SAKARYA ÜNİVERSİTESİ BİLGİSAYAR MÜHENSİLİĞİ 2018-2019 GÜZ YARIYILI KRİPTOLOJİYE GİRİŞ DERSİ ÖDEV DÖKÜMANI

ÖDEV İLE İLGİLİ AÇIKLAMALAR

- Ödev kapsamında seçilecek olan konu üzerinde bir araştırma yapılarak rapor hazırlanacaktır.
- Ödevler bireysel olarak yapılacaktır.
- Ödev teslimi Sabis'te açılacak olan ödev teslim modülü üzerinden yapılacaktır. Teslim tarihinden sonra sisteme yüklenen ödevler kabul edilmeyecektir.
- Ödev konusu hakkında araştırma yaparken farklı kaynaklardan araştırma yapılarak detaylı bir çalışma yapılması beklenmektedir.(ödev dokümanı en az 5 sayfa olmalıdır.)
- Ödevin hazırlanması sırasında kullanılan kaynaklar doküman sonunda referans olarak mutlaka belirtilmelidir.
- Konu ile ilgili bilgi verildikten sonra, gelişim süreci, kullanılan algoritmalar, yöntemler, kullanım alanları, güçlü zayıf yönleri, kullanılan yöntemlerin karşılaştırılması vb. gibi konuya göre içerik belirlenerek ödev hazırlanmalıdır. Ödev dökümanında konu ile ilgili görsel içerikler kod parçacıkları, ekran alıntıları kullanılabilir.
- Ödev konusunun belirlenmesi:
  Öğrenci numaranızın son iki hanesine aşağıdaki işlem uygulanacaktır. Elde edilen değer ödev konusunu belirleyecektir. Ödev konuları Tablo 1'de verilmiştir.

  b141210095 → 95 ≡ 15 (mod 40) 15 → Rasgele sayı üreteçleri

ÖDEV İÇERİĞİ:

- Ödev kapak sayfası (ad, soyadı, no, ödev konusu)
- İçindekiler bölümü
- Ana metin
- Kaynakça

Projenin sisteme yüklenmesi: Ödev dosyası tek bir pdf dosyası haline getirilecek ve dosya ismi öğrenci numarası olacak şekilde sisteme yüklenecektir. (b141210054.pdf)

Değerlendirme ile ilgili uyarı: İnternetten veya başka bir kaynaktan referans belirtilmeksizin alınan ve kopyala yapıştır ile hazırlandığı tespit edilen benzer ödevler 0 alacaktır.

Ödev son teslim tarihi: 30.11.2018 (23.59)

Tablo 1. Ödev Konuları

Sıra No	ÖDEV KONULARI	Sıra No	ÖDEV KONULARI
0	Enigma encryption	20	DDos attack
1	Operating System Security	21	Intrusion Detection Systems
2	Buffer overflow attack	22	Bluetooth Security
3	Sql Injection	23	Penetration Testing
4	Intrusion Prevention Systems	24	Differantial cryptanalysis
5	Rfid security	25	Classical Encryption Algorithms
6	Stenografi	26	Quantum Cryptology
7	IoT security	27	Block encryption
8	Lightweight Security	28	Asymmetric encryption
9	Digital watermarking	29	Digital Sign
10	Social engineering methods	30	Hashing
11	The history of encryption	31	Bitcoin
12	Cryptanalysis	32	Blockchain
13	Brute force attack	33	Intrusion Detection Systems
14	Software Security	34	Virtual Private Network
15	Random Number Generators	35	Mobil Gsm Security
16	Wireless network security	36	Face and fingerprint recognition system
17	Internet security	37	Biomedical System Security
18	Stream Cipher Algorithms	38	Firewall technologies
19	SSL/TLS protocol	39	Video coding techniques (h264-h265)