lab	Kredisi	AKTS
INF 523	Kriptografi	1	3	0	0	3	6

Ön Koşul	
Derse Kabul Koşulları	

Dersin Dili	İngilizce
Türü	Seçmeli
Dersin Düzeyi	Yüksek Lisans
Dersin Amacı	Bu ders şifreleme tarihini, klasik şifreleme (simetrik şifreleme) tekniklerini, onların kriptanalizini ve kullanımını anlatmaktadır. Derste ödevler yolu ile bu şifreleme tekniklerine ait bilgisayar programları yazılmakta ve ayrıca şifrelenmiş metinlerin kırılması yapılmaya çalışılmaktadır.
İçerik	1. Hafta: Kriptolojinin kısa tarihi. 2. Hafta: Tek alfabeli yerine yerleştirme kriptolama algoritması ve kriptanalizi. 3. Hafta: 1. ÖDEV: Tek alfabeli yerine yerleştirme kriptolama algoritması ile şifrelenmiş bir metnin kırılması. 4. Hafta: Homofonik şifreleme ve kriptanalizi. 5. Hafta: Sezar'ın kutu şifresi. 6. Hafta: Sezar'ın kutu şifresinin iyileştirilmesi. 7. Hafta: 2. ÖDEV: Sezar'ın kutu şifresinin iyileştirilmiş biçimi ile şifrelenmiş bir metnin kırılması. 8. Vigenere şifresi, Vigenere şifresinin kriptanalizi ve kırılmaz şifre. 9. Hafta: Luigi Sacco'nun şifresi. 10. Hafta: 3. ÖDEV: Luigi Sacco'nun şifresi ile şifrelenmiş bir metnin kırılması. 11. Hafta: Bifid şifresi. 12. Hafta: 4. ÖDEV: Bifid şifresi ile şifrelenmiş bir metnin kırılması. 13. Hafta: ADFGVX şifresi. 14. Hafta: Playfair şifresi ve bu konuda verilen 5. ÖDEV.
Kaynaklar	1. Gaines, H. F., "Cryptanalysis: A Study of Ciphers and Their Solution", Dover Publications, 1989. 2. Singh, S., "Kod Kitabı", Klan Yayınları, 2004.

Teori Konu Başlıkları

Hafta	Konu Başlıkları
-------	-----------------