Ders adı: **Kriptografiye Giriş**

Dersi Veren: Murat Cenk, Ali Doğanaksoy, Fatih Sulak, Muhiddin Uğuz,

17.Haz.19	Temel Matematik	Modüler aritmetik, grup, halka, cisim, polinom, cisim genişlemeleri, sonlu cisimler	Muhiddin Uğuz
18.Haz.19	Kriptografiye giriş ve klasik sistemler	Güvenlik hedefleri, temel kavramlar, saldırı çeşitleri, kaydırma, afin ve Vigenere şifreleri	Ali Doğanaksoy
19.Haz.19	Klasik şifreleme sistemleri	Substitution, hill ve permütasyon şifreleme, klasik sistemlerin kırılması	Ali Doğanaksoy
20.Haz.19	Blok şifreler 1	SPN, FIESTEL, DES	Murat Cenk
21.Haz.19	Blok Şifreler 2	AES, işlem modları, Doğrusal ve diferansiyel kriptanaliz	Fatih Sulak
22.Haz.19	Özet Fonksiyonlar	Kriptografik özet fonksiyonlar, mesaj doğrulama kodları	Fatih Sulak
23.Haz.19	Akan Şifreler 1	LFSR, RC4, A5/1, Güvenlik analizleri, rassal sayılar	Ali Doğanaksoy
24.Haz.19	Açık anahtar kriptografi 1	Açık anahtar kriptografi kavramı, RSA, asallık testleri	Muhiddin Uğuz
25.Haz.19	Açık anahtar kriptografi 2	Ayrık logaritmalar, Diffie-Hellman anahtar değişimi, El-Gamal sistemler	Muhiddin Uğuz
26.Haz.19	Açık anahtar kriptografi 3	Eliptik eğri kriptografi, elektronik imza, dijital sertifika, kuantum sonrası kriptografi	Murat Cenk