BLM 323
BİLGİ GÜVENLİĞİ VE KRİPTOGRAFİ

Dr. Meltem KURT PEHLİVANOĞLU

Take Home 2

Take Home 2

- **GF(2^4) sonlu cismi altında kullanıcı tarafından girilen indirgenemez polinom ve haritalama değerine göre S-kutusunu oluşturan programı yazınız.**

Örnek Çıktı:

İndirgenemez polinomu giriniz: x4+x+1 (kullanıcı girecek)

Sonlu cismi oluşturan elemanlar listeleniyor…

(burada cismi oluşturan elemanların binary hex karşılıklarını hesaplayıp listeleyeceksiniz)

***α*^1= *α* (0010-2)**

***α*^2= *α*^2 (0100-4)**

***α*^3= *α*^3 (1000-8)**

***α*^4= *α*+1 (0011-3)**

…..

***α*^15= 1 (0001-1)**

Haritalamayı giriniz: x->x^-3 (kullanıcı girecek)

Giriş	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Çıkış	0	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..

Take Home 2

- Ödevin son teslim tarihi 25.11.2020 saat 17:00'dır, belirtilen tarih ve saatten sonra gönderilen ödevler kabul edilmemektedir.
- LaTeX formatında sizinle paylaştığım şablonu kullanarak oluşturduğunuz .pdf dökümanında programınızın nasıl kullanılacağını anlatmanız gerekmektedir.
- Kodu istediğiniz programlama dilinde yazabilirsiniz.
- Ödevinizi oluşturacağınız klasör içinde **kodlarınız** ve LaTeX'te yazıp oluşturduğunuz pdf dosyası olan **program kullanım dökümanınız** yer almalıdır. Daha sonra klasörü sıkıştırarak sisteme yükleyiniz.
- Ödevinizi sisteme yüklerken her grup tek bir dosya yüklemelidir. Dökümanı **grupno_ogretimno.pdf** (grup1_1ogretim.pdf veya grup5_2ogretim gibi) şeklinde adlandırmalısınız. Grup no https://docs.google.com/spreadsheets/d/1JKJeVGYUq3uprWJX3YR-sVtaKKPdpNC-6o5bh4dzAEQ/edit#gid=0 linkindeki excel dökümanında yer alan grup numarasıdır)
- Birbiriyle aynı olan ödevler tespit edilip, bu ödevler değerlendirmeye alınmayacaktır.