

1-) Doğrusal denklem çözümüne göre aşağıdakilerden hangisi doğrudur ?

$$4X = 6 \pmod{13}, X = ?$$

- a) 5 b) 1 c) 4 **d) 6** e) 2

2-) $\gcd(148, 66) = ?$

- a) 4** **b) 1** **c) 3** **d) 2** **e) 0**

3-) Aşağıda verilenlere göre “cadegafe” nin Substitution Cipher ile şifrelenmiş hali nedir?

Alfabe : a b c d e f g h

Anahtar : c d e a g h b f

- a) ecagcbgh
- b) fdacgfch
- c) feadgfhc
- d) ffeaghdc
- e) ecagbchg**

4-) Substitution Cipher ile ilgili aşağıdakilerden hangisi yanlıştır?

- a) Frekans saldırısına (frequency attack) karşı zayıf bir şifrelemedir.
b) Amaç bir alfabede bulunan karakterlerin her birisinin yerine aynı alfabeden farklı bir karakter koyarak şifreleme yapmaktır.
c) Asimetrik şifreleme algoritmasıdır.
d) Bu şifreleme yönteminde mümkün olan toplam permütasyonların sayısı $= 26! = 4 \times 10^{26}$
e) Saniyede 3 milyar permütasyon deneyebilen 3 GHz hızı sahip bir PC 4263 yılda şifreyi çözer.

5-) Aşağıdakilerden hangisi Diffie Helman anahtar değişim protokolünde Alice'in seçebileceği a değeri aralığıdır?

- a) $0 < a < p+1$
b) $0 \leq a \leq p-2$
c) $0 < a < p$
d) $0 \leq a \leq p-1$
e) $0 < a < p+2$

6-) Alice hususi anahtarı olarak $a=6$, seçiyor. Bob da hususi anahtarı olarak $b=15$ 'i seçiyor. Diffie Helman anahtar değişim protokolünde $p=23$ ve $g=5$ ise ortak anahtar nedir?

- a) 6 b) 8 c) 3 d) 2 e) 5**

7-) Take a at random in $\{1, 2, \dots, n-1\}$
 if $\gcd(a, n) \neq 1$ then
 return("composite")
 else if $(a/n) \neq a^{(n-1)/2} \pmod n$ then
 return("composite")
 else
 return("prime") end if end if

Yukarıda verilen algoritma aşağıdakilerden hangisine aittir ?

- a) Vestane Algoritması
- b) Diffie Helman Anahtar Değişim Protokolü
- c) Miller Rabin
- d) Solovay Strassen**
- e) Substitution Permutation

8-) Asallığı test edilecek sayı n olsun. $1 \leq a \leq (n-1)$ olduğunu varsayalım. Buna göre Solovay-Strassen algoritması hangi sıralamaya göre çalışır?

- I. if $(x \neq y \pmod n)$ then return ("n is composite")
- II. if $(x=0)$ then return ("n is composite")
- III. x'in hesaplanması (a/n)
- IV. if $(x \neq 0)$ y then y sayısının hesaplanması
- V. if $(x=y \pmod n)$ then return ("n is prime")

- a) III-IV-V-II-I
- b) IV-I-II-III-V
- c) IV-III-I-II-V
- d) III-II-IV-V-I**
- e) V-I-III-II-IV

9-) $19^{280} = x \pmod{281}$ ise x = ?

- a) 19
- b) 156
- c) 0
- d) 1**
- e) 280

10-) Aşağıdaki tabloda $19^{280} \pmod{281}$ işleminin hızlı modüler üs alma tablosu verilmiştir. ? (soru işareti) ile belirtilen yere ne gelmelidir?

<i>i</i>	<i>9</i>	<i>8</i>	<i>7</i>	<i>6</i>	<i>5</i>	<i>4</i>	<i>3</i>	<i>2</i>	<i>1</i>	<i>0</i>
<i>b_i</i>	0	1	0	0	0	1	1	0	0	0
<i>c</i>	0	1	2	4	8	17	35	70	140	280
<i>d</i>	?

- a) 19
- b) 7
- c) 1**
- d) 280
- e) 279

11-) Fermat Teoremine göre 40 266 sayısının mod(289) daki değeri kaçtır?

- a) 87(mod)89 b) 83(mod)89 c) 91(mod)89 d) 97(mod)89 e) 99(mod)89

12-) Fermatın son teoremini kanıtlayan matematikçi kimdir?

a) Andrew Wiles

b) Bolzano

c) John Forbes Nash

d) Rene Baire

e) Alan Turing

13-) "mesaj" kelimesinin, "ali" anahtar kelimesine göre vigenere cipher yöntemiyle şifrelenmiş hali aşağıdakilerden hangisidir?

a) nqbbw

b) ocfs

c) sgtya

d) zacfs

e) sryhb

14-) İstanbul" kelimesinin "doğan" anahtar kelimesine göre vigenere cipher yöntemiyle şifrelenmiş hali aşağıdakilerden hangisidir?

a)mhabbfjs

b) zibbcfs

c) nmnsqtya

d) mzacftys

e) asfryhjb

15-) Synchronous stream cipher ile ilgili aşağıdaki bilgilerden hangisi yanlıştır?

a) Pratikte kullanılan en yaygın stream cipher türüdür.

b) Alıcı ve gönderici senkronize olmak zorundadır.

c) Keystream,plaintext'e bağlı olarak oluşturulur.

d) Şifreleme ve deşifreleme aynı şekilde yapılır.

e) Şifrelerken genellikle plaintext ile keystream xor işlemine sokulması yöntemi kullanılır.

16-) Aşağıdakilerden hangisi stream ciphers ile ilgili yanlış bir bilgidir?

- a) Self-synchronizing stream cipherda keystream,plaintext'e bağlıdır.
- b) Synchronous stream cipherda keystream,ciphertext'e bağlı değildir.
- c) Self-synchronizing stream cipher için güvenlik özelliklerini garanti etmek zordur.
- d) Synchronous stream cipher aktif saldırılara karşı savunmasızdır.
- e) Block cipher'a göre genellikle daha yavaş ve daha yüksek donanım karmaşıklığına sahiptir.

17-) 3DES için aşağıdakilerden hangisi yanlış bir özelliktir?

- a) Kullanılan anahtar uzunluğu 56 bittir.
- b) DES şifrelemesinin 3 kez art arda çalıştırılmasıyla elde edilmiştir.
- c) DES şifreleme yöntemine göre 3 kat daha yavaş çalışır.
- d) Şifrelenmiş veri bir anahtar yardımıyla tekrar çözülebildiği için çift yönlü çalışır.
- e) Çift yönlü çalıştığı için şifreli bir şekilde veriler saklanabilir, istenildiği zaman geri çağırılarak şifresi çözülebilir.

18-)

I. Veri, 3DES anahtarının ilk 8 baytı ile şifrelenir. Sonra veri, anahtarın ortadaki 8 baytı ile çözülür. Son olarak anahtarın son 8 baytı ile şifrelenerek 8 bayt bir blok elde edilir.

II. Daha gelişmiş bir algoritmaya sahip olan AES(Advanced Encryption Standart-Gelişmiş şifreleme standardı) şifreleme yöntemine göre 3 kat daha yavaş çalışır.

III.3DES Bankacılık Sistemi,Elektronik Ödeme Sistemi gibi alanlarda kullanılır.

Yukarıda belirtilen özelliklerden hangileri doğrudur?

- a) Yalnız I
- b) Yalnız II
- c) I ve III
- d) II ve III
- e) I , II ve III

19-) Index-Calculus yönteminde $p=61$ veriliyor. Buna göre S kümesi aşağıdakilerden hangisi olabilir?

- a) (11,23,37,41,53)
- b) (14,17,29,47,53)
- c) (12,3,5,7,9,11)
- d) (13,29,47,53,61,)
- e) (13,17,21,39,41,59)

20-) Index-Calculus yöntemi tipindeki problemlerin çözümünde ilk olarak hangi adım izlenir?

- a) S kümesindeki elemanların logaritmalarını içeren lineer ilişkiler bir araya getirilir.
- b) S kümesi elemanlarının logaritmaları seçilir.
- c) Verilen ilk denklemler t/c şeklinde logaritma düzenine ulaştırılır
- d) Verilen ilk denklemler t+c şeklinde logaritma düzenine ulaştırılır
- e) Katsayı tabanı seçilir

21-) $1 \leq a \leq n-1$

$X \leftarrow (a/n)$

IF $X=0$

Then return ("n is(1)....")

$Y \leftarrow a^{(n-1)/2} \bmod n$

IF $X \equiv Y \pmod{n}$

Then return ("n is(2)....")

Else return ("n is(3)....")

Yukarıda verilen Solovay-Strassen algoritmasında sırasıyla (1),(2),(3) yerine aşağıdakilerden hangisi gelmelidir?

- a) prime-composite-prime
- b) composite-composite-prime
- c) prime-prime-composite
- d) composite-composite-composite
- e) composite-prime-composite

22-) Solovay-Strassen algoritmasının karmaşıklığı aşağıdakilerden hangisidir?

a) $O((\log n)^2)$

b) $O(n^4)$

c) $O((\log n)^3)$

d) $O(n^3)$

e) $O(n^5)$

23-) Miller Rabin testi uygulanan 8911 sayısının değer aralığı nedir? (a=2 alınız.)

- a) 8285-8289
- b) 6363-6365
- c) 7878-7879
- d) 9991-9997
- e) 9090-9094

24-) Aşağıdaki testlerden hangisi sayıların asal (prime) olup olmadıklarını test eder?

- a) Miller&Rabin
- b) Pohlig-Hellman
- c) Pollard
- d) Tonelli-Shanks
- e) Schönhage-Strasse

25-) Miller&Rabin testi için aşağıdakilerden hangisi yanlıştır?

a)Olası asalılık testidir.

b)Güçlü asalılık testi olarak bilinir.

c)Bu test en iyi şartlarda bile en az diğer testler kadar çalışma zamanına ihtiyaç duyar.

d)Bu test sonrasında başka testler kullanılarak bileşik testler yapılabilir.

e)Solovay&Strassen testine göre gerçeğe daha yakın sonuçlar sunar.

26-) Aşağıdakilerden hangisi 100 den küçük ve eşit tabanlar kullanıldığında Miller&Rabin testini geçen 55 basamaklı bir sayı bulmuştur?

a)Higgins

b)Pomerance

c)Jaeschke

d)Maurier

e)Bleichenbacher

27-) Verilen $x^4 + x^2 + x + 3$ fonksiyonunun eleman sayısı kaçtır?

a) 24

b)16

c) 17

d) 9

e) 26

28-) I. $x^2 + 2x + 1$

II. $x^3 + x^2 + x + 1$

III. $2x^3 - 4$

IV. $x^2 - 6x + 8$

Yukarıdaki fonksiyonlardan hangileri reducible'dır?

a) I ve II

b) I , III ve IV

c) I , II ve IV

d) Yalnız IV

e) II , III ve IV

29-)Hill cipher için aşağıdakilerden hangisi doğrudur?

a)Basitçe şifrenlemek istenen metindeki her karakterin anahtara kadar kaydırılması ileşifrelenir.

b)Bir akış şifrelemesidir

c)Bir blok şifrelemesidir.(Block cipher)

d)DES'in temelini oluşturan algoritmadır

e)Plain Text farklı uzunluklara bölünebilir

30-) Hill cipher için hangisi yada hangileri yanlıştır?

I. Frekans saldırısı tekniğine karşı oldukça zayıftır.

II. Kullanılan alfabedeki harf genişliği bilinmiyorsa saldıran kişi plaintexte sahip olsa bile saldırısı başarısız olur.

III. Klasik şifreleme yöntemidir.

a) Yalnız II

b) Yalnız I

c) Hiçbiri

d) Yalnız III

e) I ve II

31-) Shift cipher yöntemine ait verilenlerden hangisi doğrudur?

a) Şifrelenmiş mesaj, gönderen-alıcı arasındaki başkaları tarafından ele geçirilse bile private key bilinmediği için plain text'e ulaşılamaz

b) Cipher texti ele geçiren bir kişi, alfabedeki harf sayısının bir eksiği kadar shift ederse mutlaka plain texte ulaşır.

c) Bir shift cipher çeşidi olarak sayılabilen quadratic cipher yönteminin en büyük avantajı, verilen quadratic polinom'un alabileceği herhangi bir değerin alfabedeki harf sayısındaki modunda tersinin olup olmadığını bulmanın zor olmasıdır.

d) Harflerin ilgili alfabedeki frekanslarına göre kırılma ihtimali az da olsa vardır ancak brute force ile kırılması mümkün değildir.

e) Kayıtlı tarihte ilk defa Julius Caesar'ın yeğeni Augustus tarafından savaş alanındaki generalleriyle haberleşmek amacıyla kullanıldığından bir adı da Augustus Şifresi olarak bilinir.

32-) Shift cipher yöntemiyle şifrelenmek istenen bir plain text, $f(x) = (3x + 4) \bmod 26$ fonksiyonu kullanılarak şifrelenecek ise hangi shift cipher yönteminin kullanıldığını kesinlikle söyleriz?

a) Linear Cipher

b) Vigenere Cipher

c) Polynomial Cipher

d) Substitution Cipher

e) El Gamal

33-)

1. $c \leftarrow 0$
2. $d \leftarrow 1$
3. $b_k b_{k-1} b_{k-2} \dots b_2 b_1 b_0$ (b 'nin binary hali)
4. i k 'dan 0'a kadar
5. ...
6. $d \leftarrow d.d(\bmod n)$
7. if $b_i = 1$
8. ...
9. $d \leftarrow d.a(\bmod n)$
10. sonuç $\leftarrow d$

$a^b(\bmod n)$ değerini hesaplayan Hızlı Modüler Üs Alma Algoritmasının adımları yukarıda verilmiştir. Buna göre sırasıyla 5. ve 8. satıra gelmesi gereken ifadeler hangileridir?

a) $c \leftarrow 2d$, $c \leftarrow d.c$

b) $c \leftarrow 2c$, $d \leftarrow d+1$

c) $c \leftarrow 2c$, $c \leftarrow c+1$

- d) $c \leftarrow 2d$, $c \leftarrow c-1$
e) $c \leftarrow c+1$, $c \leftarrow 1$

34-) $7^{256} \pmod{13}$ değeri Hızlı Modüler Üs Alma Algoritması ile hesaplanırken, üçüncü iterasyon sonunda d'nin değeri ne olur?

- a) 9 b) 8 c) 7 d) 10 e) 11

35-)

- I. ByteSub Dönüşümü
- II. ShiftRow Dönüşümü
- III. MixColumn Dönüşümü
- IV. AddRoundKey Dönüşümü

AES algoritmasında şifreleme işlemi yapılırken son döngüde bulunan basamak/basamaklar hangileridir?

- a) Yalnız III b) II, III, IV c) I, III, IV d) I, II, IV e) Yalnız IV

36-) AES algoritmasında ByteSub dönüşümünde Durum Matrisi'ndeki elemanın değeri 10011010 ise SBOX'taki hangi satır ve sütundaki değer alınmalıdır?

- a) 10. satır, 9. Sütun
b) 9. satır, 10. sütun
c) 11. satır, 10. sütun
d) 10. satır, 11. sütun
e) 10. satır, 8. sütun

37-) Başlangıç anahtarı (priming key) "B" ve düz metni "DEFTER" olan şifreleme isteğinin sonucu autokey chipher yöntemine göre aşağıdakilerden hangisidir?

- a) BHJYKV
b) EHJYXV
c) HEJYXV
d) HEJXYV
e) JEHXVY

38-) Başlangıç anahtarı (priming key) "Mavi" ve düz metni "YemekYiyelimMi" olan şifreleme isteğinin sonucu autokey chipher yöntemine göre aşağıdakilerden hangisidir?

- a) CIQMWIUCOJQKQT
b) MIQCWIUCOTQKQJ

c) IWMQICUCOJQKQT

d) IWMQICUTQKQJOC

e) WIMQICUTQKQJOC

39-) Pohling-Hellman a göre x kaçtır F_{11251} de $23^x = 9689$ ise $x = ?$

a) 500

b) 511

c) 321

d) 300

e) 221

40-) $G = E(F_{599}) : y^2 = x^3 + 1$, $P = (60, 19)$, $Q = (277, 239)$, $N = 605$ olduğna göre $Q = kP$ için k nedir

a) 205

b) 165

c) 406

d) 266

e) 327

41-) Diffie – Helman Anahtar değişim protokolünde $p=17$ ve $\alpha=5$ ise Alice ve Bob' un seçtikleri sayı ikilisi aşağıdakilerden hangisi olamaz ?

a) {16,8}

b) {6,4}

c) {12,6}

d) {7,14}

e) {9,10}

42-) Diffie – Helman Anahtar değişim protokolünde $p=17$ ve $\alpha=3$ ise Alice 15' i seçiyor Bob ise 13' ü. Buna göre aralarındaki ortak anahtar aşağıdakilerden hangisidir?

a) 10

b) 8

c) 7

d) 5

e) 6

43-) Hangisi 3-des algoritması için yanlıştır?

a) Çift yönlü çalışır, şifrelenmiş veri geri çözülebilir

b) Dese göre 3 kat hızlıdır.

c) Des algoritmasının 2 anahtar kullanılarak 3 kez uygulanmasıdır

d) Bilgisayarın donanımsal açıklarını kapatır

e) Anahtarın zayıflığı, şifrenin çözülmesini kolaylaştırır. Güvenlik tamamen kullanılan anahtara dayanmaktadır.

44-) DES algoritmasında kullanılan anahtar kaç bit uzunluğundadır?

a) 8-Bit

b) 16-Bit

c) 32-Bit

d) 56-Bit

e) 48-Bit

45-) $3^x = 19 \pmod{59}$ x değeri kaçtır?

- a) 6 **b) 17** c) 9 d) 15 e) 18

46-) $455x = 204 \pmod{469}$ denklem çözümünü bulunuz?

- a) 7 b) 29 c) 33 d) 11 **e) çözüm yoktur**

47-) Simetrik şifreleme yöntemleriyle ilgili verilen bilgilerden hangisi yanlıştır?

a) Vigenere Cipher

b) DES

c) AES

d) Elliptic Curve

e) Permutation Cipher

48-) Elliptic Curve kriptografide 'O' ne alama gelir?

a) Koordinat sisteminde eğri içinde kalan bölgeden rasgele seçilmiş bir nokta

b) Etkisiz eleman

c) Zamanın milisaniye cinsinden değeri

d) Kriptografide $(a + b)$ 'nin türevi

e) $y_1 = -y_2$ ve $x_1 = x_2$ olduğu nokta

49-) Elliptic Curve kriptografide $A(x_1, y_1)$ ve $B(x_2, y_2)$ noktaları verilmiş olsun. Bu durumda λ (eğim) aşağıdakilerden hangisiyle hesaplanır?

a) $\lambda = \frac{(y_2 - y_1)}{(x_2 - x_1)}$

b) $\lambda = (x_2)^3 + y_2 * (x_1) + y_1$

c) $\lambda = (x_1)^3 + y_1 * (x_2) + y_2$

d) $\lambda = \frac{3*(x_1)^2 + x_2}{2*(y_1)}$

e) $\lambda = \frac{(y_1 - y_2)}{(x_2 - x_1)}$

50-) Şıklarda verilen özelliklerden hangisi Elliptic Curve yöntemi için kullanılacak eğri için doğrudur?

a) Zamandan bağımsız

b) Zamana bağlı

c) Herhangi bir özelliği olması gerekmez

d) Non-Singular

e) Singular

51-) $6x = 2 \pmod{11}$, x kaçtır?

a)15

b)14

c)13

d)16

e)17

52-)Açık şifreleme işlemsel olarak kolay, şifre çözme ise işlemsel olarak zor olmalıdır şeklinde tanımlanan veri koruma özelliklerinden hangisine aittir?

a)Kapalı Anahtar Şifreleme

b)Açık Anahtar Şifreleme

c)Kriptolama

d)Güvenlik

e)Hiçbiri

53-)Hangi seçenekte aşağıdaki yerine koyma tablosuna göre (dilimizde 8 karakter olduğunu düşünelim.) şifrelenecek “fabecdhg” mesajı doğru olarak bulunmuştur?

a b c d e f g h
f d e a c h g b

a) hdfceabg

b) bdfceahg

c) bdacefhg

d) hfdcdabg

e) hfdceabg

54-)Aşağıda verilmiş yerine koyma tablosuna göre, bilinen şifreli metin “cdefgahd” ise bulunması istenen mesaj şıklardan hangisidir?

a b c d e f g h
h g f a c e d b

a) egfcbdah

b) hgfcbae

c) fgecbdah

d) fgebcdah

e) ehfcbdag

55-)Sırasıyla SHA-1 ve MD5 algoritmaları kaç bitlik özetler oluşturur?

- a) 256 , 128
- b) 512 , 256
- c) 128 , 512
- d) 512 , 160
- e) 160 , 128

56-)Kullanıcı adı ve parola ile giriş yapılan bir sistemde Hash fonksiyon kullanılıp kullanılmadığını nasıl anlarız?

- a) Kayıt için en az 8 karakterlik şifre isteniyorsa
- b) E-mailinize doğrulama kodu gönderiliyorsa
- c) Şifrenin harften ve sayıdan oluşması isteniyorsa
- d) Kullanıcı şifresini unuttuğu taktirde sistem eski şifreyi veremeyip, şifre sıfırlama ekranına yönlendiriyorsa
- e) Girişte güvenlik sorusu isteniyorsa

57-)Aşağıdaki kavramlardan hangisi "verinin üzerinde izinsiz olarak oynama yapılmasını engeller." tanımının karşılığıdır?

- a)Reddetme
- b)İnkâr edilemezlik
- c)Doğrulama
- d)Kimlik doğrulama
- e)Bilgi bütünlüğü

58-)Sıralanmış şekilde verilmiş aşamalardan hangisi digital imza algoritmasına uygundur?

- a)Anahtar oluşturma-Doğrulama-İmzalama
- b)İmzalama-Anahtar oluşturma-Doğrulama
- c)Doğrulama-İmzalama-Anahtar oluşturma
- d)Anahtar oluşturma-İmzalama-Doğrulama
- e)İmzalama-Doğrulama-Anahtar oluşturma

59-) Hangisi El Gamal yönteminde şifrenin çözülme zorluğu neye dayanır?

- a)Asal Çarpanlara ayırılma zorluğuna
- b)Anahtar'ın güvenli bir kanal üzerinden iletilmesi
- c)Asal çarpanların büyüklüğüne
- d) Anahtar 'ın uzunluğuna
- e)Discrete Logaritma Probleminin Çözülme Zorluğuna

60-)El Gamal şifreleme yöntemi aşağıdakilerden hangisi yada hangilerini kullanır?

I-Public Key Cryp.

II-Private Key Cryp.

III-Permutation Chipher

a)Yalnız I

b)Yalnız II

c)Yalnız III

d) I,II

e) I,II,III

61-) Aşağıdakilerden hangisi Encryption formülü $m^e \bmod n = 9^7 \bmod 143 = 48 = c$ olan bir RSA şifreleme algoritmasının Decryption formülü olabilir?

a) $c^d \bmod n = 48^{103} \bmod 143 = 9 = m$

b) $c^d \bmod n = 103^{48} \bmod 143 = 9 = m$

c) $c^d \bmod n = 49^{103} \bmod 143 = 9 = m$

d) $c^d \bmod n = 49^{103} \bmod 143 = 9 = m$

e) $c^d \bmod n = 49^{103} \bmod 143 = 9 = m$

62-) RSA şifreleme algoritması ile ilgili aşağıda verilen ifadelerden hangisi yanlış bir ifadedir?

a)Algoritmada p ve a değerleri iki asal sayı olmak üzere seçilir.

b)RSA şifreleme algoritması çok büyük tamsayıları çarpanlarına a algoritmik zorluğuna dayanan bir algoritmadır.

c)Günümüzde en çok kullanılan hem şifreleme hem de sayısal imza atma olanağı tanıyan bir yöntemdir.

d)Şifrelemede kullanılan anahtarlardan biri public anahtar, diğeri ise private anahtardır.

e) $K = \{(n, p, q, a, b)\}$ verilen anahtar kümesinde saldırgan n' i çarpanlarına ayırabilirse buradan a'ya ulaşarak şifreyi kurabilir.

63-)Herhangi bir Substitution-Permutation Networks şifreleme algoritmasında $l=m=Nr=8$ olduğuna göre her döngü için kaç bitlik döngü anahtarı üretilir?

a)32

b) 64

c) 8

d) 16

e) 48

64-)Bir Substitution-Permutation Networks şifreleme algoritması için saldırgan K anahtarını ele geçirdiğine göre aşağıdakilerden hangisi doğrudur?

a) K anahtarını bildiğine göre şifreyi kırabilir.

b) Döngü anahtarının bit uzunluğunu bilirse şifreyi kırabilir.

c) K anahtarının oluşturulma mantığını bilirse şifreyi kırabilir.

d) Döngü anahtarlarının oluşturulma mantığını bilirse şifreyi kırabilir.

e) Bir tane döngü anahtarını bilirse şifreyi kırabilir.

65-) 3^{99} sayısının son iki rakamı Euler formülüne göre hesaplanırsa sonuç nedir?

- a)27 **b)67** c)81 d)01 e)37

66-) n'in hangi değeri için, $\sum_{i=1}^n i^n$ sayısı (mod 5) ile sıfır sonucunu vermez?

- a)241 **b)240** c)245 d)247 e) 237

67-) Hangi algoritma discrete logaritma hesaplamasının zorluğuna dayanır?

a)Eliptic Curve

b)AES

c)El Gamal

d)Diffie-Hellman

e)DES

68-) Diffie Hellman yöntemine göre $P=23$, $\alpha=5$, x kişinin gizli anahtarı 6 ,y kişinin gizli anahtarı 15 olsun.Buna göre K ortak anahtarını hesaplayınız.

- a) 1 b) -2 c) -1 d) 0 **e) 2**

69-) RSA tarafından anahtar üretimi ve decyrption işlemlerinde kullanılan pollig hellman algoritmasının geliştirilmiş teoremi aşağıdakilerden hangisidir?

a) Çinli Kalanlar Teoremi

b) Fermat Teoremi

c)Vigenere Chipper

d) SFA-2

e) RSA Hashing

70-) RSA algoritması için aşağıdakilerden hangisi yanlıştır?

a) Asal çarpanlarına ayrılma zorluğu yöntemine dayanır

b) Bu algoritma açık anahtarlı şifreleme yöntemidir

c) RSA algoritması anahtar üretimi,şifreleme ve şifre çözme olarak 3 basamaktan oluşur

d) n ve p publictir

e) Ron Rives bulucularındandır.

71-) Finite Fields'ta verilen $F(x) = x^3 + 2x^2 + 2x + 2$ polinomunda işlem yapabilmek için maksimum kaçınıcı dereceden polinom seçilebilir?

a) 1

b) 2

c) 3

d) 4

e) 5

72-) $F(x) \in \mathbb{Z}_3[x]$ için aşağıdakilerden hangisi irreducible değildir?

a) $F(x) = x^3 - 2$

b) $F(x) = x^3 + x^2 + 2x + 1$

c) $F(x) = x^3 + x^2 + x + 2$

d) $F(x) = x^3 - 1$

e) $F(x) = x^3 + 2x^2 + 1$

73-) Bir metnin Affine Cipher şifrlenmesinde kullanılan anahtarı (3, 1) ise deşifreleme için kullanılacak anahtar aşağıdakilerden hangisi olmalıdır?

a) (9, -9)

b) (6, -1)

c) (22, -20)

d) (322, 322)

e) (24, 5)

74-) "AB" karakterlerinin Affine Cipher yöntemine göre \mathbb{Z}_{26} da (3, 1) anahtarı kullanılarak şifrenmiş hali aşağıdakilerden hangisidir?

a) BE

b) GG

c) WP

d) END

e) KE

75-) $\gcd(234, 126) = ?$ 234 ve 126'nın en büyük ortak böleni kaçtır?

a) 18

b) 16

c) 14

d) 20

e) 22

76-) $\gcd(299, 161) = ?$ 299 ve 161'in en büyük ortak böleni kaçtır?

a) 27

b) 17

c) 19

d) 23

e) 29

77-) Shanks algoritmasında $p=809$ iken log kaçtır ?

a) 309

b) 300

c) 328

d) 617

e) 618

78-) $M = [(p-1)^{1/2}]$ denklemi ile log girdisi verilen Shanks Algoritmasında bulmak istenilen sonuç nedir ?

a) $a^{b \bmod p}$

b) $a^{p \bmod b}$

c) $b^M \bmod p$

d) $p^{\bmod b}$

e) $p^{b \bmod a}$

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

79-)“ESSE Mİ DERSUN BAA” anahtar kelimesi ve yukarıda verilen tablo kullanılarak “BENBİRCEVİZAĞACIYIMGÜLHANEPARKINDA” cümlesinin şifrelenmiş hali hangisidir?

a) İPDVOÖÖRUMÜHZÜZARFĞDÇOUZİMPTR

b) FVGFÜBFİOCTNHACJÇYNONNLVVDAĞAM

c) MYNMSCFHWPRPROUQGVHBAJOECKMAFR

d) HVGFTKJGFDGBGUIKGDTHBUUGSRBDJYF

e) KAMQLABŞIZSSNMNDNRASGRVDRGSRDS

80-)Tablo kullanılarak “MAVİ” anahtar kelimesi ile “KAMQLABŞIZSSNMNDNR” cümlesinin açık metni

hangisidir?

- a) gelmeyeceksensöyle
- b) busınavsonşansımız
- c) zamanındagelmeliydi
- d) yarınakşamsınavvar
- e) akşambizegelecekler,

81-) $M = [(p-1)^{1/2}]$ denklemi ile \log girdisi verilen Shanks Algoritmasında bulmak istenilen sonuç nedir ?

a) $a^b \bmod p$

b) $a^{p \bmod b}$

c) $b^M \bmod p$

d) $p^{\bmod b}$

e) $p^b \bmod a$

82-) $3^k = 13 \pmod{17}$

Yukarıdaki denklem için birden fazla k değeri bulunmaktadır. Aşağıdakilerden hangisi k 'nın her hangi iki değerini içermektedir?

a) (3,13)

b) (5,17)

c) (4,10)

d) (4,20)

e) (4,25)

83-) Ayrık logaritma probleminde mod değeri asal olarak seçilmektedir. $a^x = B \pmod{p}$ denklemi için p asal sayı ve a, \mathbb{Z}_p 'de primitif elemandır. Ancak p nin asal olmadığı varsayılırsa ayrık logaritma probleminin x sayısını bulma zorluğu ortadan kalkar. Bu şekilde , aşağıdaki yöntemlerden hangisi bizi x sayısına ulaştırabilir?

a) Çinli Kalanlar Teoremi

b) Euler Fonksiyonu

c) Fermat Teoremi

d) Genişletilmiş Öklit Algoritması

e) Wilson Teoremi

84-) Hangi algoritma aşağıdaki tanıma aittir?

Yapısı itibari ile blok şifreleme örneğidir. Yani basitçe şifrelenecek olan açık metni parçalara bölerek (blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrelenmiş metni açmak içinde aynı işlemi bloklar üzerinde yapar. Bu blokların uzunluğu 64 bittir.

a) DES

b) Stream

c) AES

d) Block

e) Vigenere

85-) Pohlig-Hellman algoritmasına göre $p=8101$ $\alpha=6$ $\beta=7531$ $x=?$
 $x = \log_6 7531 \pmod{8101}$

a)5210

b)6689

c)6680

d)5320

e)6489

86-) Pohlig-hellman algoritmasında $p=41$ $\alpha=7$ $\beta=12$ ise $x=?$

a)12

b)9

c)13

d)8

e)11

87-) "defend" kelimesini $\text{key}(a,b)=(3,5)$ ve Z26(İngilizce Alfabe) olacak şekilde Affine Cipher kullanarak şifreleyiniz.

a) orurso

b) defend

c) avfvdf

d) cannot

e) ghtrnm

88-)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenere karesine göre İSTANBUL

UNIVERSITY düz metnini KRIPTOGRAFI anahtarıyla şifrelenmiş aşağıdakilerden hangisidir?

a)SJXPGPAC USQFCTHBHE

b)SJBPGPAC USQFVZHBHE

c)SJBPGPABC URPGBUAIF

d)SJXPGPAC USQFVTHBHE

e)SJXPGPAC URPGBUAIAIF

89-) $x = 5 \pmod{13}$

$x = 4 \pmod{11}$,

$x = 1 \pmod{7}$

Çinli kalanlar teoremine göre x nedir?

a)785

b)686

c)648

d)588

e)789

90-) $x \equiv 1 \pmod{2} \dots(1)$

$x \equiv 2 \pmod{3} \dots(2)$

$x \equiv 3 \pmod{4} \dots(3)$

kongruans sistemi için $100 < x < 110$ olduğuna göre x nedir?

a)101

b)102

c)103

d)107

e)108

A	B	C	D	E	F	G	H	I	J	K	L		
0	1	2	3	4	5	6	7	8	9	10	11		
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12	13	14	15	16	17	18	19	20	21	22	23	24	25

91-)Hangisi EMCSNWEWL olarak şifrelenmiş metnin(ciphertext) açık metin(plaintext) halidir?

a) MUKAVEMET

b) MUKABİL

c) MUKADDES

d) MUHABBET

e) MUKAVELE

92-)Tabloya göre DLBRMVCV olarak şifrelenmiş metnin(ciphertext) açık metin(plaintext) hali aşağıdakilerden hangisidir?

a) MUKAVEMET

b) MUKABİL

c) MUKADDES

d) MUHABBET

e) MUKAVELE

93-) Z26'da Affine Cipher ile şifreleme yapılıyorsa key(a,b) ikilisi aşağıdakilerden hangisi olabilir?

a) (0 , 3)

b) (2 , 3)

- c) (2 , 5)
d) (3 , 12)
e) (16 , 9)

94-) P, α, β olarak verilen inputlara göre index Calculus yönteminde output nedir?

- a) $\alpha^\beta \pmod{p}$
b) $\log \alpha^\beta \pmod{p}$
c) $\alpha \beta \pmod{p}$
d) $\beta^\alpha \pmod{p}$
e) $(\beta/\alpha) \pmod{p}$

95-) Index Calculus yönetimine göre $\alpha=6, p=229, \beta=13$ ise cevap nedir ?

- a) 117 b) 123 c) 137 d) 148 e) 161

96-) Anahtar olarak aşağıdaki matrisin kullanıldığı Hill Cipher'da EB metninin şifrelenmiş hali nedir?

$$A = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$$

- a) NK b) OK c) SP d) TU e) YB

97-) Anahtar olarak aşağıdaki matrisin kullanıldığı Hill Cipher'da şifrelenmiş hali YS olan metnin şifrelenmemiş hali nedir?

$$A = \begin{bmatrix} 3 & 5 \\ 0 & 1 \end{bmatrix}$$

- a) QA b) KS c) HS d) ES e) MK

98-) Aşağıdakilerden hangisi Des işlem tiplerinden biri değildir?

- a) Algoritmaya giriş besleme kipi
b) Elektirik kod kitap kipi
c) Şifre geri besleme kipi
d) Şifre öbek zircirleme kipi
e) Şıkış geri besleme kipi

99-) Aşağıdaki şifreleme tekniklerinin hıza göre sıralaması yapılmıştır. Hangisi doğrudur?

1-One-Time Pad

2-Block Cipher

3-Stream Cipher

a) 1>3>2

b) 3>2>1

c) 2>3>1

d) 3>1>2

e) 2>1>3

100-) Hangisi Aes temel basamaklarından biri değildir?

a) AddRoundKey dönüşümü

b) ByteSub dönüşümü

c) ShiftRow dönüşümü

d) Mix Column dönüşümü

e) SubIndex dönüşümü