SAKARYA ÜNİVERSİTESİ BİLGİSAYAR MÜHENSİLİĞİ 2020-2021 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.
- 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.

  b171210095 → 95 ≡ 15 (mod 40) 15 → Rasgele sayı üreteçleri

ÖDEV İÇERİĞİ:

- Ödev kapak sayfası (ad, soyadı, no, ödev konusu)
- İçindekiler bölüm
- Ana metin (Konunun açıklanması)
  Gelişim süreci, kullanılan algoritmalar, yöntemler, kullanım alanları, güçlü zayıf yönleri, kullanılan yöntemlerin karşılaştırılması
- Kaynakça

Projenin sisteme yüklenmesi: Ödev dosyası bir pdf ve ppt sunum dosyası rar dosyası haline getirilerek, dosya ismi öğrenci numarası olacak şekilde tek bir dosya olarak sisteme yüklenecektir.

(b171210095.pdf / b171210095.pptx)-> b151210143.rar

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: 25.12.2020

Tablo 1. Ödev Konuları

Sıra No	ÖDEV KONULARI	Sıra No	ÖDEV KONULARI
0	DDos attack	20	Enigma encryption
1	Intrusion Detection Systems	21	PGP Kerberos
2	Bluetooth Security	22	Buffer overflow attack
3	Penetration Testing	23	Sql Injection
4	Differantial cryptanalysis	24	Intrusion Prevention Systems
5	Classical Encryption Algorithms	25	Rfid security
6	Quantum Cryptology	26	Stenografi
7	Block encryption	27	IoT security
8	Asymmetric encryption	28	Lightweight Security
9	Digital Sign	29	Digital watermarking
10	Hashing	30	Social engineering methods
11	Bitcoin	31	Key Exchange (IKE-IKEv2)
12	Blockchain	32	Cryptanalysis
13	Intrusion Detection Systems	33	Brute force attack
14	Virtual Private Network	34	Software Security
15	Mobil Gsm Security	35	Random Number Generators
16	Face and fingerprint recognition system	36	Wireless network security
17	IPSec protokol	37	Internet security
18	Firewall technologies	38	Stream Cipher Algorithms
19	Video coding techniques (h264-h265)	39	SSL/TLS protocol