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

PROJE İLE İLGİLİ AÇIKLAMALAR

- Proje kapsamında seçilecek olan bir şifreleme algoritmasının kodlaması yapılarak, şifreleme ve şifre çözme işlemleri gerçekleştirilecektir.
- İki kişilik gruplar halinde projeyi yapabilirsiniz.
- Şifreleme işlemlerinde text, resim, ses vb. veriler kullanılabilir.
- Kodlama işleminde herhangi bir programlama dili tercih edilebilir.
- Ödev teslimi Sabis'te açılacak olan ödev teslim modülü üzerinden yapılacaktır. Teslim tarihinden sonra sisteme yüklenen ödevler kabul edilmeyecektir.
- Projede **şifrelenecek olan veri, kullanılacak anahtarlar** kullanıcıdan alınmalı, **şifreleme ve çözme işlemi sonucu elde edilen sonuçlar** geliştirilecek ara yüzde gösterilmelidir.
- Her bir şifreleme algoritmasından en iyi proje seçilecek, dönemin son haftasında sunumu gerçekleştirilecektir.
- Gruba ait şifreleme algoritmasının belirlenmesi:
  Öğrenci numaralarının son iki hanesine aşağıdaki işlem uygulanacaktır. Elde edilen değer grubun kullanacağı algoritmayı belirleyecektir. Tablo 1'de kullanılacak olan şifreleme algoritmaları verilmiştir.

  b141210095 - b141210024 → 95+24=119 ≡ 15 (mod 26) 15 → Klein Algoritması

ÖDEV İÇERİĞİ:

- Proje kaynak kod dosyaları
- Proje açıklama dosyası (readme)
- Program çalıştırılabilir dosyası (*.exe)
- Proje ödev dökümanı (içeriği aşağıdaki gibi düzenlenecektir.)
  * Kapak sayfası
  * Kullanılan şifreleme algoritmasına ait bilgilendirme dökümanı (kodları buraya yapıştırmayın)
  *Uygulamanın örnek çalıştırma ekran çıktıları

Projenin sisteme yüklenmesi: Ödev içeriğinde yer alan tüm dokümanları tek bir klasöre (klasörün ismi öğrenci numaranız olmalı) kopyalayarak, sıkıştırdıktan sonra tek bir parça halinde yüklemeniz gerekmektedir. (b141210095-b141210024.zip)

Değerlendirme ile ilgili uyarılar: Bu ödevin amacı, en azından bir şifreleme algoritmasının kodlama ve uygulamasının gerçekleştirilmesini sağlamaktır. Bu sebeple internet üzerinden bulacağınız hazır kodlar veya arkadaşlarınızın kodlarını projenizde kullanmamalısınız. Yapılan kontrollerde böyle bir durumun tespiti halinde proje değerlendirmesinin sonucu sizi hiç mutlu etmeyecektir.

Proje son teslim tarihi:14.12.2018 (23.59)

PROJEDE KULLANILABİLECEK ŞİFRELEME ALGORİTMALARI:

Tablo 1. Şifreleme Algoritmaları

Sıra No	Şifreleme Algoritmaları	Sıra No	Şifreleme Algoritmaları
0	PRESENT	13	TEA
1	RSA	14	RC5
2	BLOWFISH	15	KLEIN
3	AES	16	DIFFIE HELMAN
4	SHA-1	17	3DES
5	DES	18	L-BLOCK
6	KATAN	19	RC6
7	IDEA	20	RABBIT
8	TWOFISH	21	XTEA
9	TWINE	22	SKIPJACK
10	SEA	23	MD5
11	RC4	24	HIGHT
12	ECC(Eliptic Curve)	25	SHA-2