2015-2016 Kriptoloji Final Sınavı Soruları

---
*----->Döküman Formatı
*Öğrenci No / Ad Soyad
*Konu başlığı
*Soru
*Cevap
*Çizgi Ayracı
*<-----
"Yapılan değişiklikler loglanıyor trolleme girişiminde bulunmayın
"Herkes Sorularını yeni bir sayfada yazsın.
"yazı tipi arial punto 12

(11-Euler Fonksiyonu)
Soru (1)
Tanım: ϕ(n) say›s›, 0 < d ≤ n ve EBOB(d, n) = 1 özelli¤ini sağlayan d'lerin sayısıdır.

Yukarıdaki tanım hangi şıkka aittir?
A)Fermat Teoremi B)Eluer-Fermat Teoremi C)Euler Fonksiyonu D)f Fonksiyonu E)DES Algoritması

Soru(2)

3^ϕ(8)mod8 nedir?
A)0 B)1 C)2 D)3 E)4

1306110066-Agit ELGÜN
Quadratic Residue

1. Z5 'nin quadratic residueleri aşağıdakilerden hangisinde tam olarak verilmiştir?

a-)(1,4)
b-)(2,4)
c-)(3,5)
d-)(0,2)
e-)(2,3)

CEVAP:A

2)p:tek asal sayı; a: tam sayı olmak üzere
I. 0, if a≡ 0 mod p
II. 1, if a is Quadratic residue of mod p
III. 2, if a is Quadratic non-residue of mod p
Legendre Sembol(ap) için yukardıkilerden hangisi doğrudur?
a-) Yalnız II b-) Yalnız III c-) I ve III d-) I ve II e-) I,II,III

CEVAP:D

3)Aşağıdakilerden hangis Z7 'nin Quadratic Residue değerlerinin kümesidir ?
A-) {3,5,6}
B-) {1,2,4}
C-) {2,3,4}
D-) {1,2,5}
E-) {2,3,5}

CEVAP:B

1306110057 SELEN ALTINSOY
3-DES

soru 1
Aşağıdakilerden hangisi 3-des algoritması için yanlıştır?

A)des algoritmasının 2 anahtar kullanılarak 3 kez uygulanmasıdır
B)çift yönlü çalışır,şifrelenmiş veri geri çözülebilir
C)des e göre 3 kat hızlıdır
D)bilgisayarın donanımsal açıklarını kapatır
E)Güvenlik tamamen kullanılan anahtara dayanmaktadır. Anahtarın zayıflığı, şifrenin çözülmesini kolaylaştırır.

cevap C

soru 2

3 des algoritmasında kullanılan anahtar kaç bittir
a)64
b)128
c)168

d)180
e)56

cevap C

soru 3
..... algoritmasında iki adet anahtardan birisi kullanılarak metin des e göre şifrelenir.ikinci anahtar ile şifrelenmiş metin üzerine des in çözme algoritması
uygulanır.İki kez karıştırılmış mesaj son olarak ilk anahtar kullanılarak tekrar şifrelenir.
boşluğa aşagıdakilerden hangisi gelmelidir?

a)3 des
b)aes
c)affline cipher
d)hill cipher
e)vignere cipher
cevap A

1306110052- Umut Coşkun
DES

1) Aşağıdakilerden hangisi DES işlem kiplerinden biri değildir?
a) Elektronik kod kipi (ECB)
b) Şifre geri besleme kipi (CFB)
c) Şifre Öbek Zincirleme kipi (CBC)
d) Giriş geri besleme kipi (İFB)
e) Çıkış geri besleme kipi (OFB)
CEVAP : D
2) DES algoritmasında 100111 olarak gelen 6 bit SBOX ta kaçıncı satır ve kaçıncı sütuna denk gelmektedir?
a) 3. Satır 3. Sütun
b) 2. Satır 6. sütun
c) 1. Satır 8. sütun
d) 0. Satır 0. sütun
e) 0. Satır 15. Sütun
CEVAP: A
3) DES algoritmasında 1 den 16 ya kadar dönen döngüde R' lerin elde edilmesi için kullanılan formül aşağıdakilerden hangisidir
a) $R_i = L_{i-1}$
b) $R_i = L_{i-1} \oplus f(K_i)$
c) $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
d) $R_i = R_{i-1}$
e) $R_i = R_{i-2}$
CEVAP: C

1306110012-Eyyüp Yıldız
Euler-Fermat teoremi

1) 3^{4} (mod10) =?
A-) 1 B-) 2 C-) 3 D-) 4 E-) 5
CEVAP - C
2) 28^{4} (mod25) =?
A-) 1 B-) 2 C-) 3 D-) 4 E-) 5
CEVAP - C
3) 17^{6} (mod14) =?
A-) 1 B-) 2 C-) 3 D-) 4 E-) 5
CEVAP - C

1306110036 / Hamit Doğan
(18 - Vigenere Cipher)

Sorular 1

"istanbul" kelimesinin "dogan" anahtar kelimesine göre şifrelenmış hali aşağıdakilerden hangisidir?

A) mhabbfjs
B) mıbbcfks

C) imnsgtya
D) mhacftys
E) asfryhjb

Sorular 2

Şifrelenmis hali "vvkpieui" olan kelimenin "anahtar" anahtar kelimesine göre çözülmüş hali aşağıdakilerden hangisidir?

A) vikipedia
B) vikipedi
C) tarayıcı
D) tartışma
E) Veresiye

Sorular 3

"mesaj" kelimesinin, "ali" anahtar kelimesine göre şifrelenmiş hali aşağıdakilerden hangisidir?

A) macfs
B) bcfks
C) sgtya
D) nqbbw
E) sryhb

1306100103 / Mustafa TUZLU
(7 - Çinli Kalanlar Genel)

1. Soru: Aşağıdaki kuralları sağlayan teorem hangisidir?

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

Tüm Çözümler x Bu sistem uyumlu olan modul $N = n_1 n_2 \ldots n_k$ Böylece

$$x \equiv y \pmod{n_i}_{\text{tüm}} 1 \leq i \leq k$$ ancak ve ancak
$$x \equiv y \pmod{N}$$

a) **Çinli Kalanlar**
b) Euler
c) AutoKey Chiper
d) Cebirin Temel Teoremi
e) MD5 Hashing
CEVAP: A

---

2. Soru: RSA tarafından anahtar üretimi ve decyrpt işlemlerinde kullanılan, pollig hellman algoritmasının geliştirilmiş teoremi aşağıdakilerden hangisidir?

a) SHA-2
b) Fermat Teoremi
c) AutoKey Chiper
d) **Çinli Kalanlar**
e) RSAHashing
CEVAP: D

1306110074-İlknur ÖZGEN
Solovay Strassen Algoritması

1)Solovay-Strassen algoritması niçin kullanılır?
a)Üs almak için
b)Verilen metni şifrelemek için
c)$\alpha^{x}=\beta(\text{mod}p)$ denklemindeki x'i bulmak için
d)bir sayının asallığını test etmek için
e)bir sayının quadratic residue olup olmadığını belirlemek için
Cevap:d

$x \leftarrow \left(\frac{a}{n}\right)$
if $x = 0$ **then**
return n is composite
end if
$y \leftarrow a^{\frac{n-1}{2}} \pmod{n}$
if $x \equiv y \pmod{n}$ **then**
return n is prime
else
return n is composite
end if

2)Yukarıda verilen algoritma aşağıdakilerden hangisine aittir?
a)Shanks Algoritması
b)Miller Rabin
c)Solovay Strassen
d)Diffie Helman Anahtar Değişim Protokolü
e)Pohlig-Hellman Algoritması

Cevap:c
3)Asallığı test edilecek sayı **n** olsun.1≤a≤(n-1) olduğunu varsayalım.Buna göre Solovay-Strassen algoritması hangi sıralamaya göre çalışır?
i) if(x≠y(mod n))) then return("n is composite")
ii)if(x=0) then return("n is composite")
iii)x'in hesaplanması
iv)if(x≠0) y sayısının hesaplanması
v)if(x≡y(mod n)) then return("n is prime")

a)i-iv-v-ii-iii **b)iii-ii-iv-v-i** c)ii-iii-v-i-iv d)iv-i-v-iii-ii e)v-iii-i-iv-i

cevap:b
1306110078/Özlem DEMİRCİ
Index Calculus Yöntemi

1) Index Calculus yönteminde input=p,α,β ise output nedir?
A. α^{β}(modp)
B. $\log_{\alpha}\beta$(modp)
C. αβ(modp)
D. β^{α}(modp)
E. (β/α)(modp)
2) Index Calculus yönteminde p=61 veriliyor. Buna göre S kümesi aşağıdakilerden hangisi olabilir?

A. (1,3,5,7,9,11)
B. (2,5,8,11,14,17)
C. (11,23,37,41,53)
D. (13,29,47,53,61,)
E. (7,17,21,39,41,59)

3) α=6 , p=229 , β=13 olarak veriliyor. Index Calculus yötemi ile çözünüz.
A. 117
B. 123
C. 137
D 148
E 161

1306110062 Hazal KÖKSAL

AES

1. AES için aşağıdakilerden hangisi yanlıştır?
A. 128 bit input, 128 bit output vardır
B. Algoritma 10 döngüden meydana gelir.
C. Her döngüde kullanılan basamaklar vardır.
D. 64 bit K anahtarı kullanılır.
E. Simetrik şifreleme algoritmasıdır.

Cevap: D

2) 10001011 değeri SBOX ' ta yerini alırken hangi satır ve sütuna göre göre yerleşir?
A. 8. Satır 11. Sütun
B. 6. Satır 8.Sütun
C. 11. Sütun 8. Satır
D. 5. Satır 7. Sütun
E. 1. Satır 1. Sütun

Cevap: A

3) AES şifreleme algoritmalarında son döngüde aşağıdakilerden hangisi kullanılmaz?
A. Byte Sub Dönüşümü

B. Shift Row Dönüşümü
C. **Mix Column Dönüşümü**
D. Add Round Key
E. SBOX
Cevap: C

1306120121/HAKAN TAVACIOĞLU

28-QUADRATIC RESIDUE

SORU 1

TANIM:p asal,tek, a∈Z olmak üzere eğer a≠0(mod p) , ⟦ y⟧ ^2≡a(mod p) ve y∈z_p ise bunu sağlayan tüm a'lar .....dır.

Tanıma göre boşluğa gelmesi gereken ifade nedir?
A)Ayrık Logaritma Problemi B) 3-DES C) DES **D) Quadratic Residue** E) RSA
CEVAP D

SORU 2
z_13 'de aşağıdakilerden hangisi quadratic residue'dur?

A)11 B)8 **C)12** D)7 E)6
CEVAP C

SORU 3
z_17'de aşağıdakilerden hangisi quadratic residue değildir?

A)9 B)13 **C)14** D)15 E)16
CEVAP C