İKİNCİ ÖĞRETİM SORULARI

KONU ADI : gcd

1)gcd (234, 126) =?
234 ve 126 nın en büyük ortak böleni kaçtır?
a) 18 b)16 c)14 d)12 e)22

2)gcd (299, 161) =?
299 ve 161 in en büyük ortak böleni kaçtır?
a)23 b)17 c)19 d)27 e)29

3)gcd (779, 533) =?
799 ve 553 ün en büyük ortak böleni nedir?
a)29 b)33 c)39 d)40 e)41

KONU ADI : mod, çinli kalanlar

4)6x = 2 mod 11, x kaçtır?
a) 15 b)12 c)13 d)14 e)17

5)7x = 3 mod 62, x kaçtır?
a)27 b)24 c)23 d)26 e)22

6)x = 5 mod 13
x = 4 mod 11 ,
x = 1 mod 7
x çinli kalanlar teoremine göre nedir?

a)706 b)759 c)783 d)784 e)785

KONU ADI :Kriptoloji Nedir ?

7) Kriptoloji Nedir ?

A- Mikrooişlemcili sistemlerde kullanılan bir tür veri deposudur.

B - Gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür

C- İki merkez arasında, kararlaştırılmış işaretlerin yardımıyla yazılı haberlerin veya belgelerin iletimini sağlayan bir telekomunasyon düzenidir.

D- Dijital ses oynatıcıları ve akıllı telefonlar gibi cihazların kablosuz olarak internete bağlanmasını sağlayan teknolojidir.

E- Çeşitli iletilerin, yazıların belli bir sisteme göre şifrelenmesi, bu mesajların güvenlikli bir ortamda alıcıya iletilmesi ve iletilmiş mesajın deşifre edilmesidir.

8)Kriptoloji ne bilimidir ?

A - Fizik
B- Matematik
C-Geometri
D- Yöneylem
E - Makine

9) Aşağıdakilerin hangisi Kriptoloji şifreleme tekniklerinden biri değildir ?

A-Sezar şifrelemesi

B-Rotor makinesi (Enigma)

C-ETL Süreci

D-Açık anahtarlı şifreleme

E-Veri gizleme teknikleri

KONU ADI : Şifreleme Algo. Sınıflan., AES

10) Aşağıdakilerden hangisi yanlıştır?
A)AES algoritması asimetrik şifreleme algoritmalarına bir örnektir.
B) Simetrik şifreleme algoritmaları asimetrik olanlara göre daha hızlıdır.
C) Asimetrik şifreleme algoritmaları matematiksel problemlerin çözümlerinin karmaşık olmasına dayanmaktadır.
D) Asimetrik şifreleme algoritmaları simetrik şifreleme algoritmalarına göre daha güvenlidir.
E) Simetrik şifreleme algoritmalarında şifrelemede kullanılan anahtar ile şifre çözmede kullanılan anahtar aynıdır.

11) Aşağıdaki şifreleme algoritmalarından hangisi Akış Şifrelemesi(Stream Cipher) algoritmalarına bir örnektir?
A) Affine Cipher
B) Hill Cipher
C) Vigenere Cipher
D) Permutation Cipher
E)AutoKey Cipher

12) Aşağıdakilerden hangisi AES şifreleme algoritmasında her döngüde kullanılan basamaklardan biri değildir?
A) MixColumn Dönüşümü
B) ByteSub Dönüşümü
C) ShiftColumn Dönüşümü
D) AddRoundKey Dönüşümü
E) ShiftRow Dönüşümü

13)Aşağıdakilerden hangisi 3DES'i DES'ten daha güvenli kılan özelliktir?

A) Rijndael Algoritmasının 3DES kullanarak daha karmaşık olması
B) Uzun plaintext uygulanabilirliği
C) Private key kullanması
D) 3 veya 2 key ile uygulama seçeneklerinin bulunması
E) DES yöntemlerinin 3 kez kullanılması ile karmaşık hale gelmesi

14)Aşağıdakilerden hangisi simetrik şifrelemenin özelliklerinden değildir?

A) Gerçeklenebilirliği daha kolaydır
B) Örneklerinden bazıları DES ve 3DES algoritmalarıdır
C) Asimetrik şifreleme ile karşılaştırıldığında performansı düşüktür
D) Simetrik şifrelemeler içerdiği basit işlemlerden dolayı elektronik cihazlarda uygulamak çok daha kolaydır.
E) Simetrik şifreleme anahtar karşıya güvenli bir şekilde iletildiği sürece Açık anahtarlı şifrelemeden daha güvenlidir.

15)Aşağıdakilerden hangisi asitmetrik şifrelemenin özelliklerinden biri değildir?

A) Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir
B) Simetrik şifreleme sistemleriyle karşılaştırıldığında, asimetrik sistemler çok daha yavaştır
C) Örneklerinden bazıları DES ve AES algoritmalarıdır
D) Asimetrik şifreleme kullanılan bir ortamda, her kullanıcı için ayrı anahtar oluşturma zorunluluğu vardır
E) Asimetrik şifreleme anahtarın saklı olmaması avantajını anahtarlar arasındaki zor matematiksel ilişki(çarpanlara ayırma vb.)den alır

KONU ADI :DES ve AES

16)Hangisi DES in işlem kiplerinden değildir?
A)ECB B)CFB C)ECE D)ECB E)CBC

17) AES Algoritması kaç döngüden oluşur?
A)5 B)7 C)8 D)9 E)10

18)AES Algoritmasında bir döngü kaç bitle başlar ve kaç bitle sonlanır?
A)128-128 B)32-64 C)128-64 D)64-128 E)64-64

KONU ADI : Data Encryption Standart

19) DES algoritmasında kullanılan anahtar kaç bit uzunluğundadır?
A) 8-Bit
B) 16-Bit
C) 32-Bit
D) 56-Bit
E) 64-Bit

20)Aşağıdakilerden hangisi DES in temelini oluşturan algoritmadır?
A)Lucifer
B) Hill Ciper
C) Vigenere Ciper
D) Oklid
E) Block Ciper

21) Aşağıdakilerden hangisi DES (Data Encryption Standard) işlem kiplerinden değildir?
A) ECB (Elektronic codebook mode)
B) OFB (Output feedback mode)
C) OCB (Output codebook mode)
D) CBC (Cipher block chaining mode)
E) CFB (Cipher feedback mode)

KONU ADI : RSA

22)RSA algoritması kaç yılında üretilmiştir?

A. 1976
B. 1961
C. 1951
D. 1940
E. 1977

23)RSA kullanılarak yapılacak bir şifreleme için p değeri 3, q değeri ise 11 olarak verilmiştir. Bob ve Alice hakkında aşağıdakilerden hangisi doğrudur?

A. Alice 25 sayısını çözerek 16 sayısını elde etmiştir
B. Alice 32 sayısını şifreleyerek 50 sayısını elde etmiştir.
C. Alice 8 sayısını şifreleyerek 15 sayısını elde etmiştir.
D. Alice 16 sayısını şifreleyerek 25 sayısını elde etmiştir..
E. Alice 16 sayısını çözerek 25 sayısını elde etmiştir.

24)RSA kullanılarak yapılacak bir şifreleme işlemi için p = 101, q = 113 ve n = 11413 olarak verilmiştir. Ali 9726 sayısını şifrelerse aşağıdakilerden hangisini elde edecektir?

A. 5341
B. 4241
C. 5661
D. 6752
E. 5761

KONU ADI : Pohlig-Hellman Algoritması

25)Pohlig-Hellman Algoritması kim ya da kimler tarafından bulunmuştur?

A. Steven Pohlig - Vesly Hellman
B. Steven Pohlig - Marin Hellman
C. Marin Hellman
D. Alice Pohlig
E. Bob Marley

26)Aşağıdaki algoritmalardan hangisi DLP Discrete Logaritma hesaplanma zorluğuna dayanmamaktadır?

A. Shank Algoritması
B. Diffie Hellman Anahtar Değişim Algoritması
C. RSA
D. Pohlig-Hellman Algoritması
E. El Gamal Şifreleme Algoritması

27)Pohlig-Hellman Algoritması çözümünde elde edilen denklemler en son hangi yöntem ile çözülür?

A. Euler-Pi Teoremi
B. Euler Teoremi
C. Çinli Kalanlar Teoremi
D. Wilson Teoremi
E. Hiçbiri

KONU ADI :INDEX-CALCULUS YÖNTEMİ

28) 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)Hiçbiri
d)t+c şeklinde logaritma düzenine ulaştırılır verilen ilk denklemler
e)Katsayı tabanı seçilir

29)Index-Calculus yönteminde 4.adımdaki B.α^r ifadesini S deki elemanların çarpımı cinsinden yazılamazsa ne yapılır?
a)0 <= r <= (p-1) olmak üzere rastgele bir r ifadesi seçilir .
b)S kümesindeki elemanların ters logaritması alınır
c)lineer ilişkiler t+c şekline çevrilmeye calısılır.
d) katsayı tabanı değiştirilir.
e) B.α^r ifadesi S ifadesine göre modu alınır.

30) Index Calculus Yöntemi çözüm basamakları toplam kaç basamaktan oluşur?
a)4 b)2 c)5 d)3 e)1

KONU ADI :Şifreleme Algoritmaları

31) Aşağıdakilerden hangisi şifreleme algoritmalarından herhangi biri değildir ?

A) DES
B) DSA
C) UZİ
D) KEA
E) RSA

32) Aşağıda verilen bilgilerden hangisi yanlıştır ?

A) DES Algoritması günümüzde kullanılan en güçlü algoritmalardan biridir.
B) DES günümüzdeki birçok simetrik şifreleme algoritması gibi şifreleme için Fiestel yapısını kullanılır.
C) DES algoritması gizli anahtar yönetimini kullanan simetrik şifrelemeli bir algoritmadır.
D) 3DES algoritması DES şifrelemesinin 3 kere art arda yapılması şeklinde çalışır.Bu yüzden DES'e göre 3 kat daha yavaştır.
E) 3DES şifreleme yapmak için uzunluğu 24 bayt olan bir anahtar kullanılır.

33) Substitution Cipher yöntemine göre; şifrelenecek mesajı "baba dede" ve anahtarı "fdeachgb" olan mesajın şifreli metni aşağıdakilerden hangisidir ?

A) Şifreli Metin: "dfdf acac" olacaktır.
B) Şifreli Metin: "klbc gcbc" olacaktır.
C) Şifreli Metin: "efcf fybc" olacaktır.
D) Şifreli Metin: "kfdc dcab" olacaktır.
E) Şifreli Metin: "efdf gyab" olacaktır.

KONU ADI :Affine Cipher

34)Mod 14 te yapılan bir Affine cipher yönteminde a kaç tane değer alabilir?
a)6
b)7
c)8
d)9
e)1

35)Mod 14 te yapılan bir Affine cipher yönteminde b kaç tane değer alabilir?
a) 14
b)7
c)13
d)5
e)1

36)Mod 14 te yapılan bir Affine cipher yönteminde anahtar uzayı nedir ?
a) 80
b)200
c)144
d)182
e)84

KONU ADI :EULER FONKSİYONU

37)n pozitif tamsayısı için Φ(n), n sayısının Euler fonksiyonunu göstermek üzere

$\Phi(2n) = \Phi(n)$

olacak şekilde $100 \leq n \leq 200$ şartını sağlayan kaç tane pozitif tamsayı vardır?

A) 50 B) 30 C) 40 D)70 E)100

38)Φ(180) in değeri kaçtır?

A) 48 B)20 C)50 D)60 E)96

39)3^{999} sayısının son iki rakamı nedir?

A) 63 B)64 C)65 D)66 E) 67

KONU ADI :SEZAR ŞİFRELEME ALGORİTMASI

40)Aşağıdakilerden hangisi Sezar Şifreleme Algoritmasının özelliklerinden değildir?

a-)Julius Caesar tarafında askeri bilgileri yollarken sorun çıkmaması için üretilmiş bir şifreleme algoritmasıdır.
b-)Sadece harfleri kaydırarak şifreleme yapar.
c-)Sezar algoritmasında harflerin 14'erli kaydırılmasıyla oluşturulmaktadır.
d-)Ağ haberleri aktarma protokolünü kullanmaktadırlar.
e-)Üretilen ilk şifreleme algoritması kabul edilir

41)Aşağıdakilerden hangisi Sezar Şifreleme Algoritmasının zayıflıklarından değildir?

a-)Şifrelenmiş metinden hangi dilin kullanıldığı rahatlıkla anlaşılabilir.
b-)Türkçe için düşündüğümüzde sadece 28 ayrı şifreleme geliştirilmiş olabilir.
c-)Modüler aritmetik üzerine inşa edilmiştir.
d-)Sezar şifrelemesi gibi algoritmaların bilindiği yöntemlerde olası bütün kombinasyonların denenmesi demektir.
e-)Sezar şifrelemesi ile şifrelenmiş bir metin “Brute Force” bir saldırı ile kırılabilir.En zayıf ama en kesin saldırı yöntemidir.

42)Sezar şifreleme sisteminde, “SEZAR” açık yazısı, Türkçe alfabede, hangi gizli yazıya dönüşür?

A-)RDYZP
B-)BRÜTÜS
C-)SFABS
D-)UĞCÇT
E-)KAVAKLI

KONU ADI :Quadratic Residue & Legendre Symbol

43)Aşağıdakilerden hangisi Z_{13} in quadratic residue'lerinden biridir?

A) 2
B) 4
C) 6
D) 8
E) 14

44)Aşağıdakilerden hangisi Z_{15} in quadratic non- residue'lerinden birisi değildir?

A) 2
B) 3
C) 4
D) 5
E) 7

45)Legendre Symbol e göre $(12345/331)$ işleminin sonucu kaçtır?

A) -1
B) 0
C) 1
D) 37
E) 98

KONU ADI :Substitution Cipher

46)Substitution şifrelemesinde key space ne kadardır?
A- 25×25! B- 26×26! C-28×28! D- 29×29! E-27×27!

47) “BECAUSE” metnini verilen key e göre substitution cipherda şifrelendiğinde şifreli metin hangisidir?
Key:B A D C Z H W Y G O Q X S V T R N M S K J T P F E U
A- AZDBJSZ
B- AZBJSZD
C- ABJSDZC
D- BSDJAZC
E- DSBJASZ

48)Plaintext:we are discovered
Chiphertext:zebrascdfghijklmnopqtuvwx
Verilen plaintext i chiphertext e göre substitution cipher ile şifrelendiğinde şifreli metin hangisidir?
A-va zoa rfpbluaoar
B-db psd whvjtuszuo
C-tz kls pwajydiear
D-sa vrz adcpldfsaz
E-wa vao ytsaenbltpx

KONU ADI : Shift cipher

49)Key=11,
Plain text=”CRYPTOGRAPHYISFUN” olarak verilen metni shift cipher şifreleme algoritmasını kullanarak şifreleyin.
A)MCJSHYDFRGSBNIOPY
B)NCJSTAHYAGREVNBHYS
C)NCSHYGAHTOPTKFHJS
D)MHAGSFKLIYURTHYBS
E)NCJAVZRCLASJTDQFY

50)Key=19,
Plain Text=”KHAN” olarak verilen metni shift cipher şifreleme algoritmasını kullanarak şifreleyin.
A)”DAGT”
B)”ZAGT”
C)”DAHG”
D)”ADTG”
E)”DATG”

51) K=3,
Plain Text=”meet me after the toga party” olarak verilen metni shift cipher şifreleme algoritmasını kullanarak şifreleyin.
A)OPHU YY AYSDA FGY JUIS HUGDS
B)PHHW HP DIERT FGH ASDS GHYUS
C)PHWH GH ASHRT HYU KJDS HYGUS
D)HPWH HH ASHGJ DFG HUYS HYGSS
E)PHHW PH DIWHU WKH WRJD SDUWB

KONU ADI :Genel Kriptoloji Bilgileri

52) Enigma aşağıdaki ülkelerden hangisinin savaş döneminde kullandığı şifreleme yöntemidir?

A-Irak
B-İran
C-Sırbistan
D-Yunanistan
E-Almanya

53)Banka hesapları sosyal medya hesapları lokasyan bilgileri mesaj içerikleri gibi bilgilerin yer aldığı Big Data hangi yöntemle korunur?

A-Typex
B-Sigaba
C-Des
D-Firewall
E-Kriptoloji

54)Brute-Force(kaba kuvvet) saldırısıyla kolay çözülen şifreleme yöntemi hangisidir?

A-Sezar şifrelemesi
B-Açık anahtarlı şifreleme
C-Veri gizleme
D-Çırpı fonksiyonu
E-Rotar makinesi

KONU ADI : Shanks Algoritması

55) Shanks algoritması kaç yılında geliştirilmiştir?
A)1926
B)1938
C)1946
D)1962
E)1973

56) Shanks algoritmasında p=809 iken log kaçtır ?
A)309
B)128
C)310
D)617
E)618

57) M=[(p-1)^1/2] denklemi ile log girdisi verilen Shanks Algoritmasında bulmak istenilen sonuç nedir ?
A)b^M mod p
B) a^p mod b
C) p^b mod a
D) p^a mod b
E) a^b mod p

KONU ADI :Affine Cipher

58)’ISTANBUL UNIVERSITESI’ kelimesinin kısaltmasının harflerini Affine Cipher ile şifreleyiniz. (Z26) k=(7,3)

A)’GK’
B)’BS’
C)’BA’
D)’NA’
E)’HN’

59) ‘MPA’ textini k=(5,12) keyine göre affine cipher algoritması ile deşifre ediniz.(Z26)

A)’YUT’’
B)’BBS’
C)’NAL’
D)’DEA’
E)’ALI’

60)Z20çalışma uzayı için anahtar uzay kaçtır?
A)8
B)9
C)10
D)11
E)16

KONU ADI : Miller-Rabin

61) Aşağıdakilerden hangisi bir Olası (probabilistic) Asallık Testi değildir?

A-Fermat
B-Slovay & Strassen
C-Euler
D-Frobenius
E-Miller&Rabin

62) Miller-Rabin testine göre 256 bitlik bir n sayısı için, 6 test sonunda hatalı cevap alma olasılığı aşağıdakilerden hangisi olabilir?

A- 2^{-59}
B- 2^{-34}
C- 2^{-40}
D- 2^{-58}
E- 2^{-118}

63) Miller-Rabin testi uygulamasında aşağıdaki aşamalardan hangisi yanlıştır?

A- 4. Eğer ($j > 0$) ve ($z = 1$) ise n asaldır.
B- 2. $j = 0$ olarak ayarlanıp $z = a^r \bmod n$ hesaplanır.
C- 3. Eğer ($z = 1$) veya ($z = n - 1$) ise n asallık testini geçer ve asal olabilir.
D- 1. n den küçük olacak bir rastsal a sayısı bulunur.
E- 5. $j = j + 1$ olarak ayarlanır. Eğer ($j < s$) ve ($z \neq n-1$) ise ($z = z^2 \bmod n$) olarak ayarlanır ve 4. Adıma geri dönülür. Eğer ($z = n - 1$) ise n asallık testini geçer ve asal olabilir.

KONU ADI : RSA,AES,DES

64) RSA şifreleme algoritması için aşağıdakilerden hangisi yanlıştır?
A) Asal çarpanlarına ayrılma zorluğu yöntemine dayanır.
B) n,b public dir.
C) p,q private dir
D) a public dir.
E) p ve q asaldır

65) AES şifreleme algoritması ile ilgili aşağıdakilerden hangisi yanlıştır?
A) Son döngüde AddRoundKey kullanılır.
B) SubBytes çevriminde Durum matrisindeki her bayt bir tabloya göre ve doğrusal olmayan bir dönüşümle güncellenir.
C) ShiftRows çevriminde Her satır belirli bir sayıda çembersel olarak kaydırılır.
D) MixColumn Her bir sütundaki dört bayt, birbirleri ile karıştırılır.
E) Toplam 4 çevrimden oluşur.

66) Aşağıdakilerden hangisi DES (Data Encryption Standard) işlem kiplerinden değildir?
A) ECB (Elektronic codebook mode)
B)CFB (Cipher feedback mode)
C)OCB (Output codebook mode)
D)CBC (Cipher block chaining mode)
E)OFB (Output feedback mode)

KONU ADI :Diffie Hellman

67)Diffie Hellman yöntemine göre P=23, α=5,x kişisinin gizli anahtarı 6 ,y kişisinin gizli anahtarı 15 olsun.Buna göre K ortak anahtarını hesaplayınız.
A)1
B)7
C)4
D)5
E)2

68)Aşağıdaki algoritmalardan hangisi discrete logaritma hesaplamasının zorluğuna dayanır?
A)RSA
B)AES
C)El Gamal
D)Diffie-Hellman
E)DES

69)Diffie Hellman Anahtar Değişim Algoritmasında anahtar denklemindeki p ve α değerleri için aşağıdakilerden hangisi doğrudur?
A)p: private; α public ve Zp de primitif eleman.
B) p:public; α private ve Zp de primitif eleman değil.
C) p:private; α private ve Zp de primitif eleman değil.
D)p:public; α public ve Zp de primitif eleman.
E)p:private; p: private; α public ve Zp de primitif eleman değil.

KONU ADI :Elliptic Curve

70)Elliptic curve'de x1≠x2 iken λ, x3, y3 değerleri aşağıdakilerden hangisi gibi olur?

A)$\lambda=(y2-y1)/(x2-x1)$
$X3=\lambda^2-x1-x2$
$y3=\lambda(x1-x3)-y1$

B)$\lambda=(y1-y2)/(x1-x2)$
$X3=\lambda-x1-x2$
$y3=\lambda(x1-x3)-y1$

C)$\lambda=(y2-y1)/(x2-x1)$
$X3=\lambda-y2-x1$
$y3=\lambda(x1-x3)-y2$

D)$\lambda=(y2-y1)/(x2-x1)$
$X3=\lambda-x1-x3$
$y3=\lambda(x2-x3)-y1$

E)$\lambda=(x2-x1)/(y2-y1)$
$X3=\lambda^2-x1-x3$
$y3=\lambda(x2-x3)-y1$

71) Elliptic curve'de x1=x2 ve y1=y2 iken λ değeri aşağıdakilerden hangisi gibi olur?

A) $(3(x1)^2+a)/2y(1)$
B) $(3(x2)^2+a)/2y(1)$
C) $(3(x2^2)/2y(1)$
D) $((x1)^2+a)/2y(1)$
E) $(x1)^2/2y(1)$

72) Elliptic curve genel denklemi nedir?

A) $y^2=x+2abx+b$
B) $y=x^3+ax+b$
C) $y^2=x^2+acx+b$
D) $y^2=x^3+2abx+b$
E) $y^2=x^3+ax+b$

KONU ADI :ElGamal Şifreleme Algoritması

73) 1.Şifreleme Algoritması
2.Deşifreleme Algoritması
3.Anahtar Sayacı
4.Anahtar Üreteci
ElGamal şifreleme algoritmasının bileşenleri yukarıdakilerden hangileridir?

A) 1. 2. ve 4. B)1. ve 2. C)2. ve 4. D)1. 2. ve 3. E)Yalnız 4

74) p=250 , α=2 , a = 33 değerleri veriliyor ve ElGamal algoritmasını kullanarak β değeri kaç olur?

A)13 B)28 C)92 D)180 E)184

75) Soru 2 deki verilerle ek(1093, 29) a göre , y1 değeri kaç olur?

A)381 B) 396 C)482 D)455 E)964

KONU ADI :Euler ϕ

76) ϕ(91)=? Euler ϕ degeri kaçtır

a)144 b)18 c)48 d)84 e)288

77)ϕ(99)=? Euler ϕ değeri nedir

a)150 b)25 c)45 d)120 e)60

78)ϕ(169)=? Euler ϕ değeri nedir

a)153 b)154 c)313 d)312 e)156

KONU ADI : Permutation Cipher

79)

x	1	2	3	4	5
μ(x)	4	3	5	1	2

Yukarıdaki tabloya göre m=5 düzeninde şifrelenmiş olan aşağıdaki textin çıktısı nedir ?
P=”var boyle donemler ve hicbir sey ins”
A-) “kgo eyviu komgkmeb ij fbkrmr bqr vif”
B-) “chy ivfsl kvultsly cl opjipy zlf puz”
C-) “ydu erboh grqhpohu yh klfelu vhb lqv”
D-) “ova rbedo lylnmee he virsir bcn eyis”
E-)“bro vadeo yllmene he irvrisc bni sey”

80)

x	1	2	3	4	5	6
μ(x)	6	3	1	5	2	4

Yukarıdaki tabloya göre m=6 düzeninde şifrelenmiş olan aşağıdaki decrypted textin plain text hali hangisidir ?
C=”srheekahiynaintkiaremaskzaiasm”
A-) “herkesinhayatinakimsekarısamaz”
B-) “herkesinbelirlizaaflarivardir”
C-) “hepimizbirimizicinsavasiyorken”
D-) “hayallerparishayatlarbagcilarbe”
E-) “heristebirhayirgormeklazimtabi”

81)

x	1	2	3	4	5
μ(x)	2	4	1	5	3

Permutation Cipher’ın bir gelişmiş versiyonu uygulanmak isteniyor. Bu versiyonda harf bazında yapılan şifreleme uygulamasından sonra kelimeleri de aynı yöntemle şifrelemek istersek yukarıdaki tablo ışığında aşağıdaki Plain Text’in şifrelenmiş hali hangisi olmalıdır ?
P=”bendeki de ileri duzey klostrofobi”

A-) “Ki rzyuk edbenie eotlrsfboio deild”
B-) “un dkeib mrooun oustinbounap field”
C-) “kdfaud ki sfgtr mueoa lgookria”
D-) “li djuac kedmvne ossaeuejbol leidf”
E-)“an kleiba dkeib beild eosrloboint”

KONU ADI : Eliptik Eğri Şifreleme(ECC)

82) Aşağıdakilerden hangisi Eliptik Eğri Şifreleme(ECC) nin özelliklerinden biri değildir?

A) İşleyişi RSA'ya benzerdir.
B) $y^2=x^3+ax+b$ ye dayanır.
C) RSA ya göre daha yüksek anahtar değeri taşır.
D) Temel birimler eliptik eğri üzerindeki noktalardır.
E) q=n*p dir.

83) Aşağıdakilerden hangisi Eliptik Eğri Şifreleme(ECC)'nin RSA ve Diffie Hellman'dan farklarından biri değildir?

A) Daha hızlı çalışır.
B) Kırılması daha zordur.
C) Daha çok bellek kullanır.
D) Aynı anahtar boyutu için RSA ve Diffie Hellman'a göre daha güvenlidir.
E) 163 bit ECC şifreleme 1024 bit RSA şifreleme ile denktir.

84) 1985 yılında Victor Miller ve Neal Koblitz tarafından geliştirilen açık anahtar kripto sistemli, ayrık logaritma probleminin zorluğuna dayanan ve diğer şifreleme yöntemlerine göre daha az anahtar uzunluğu olan algoritma hangisidir?

A) ECC
B) RSA
C) DSA
D) AES
E) Diffie Hellman

KONU ADI : DSA

85)Dijital imzalama algoritması(DSA) hangi ülke tarafından kullanılmaya başlanmıştır?

A)Fransa
B)Amerika Birleşik Devletleri
C)Çin
D)Japonya
E)İngiltere

86)DSA'nın RSA dan farkı aşagıdakilerden hangisidir?

A)Sadece imzalama için kullanılabilmesi,şifreleme yapılamaması
B)RSA'nın 128bit, DSA'nın 64 bit kullanabilmesi
C)DSA'nın kullanım alanın daha geniş olması
D)Hem imzalama için kullanılıp hem de şifreleme yapılabilmesi
E)İmzalama için kullanılamayıp,şifreleme yapılabilmesi

87)Dijital imza algoritması için verilen bilgilerden hangisi yanlıştır?

A) Birkaç imzadaki k nın bazı bitleri sızdırılarak Dijital İmza Algoritması kırılamaz.
B) Bunlardan birinin olmaması halinde saldıran gizli anahtarı açığa çıkartabilir.
C)Aynı değer iki kez kullanılırsa (kyı gizli tutsa bile), tahmin edilebilir
D)Dijital İmza Algoritmasında k rassal imza değerinin entropisi, gizliliği ve tek olması önemlidir.
E) Dijital İmza Standardı anahtar uzunluğundaki L'nin değerini 512 ile 1024'ün arasında 64'ün katı olarak kısıtlamıştır.

KONU ADI :Cipher

88)Hangi şifreleme yönetiminde Key bir matristir?

A)Hill cipher
B)Substitution cipher
C)Affine cipher
D)Vigenere cipher
E)Shift cipher

89) Aşağıdaki şifreleme yöntemlerinden hangilerinde bilinen açık mesaj saldırısı (known plain text) başarılı sonuç verir?

A)Affine Cipher
B)Substitution cipher
C)Viegnere Cipher
D)Hill Cipher
E)Hepsi

90)Aşağıdakilerden hangisi Hill cipher şifreleme yöntemi özelliklerinden değildir?

A)Düz metin n uzunluğundaki bloklar şeklinde şifrelenir.
B)Hill şifreleme yöntemi bir blok şifreleme örneğidir.
C)Düz metin bitişik ve farklı uzunluktaki farklı bloklara bölünür.
D)Klasik şifreleme yöntemidir.
E)Öncelikle mesajın göndericisi ve alıcısı bir nxn lik matrix üzerinde anlaşmış olmalılardır.

KONU ADI :Genişletilmiş Euclid Algoritması,Şifreleme genel

91) Canı sıkılan bir analitik geometrici eğimi olan ve A(1,12) noktasından geçen doğruyu kullanarak "ASİTANE" kelimesini şifreleyip edebiyatçıya takılmak isteyince kullandığı şifre metni ne olur?(uzay kümesini 29 alfabe olarak belirleyiniz.)

A) HLRKGUZ
B)HLZUTRK
C)HLRKUHZ
D)HRKLZUH
E)HLKRHZU

92) Genişletilmiş euclid algoritmasına göre gcd(49,36) ' i hesaplayarak U,T ikilisinden oluşan denklemi ve 49 sayısının mod36 'e göre tersini R belirtiniz.

A) -15 , 11 , 11
B) -11 , 15 , 15
C) -15 , 11 , 25
D) -11 , 15 , 25
E) -15 ,-11 , 15

93) AES algoritması, 128 bit veri bloklarını 128, 192 veya 256 bit anahtar seçenekleri ile şifreleyen bir blok şifre algoritmasıdır. Verilen bu bilgiye göre aşağıdakilerden hangisine ulaşılabilir?

A)Döngüsel işlemin artmasıyla veri daha çok güvenilir hale gelir. Fakat aynı zamanda yapılacak olan döngüsel işlemlerin de artmasıyla hem işlem sayısı artar hem de bellek alanı artar.
B) AES şifrelemede kullanılan döngü sayısı değişmez ve döngü sayısı 10 turdur.
C) Anahtar uzunluğunun değişmesi AES şifrelemesi için kullandığı döngü sayısını etkilemez.
D) AES şifrelemede kullanılan döngü sayısının artması yada azalması işlem sayıs ve bellek alanını etkilemez.
E) Hiçbiri

KONU ADI : Hill Cipher

94) Aşağıdaki verilenlerden hangisi Hill Cipher için doğrudur?

A) Bir akış şifrelemesidir. (Stream Cipher)
B) Basitçe şifrelenmek istenen metindeki her karakterin anahtara kadar kaydırılması ile şifrelenir.
C) Bir blok şifrelemesidir. (Block cipher)
D) Plain Text farklı uzunlara bölünebilir.
E) DES'in temelini oluşturan algoritmadır.

95) Hill Cipher algoritması ilk olarak kaçıncı yayınlanmıştr?

A) 20
B) 21
C) 19
D) 18
E) 17

96) Hill Cipher için,

I) Frekans saldırısı tekniğine karşı oldukça zayıftır.
II) Kullanılan alfabedeki harf genişliği bilinmiyorsa saldıran kişi plaintext'e sahip olsa bile saldırısı başarısız olur.
III)Klasik şifreleme yöntemidir.

yargılarından hangisi yada hangileri yanlıştır?

A) I ve II B) I C) Hepsi D) III E) I ve III

KONU ADI : Şifreleme Algoritmaları

97) Bir metnin içinde bulunan harflerin yer değiştirmesi mantığına dayanan şifreleme yöntemi aşağıdakilerden hangisidir?

A) Permutation Cipher
B) Stream Cipher
C) Hill Cipher
D) Autokey Cipher
E) Shift Cipher

98) Şifrelenecek metni anahtar olarak kullanan şifreleme algoritması aşağıdakilerden hangisidir?

A) Autokey Cipher
B) Vigenere Cipher
C) Affine Cipher
D) Substitution Cipher
E) Shift Cipher

99) Şifreleme algoritmalarından hangisinin yöntemi geometrideki doğrunun denklemi olan y=ax+b doğrusal fonksiyonunu şifreleme işleminde kullanmaktır?

A)Affine Cipher
B) Hill Cipher
C) Stream Cipher
D) Autokey Cipher
E) Permutation Cipher

KONU ADI :Eliptic Curve

100) Eliptic Curve Kriptografi ile ilgili aşağıdakilerden hangisi doğru değildir ?

A.) x ve y elemanıdır RxR (x,y£ RxR);
B.) Eğri denklemi (y^2) +a.x+b de 4a^3 + 27b^2 != 0
C.)Eğri üzerinde olmayan herhangi bir nokta şifrelenebilir
D.)Special Point kullanımı vardır
E.)Eğri mutlaka non-singular olmalıdır

101)Eliptic Curve algoritması üzerinde elgamal şifrelemenin uygulanmasıyla ilgili hangisi yanlıştır?

A.) L , B , a ,P) public(Doğru cevap)
B.) a.L = B (mod p)
C.)L pirimitif elemandır
D.) dk(y1,y2) = y2-a.y1
E.) y2 = (x+k.B) dan hesaplanır

102) Finite Fields ile ilgili aşağıdakilerden hangisi doğrudur ?

A.) Verilen denklemde en büyük üslü değişkenin bir eksiğinin 2^x te yerine koyulması ile çarpanlarına ulaşılabilir
B.)Çarpanlarına ayrılan denklem kümeleri kullanılır
C.) Denklemlerde katsayıların Z2[x] den büyük olması önemli değildir
D.) Z2[x] uzayında çalışılır
E.)Bu uzayda tüm denklemler çarpanlarına ayrılabilir

KONU ADI :INDEX-CALCULUS YÖNTEMİ

103)
I: (α ^r). β hesaplanır,s deki elemanların çarpımı şeklinde yazılmaya çalışılır.
II:s kümesinin elemanlarının logaritmaları hesaplanır.
III:p nin ayrık logaritmalarını hesaplayabilmek için S kümesindeki elemanların logaritmalarını içeren lineer ilişkiler oluşturulur.
IV:Katsayı tabanı seçilmesi.Zp* da bir asal sayılar alt kümesi seçilir.(s={p1,p2,p3…})
Index-Calculus yöntemine göre yukarıdaki adımlar hangi sıra ile gerçeklenir.
a. I- II- III- IV b. IV- I- III- II c. I- II- IV- III d. II- I- III- IV e.IV- III- II- I

104)Index-Calculus yöntemi için hangisi yanlıştır?
a.(α ^r). β (mod p) hesaplanırlen ön koşul 0 <= p-1<= r aralığıdır.
b.s kümesinin elemanlarının logaritmaları hesaplanırken (alpha tabanında log pi'de)lineer denklem takımlarının çözüm aralığı 0<=i<=t şeklindedir.
c. adım 2 de α ^k (modp) 0<=k<=(p-1) aralığındadır.
d. (α ^r). β = (alt sınır pi ,üst sınır t) ∏.di iken di>=0
e.adımlar başarılı olmadığında tekrara gidilebilir.

105)
p=229 , α = 6, β =13 olsun ,x= α tabanında log β nedir?
a.119 b.118 c.115 d.116 e.117

KONU ADI :Vigenere Cipher

106)Anahtar boyutu 3 olarak verilen bir Vigenere Cipher da şifrenmiş bir metne saldırmak isteyen kişi hangi yöntemi kullanılır?

A) Şifreli metni her 3 harfte bir harf frekans analizine tabi tutarak çözümleyebilir.
B) Block uzunluklarını 3 ten başlatarak arttırabilir ve tüm ihtimalleri deneyebilir.
C) Karakterlerin hangi fonksiyona göre yer değiştirdiği bulunabilir.
D) Kaba kuvvet saldırısı(Brute froce attack) ile şifre kırılmaya çalışabilir.
E) Her anahtar tek tek denenerek doğru olanı tespit edilebilir

107)Vigenere algoritması ile şifrelenmiş Cipher text'in : " MZXWXFNWYPWZPIKZSIWTPYM" olduğu ve "CIPHER" anahtarı kullanıldığı bilindiğine göre plaintext i bulunuz .

A) Kriptolojidersinotları
B) Kriptolojisınavsoruları
C) Kriptolojiödevkonuları
D) Kriptolojisınavsüresi
E) Kriptolojisınavkonuları

108)Vigenere şifrelemede kullanılan şifreleme yöntemi aşağıdakilerden hangisidir ?

A) Çok alfabeli şifreleme (Polyalphabetic)
B) Tek alfabeli şifreleme (Monoalphabetic)
C) Asimetrik şifreleme
D) Çok anahtarlı şifreleme
E) Blok şifreleme

KONU ADI :Şifreleme Yöntemleri

109)Farzedelim ki mesaj y=(11x+4)MOD26 fonksiyonu ile şifrelensin.Şifreli metnimiz MONEY.MONEY metnimizin uygun sayısal değerleri 12, 14, 13, 4 ve 24 tür.Buradaki her bir değer için daha önce belirlediğimiz y=(11x+4)MOD26fonksiyonunu kullanırsak, şifreli metin ne olur?

A-)WCRIG

B-)BWCRI

C-)CTRLK

D-)CRWIG

E-)GCRWI

110) 3,5,7,11,17,31,41,59,67,83,109,127,157, ? sonucu nedir ?

A-)167

B-)159

C-)173

D-)169

E-) 179

KONU ADI : RSA Algoritması

111) Aşağıdakilerden hangisi RSA'nin ozelliklerinden birisi değildir?

A) Asimetrik bir şifreleme algoritmasıdır.
B) Güvenilirlik derecesi, şifrelemede kullanılan asal sayıların büyüklüğü ile orantılıdır.
C) RSA'da şifrelenmiş veriyi alan tarafın veriyi deşifre edebilmesi için gizli anahtarın paylaşımı gereklidir.
D) Güvenli veri paylaşımına ve sayısal imza ile kimlik doğrulaması yapılmasına olanak sağlamaktadır.
E) Sistemin hızının yüksek olması için kullanılacak anahtarın sayısal büyüklüğü önemlidir.

112)

1. Rasgele bir e sayısı üretin. e sayısı 1 ile phi arasında olmalı ve e ile phi aralarında asal olmalıdır.
2. n = p * q işlemi ile 'modulus' üretilir. (mod)
3. d*e ≡ 1 mod(phi) olacak şekilde d sayısı üretilir.
4. Çok büyük iki asal sayı üretilir. (p ve q)
5. phi = (p-1) * (q-1) üretilir. (totient)

RSA Algoritmasının sırası aşağıdakilerden hangisidir?

A) 4-2-5-1-3
B) 3-5-4-2-1
C) 4-3-2-1-5
D) 3-1-2-5-4
E) 1-4-3-2-5

113) Aşağıdakilerden hangisi RSA'nin avantajlarından birisi değildir?

A) Gizli anahtarın paylaşılmasına gerek olmadığından sistemi büyük bir depolama yükünden kurtarır.
B) Büyük sayılarla işlem yapmak zor olduğu için güvenilirliği son derece yüksektir.
C)Kablosuz ağ sistemlerinde kullanılırken band genişliğini fazlaca tüketir
Hem şifreleme hem de sayısal imza atma olanağı tanır.
D) Çok kullanıcısı olan sistemlerde güvenli veri paylaşımına olanak sağlamaktadır.
E) Hem şifreleme hem de sayısal imza atma olanağı tanır.

KONU ADI : Şifreleme Algoritmaları

114) DES'in işlem kipleriyle ilgili olarak aşağıdakilerden hangileri doğrudur?

I. Bir plaintext aynı k anahtarı kullanılarak şifreleniyorsa bu şifre öbek zincirleme kipi (CBC) dir.
II. CFB,ECB ile aynı k anahtarı kullanılarak şifrelenir.
III. CBC'de her şifrelenmiş metin y 'yi k anahtarıyla şifrelemeden önce bir sonraki şifrelenmemiş metin ile "OR"lanarak şifreler.
$y_i = e_k (y_{i-1} + x_i) , \ i \geq 1$

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

115) Vincent Rijmen ve Joan Daemen tarafından geliştirilen Rijndael algoritmasıyla ilgili aşağıdakilerden kaçı yanlıştır?

I. ARK, 10.orjinal anahtarı kullanır.
II. Plaintext 4x4 lük bir matris şeklindedir.
III. GroupField(GF) elemanları 16 bit' ten oluşan byte'lardır.
IV. Rijndael , $x^8+x^4+x^3+1$ şeklindeki 8 dereceli sabit polinomu kullanarak işlemleri gerçekleştirir.

a) 3
b) 2
c) 1
d) 4
e) Hiçbiri

116) Şifrelenecek olan açık metni (plain text) parçalara bölerek (blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrenmiş metni (cipher text) açmak içinden aynı işlemi bloklar üzerinde yapar. Bu blokların uzunluğu 64 bittir. 64 bit uzunluğunda bir anahtar alır. Ancak bu anahtarın geçerli olan uzunluğu 56 bittir çünkü 8 bit parity için harcanır.

Yukarıdaki özellikler hangi şifreleme algoritmasına aittir?

a) DES
b) RSA
c) AES
d) 3DES
e) DSA

KONU ADI :Vigenere Cipher

117) K = CIPHER anahtar texti kullanarak ‘hello world’ textini vigenere cipher yönetmiyle şifreleyiniz.
A)’GHTRCXDWSA’
B)’JMASUNPGAK’
C)’JMASZXCDER’
D)’GHTRCXDFGH’
E)’JMASSNQZAK’

118) K= ABC anahtar textini kullanarak ‘SJUTFO’ textini vigenere cipher yöntemiyle deşifre ediniz.
A)’SISTDN’
B)’SERSEM’
C)’SHSUFN’
D)’SIRSEM’
E)’SISTEM’

119) K=MUTLU anahtar texti ile ‘YENIYIL’ texti vigenere cipher yöntemiyle şifrelendiğinde baştan dördüncü karakter ne olur?
A)Z
B)U
C)V
D)Y
E)T

KONU ADI : Kriptoloji Genel

120)

Modern şifrelemenin kullanışlı olması için;

I - Orijinal metni, yani şifresiz belgeyi çözmek için gerekli olan algoritma ya da yöntem,

II - Şifresiz metni şifrelemek ve çözmek için gerekli olan anahtar,

III - Bu anahtarın ne kadar geçerli olacağını belirten süre ya da zaman aralığı.

Yukarıdakilerden hangileri gereklidir?
A) Yalnız I B) I ve III C) I ve II D) II ve III E) I , II ve III

121)
Aşağıda kripto sistemleri ile ilgili bazı tanımlar verilmiştir;
I - Şifrelenmemiş (anlaşılabilir) mesaja açık yazı denir.
II - Şifrelenmiş mesaja kapalı yazı denir.
III - Açık yazı ve kapalı yazıyı oluşturmak için bir alfabe tanımlanması gerekir.
Bu tanımlardan hangileri doğrudur?
A) Yalnız I B) I ve III C) I ve II D) I , II ve III
E) II ve III

122)
DES (Data Encrytion Standard - Veri Şifreleme Standartı) ile ilgili;
I - Blok şifreleme algoritmasıdır.
II - 64 bitlik anahtar uzunluğuna sahip olmasına rağmen 56 bit uzunluğunda simetrik kriptolama tekniği kullanan bir sistemdir.
III - 2000'li yılların başında kırılmasıyla günümüz teknoliojsi için yetersiz kaldığı görülmüştür ve itibarını kaybetmiştir.
Bu tanımlardan hangileri doğrudur?
A) Yalnız I B) I ve III C) I ve II D) I , II ve III
E) II ve III

KONU ADI :ŞİFRELEME ALGORİTMALARI

123) Aşağıdakilerden hangisi simetrik şifreleme algoritmalarının özelliklerinden biri değildir?

a) Algoritmalar olabildiğince hızlıdır.
b) Donanımla birlikte kullanılabilir.
c) Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek kolaydır.
d) Sayısal imza desteği yok.
e) Güvenli anahtar dağıtımı zordur.

124) Aşağıdakilerden hangisi DES'le ilgili yanlış bir bilgidir?

a) DES'in daha zor saldırılır hale gelmesi için 128 bit anahtar uzunluğu kullanan üçlü DES uygulaması geliştirilmiştir.
b) DES ile şifrelenmiş bir metni açmak için aynı algoritmaya şifreli metni (cipher text) aynı anahtar ile vermek yeterli değildir.
c) Kriptolojinin ve kriptoanalizin askeri olmayan çalışmalarının başlangıcı olarak DES kabul edilmektedir.
d) DES algoritması bir Block Cipher algoritmasıdır.
e) DES 64 Bitlik düz metin blokları üzerinde işlem yapmaktadır.

125) Aşağıdakilerden hangisi AES'in özelliklerinden biri değildir?

a) AES simetrik blok cipher türünde geliştirilen bir türdür.
b) AES, hızlı ve esnektir.
c) AES, 128 bitlik veri bloklarını şifrelemek için 128,196 veya 256 simetrik anahtar kullanır.
d) AES,elektronik verinin şifrelenmesi için sunulan bir standarttır.
e) Brute force saldırısı bu algoritmaya karşı bilinen tek etkili saldırıdır

KONU ADI : Stream, Autokey Cipher

126)
Ayşe Bora'ya tatile gideceği şehri söylemek için şu mesajı göndermektedir : "PALTNOVF" Bora bu mesaja ulaştığında anlamadığından Ayşe'ye telefon açıp bu mesaj için kullandığı algoritmayı ve şifreyi öğrenmek ister. Ayşe cevap olarak ; K = 7 ve algoritma olarak Autokey Cipher'ı kullanmasını ister. Bora bu mesajı aşağıdakilerden hangisi gibi çözmüştür ?

a) "IOANNINA" - YUNANİSTAN
b) "IGLOOLIG" - KANADA
c) "ISTANBUL" - TÜRKİYE
d) "ISHIGAKI" - JAPONYA
e) "ISPARTA" - TÜRKİYE

127) Ayşe Bora'ya şu mesajı göndermekteridir : "MUHHS". Bora bu mesaja ulaştığında aynı mesaja Güven de ulaşmıştır. Fakat Ayşe Bora'ya geçen mesajda kullandığı Autokey Cipher üzerinde değişiklik yaptığını ve anahtarın bir önceki karakter olmadığını, yeni anahtarın bir önceki şifrelenmiş karakter olduğunu söyler. Buna göre şifreli metin nedir ?

Örnek;		S	U
	Plaintext	18	20
K = 7	Key	7	25
	Ciphertext	25	

a) "SHHUM"
b) "SSMMH"
c) "FAMIL"
d) "FAKAT"
e) "FINAL"

128) Klasik şifreleme yöntemleri arasında anahtarı bir önceki karakter olan şifreleme algoritması nedir ?

a) Shift Cipher
b) Subsutation Cipher
c) Hill Cipher
d) Permutation Cipher
e) Autokey Cipher

KONU ADI : Şifreleme Algoritmaları / Saldırılar

129) Aşağıdakilerin hangisi asimetrik şifrelemenin özelliklerinden biri değildir?

a) Şifreleme ve deşifreleme için kullanılan anahtar farklıdır.
b) Simetrik şifrelemeye göre kırılması daha zordur.
c) Şifreleme ve deşifreleme için kullanılan anahtar aynıdır.
d) Ayrık logaritma problemine dayanır.
e) Diffie-helman anahtar değişim protokolünden çıkmıştır.

130) Olası karakter kombinasyonlarını deneyerek parolayı tahmin etmeye çalışılan atak yöntemi nedir?

a) Birthday Atak
b) Dictionary Based Atak
c) Phishing
d) Email Spoofing
e) Brute Froce

131) Aşağıdakilerden hangisi pasif atak türlerinden biri değildir?

A -Backdoor
B -Fingerprinting
C- Buffer Overflow
D-Footprinting
E- Sniffing

132) Proxy /Socks sunucularını kullanarak veya IP paketlerini editleyerek yapılan saldırı türü nedir?

c) Email Spoofing
c) Hoax mail
d) Sniffing
d) Phishing
e) Ip Spoofing

KONU ADI:Kriptoloji Genel

133) Kriptoloji de kullanılan yöntem ve algoritmalarla ilgili verilen ifadelerden hangisi yanlıştır ? a) Hash fonksiyonları çift yönlü olarak çalışır.
b)Hash fonksiyonu değişken uzunluklu veri kümelerini ,sabit uzunluklu veri kümelerine çeviren algoritmadır.
c)Açık anahtarlı şifreleme ,şifre ve deşifre işlemleri için farklı anahtarın kullanıldığı bir şifreleme sistemidir.
d)Digital imza , yüksek güvenlik gereksinimi karşılamada kullanılan tekniklerden bir tanesidir.
e)AES, 3DES ,RC4 algoritmaları simetrik şifreleme tekniğine dayanan algoritmalardır.

134) Bir şifreleme algoritmasının performansını hangi kriterlere göre belirleyebiliriz?
a)Kırılabilme süresinin uzunluğu.
b).Hepsi
c.) Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği.
d.) Algoritmanın kurulacak sisteme uygunluğu.
e.) Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı.

135) Aşağıdakilerden hangisi modern kriptografinin ilgilendiği konulardan biri değildir?
a)Mesajın istenmeyen kişiler tarafından anlaşılmaması
b)Mesajın iletilmesi sırasında değiştirilmemesi
c)Mesajın karşı tarafa ne kadar sürede gönderileceğinin belirlenmesi
d)Mesajın kimin tarafından gönderildiğinin anlaşılabilmesi
e)Mesajı gönderenin daha sonra mesajı kendisinin gönderdiğini yalanlayamaması

KONU ADI :Karışık

136)“ mesajın göndericisi ve alıcısı bir anahtar nxn lik A matrisi üzerinde anlaşmış olmalılardır. Bu A matrisini seçerken dikkat etmemiz gereken bir özellik ise MOD26 ya göre terslenebilen bir matris olmasıdır. Düz metin n uzunluğundaki bloklar şeklinde şifrelenir. “
Verilen açıklama hangi şifreleme yöntemine aittir?
a-)Hill
b-)Afin
c-)Vigenere
d-)Shift
e-)Caesar

137)Aşağıdakilerden hangisi ECC (elliptic curve cryptography) için doğru değildir?
a-) Eğri noktaları asal ise kırılması daha zordur
b-) mobile, pda, laptop gibi cihazlardada tercih edilir
c-) Performans açısından RSA’ya göre daha yavaştır
d-) Eğrinin noktaların toplam 12+1 noktadan oluşur
e-) Genel denklemi $y^2 = x^3 + ax + b$ dir

138)y2 ≡ a(mod p) eşitliğini sağlayan a değerleri Zp’de ….. olarak tanımlanır.
a-) quadratic residue
b-) asal
c-) primatif eleman
d-) private key
e-) primitif kök

KONU ADI : DES- 3DES- AES

139)Triple-DES ile ilgili aşağıdakilerden hangisi doğrudur?

a)DES'e göre daha hızlı çalışır.
b)DES algoritmasından önce kullanılmaya başlamıştır.
c)58 bit'lik bloklar kullanır.
d)DES'e göre 3 kat daha fazla işlemci gücü gerektirir.
e)DES genellikle insansız hava araçları sanayisinde kullanılmaktadır.

140)AES ile DES'i karşılaştırdığımızda aşağıdakilerden hangisi iki algoritmada da ortak olan özelliklerdendir?

a)Her iki algoritmanın da anahtar uzunlukları 56 bit'dir.
b)Her ikisi de 64 bit'lik bloklar kullanmaktadır.
c)Her iki algoritma da güvenli olarak kabul edilmektedir.
d)Her ikisi de Rijndael algoritmasının modifiye edilmiş versiyonlarıdır.
e)İkisi de Simetrik şifreleme algoritmalarına dahildir.

141)Aşağıdakilerden hangisi AES algoritmasının özelliklerindendir?

a)Asimetrik şifreleme algoritmasına dahildir.
b)Blok uzunluğu 512 bit'dir.
c)Daha önce kırıldığı için güvensiz bir algoritma olarak tanımlanmaktadır.
d)AES, Feistel mimarisini kullanmaktadır.
e)AES algoritmasına göre anahtar uzunlukları 128, 192 ve 256 bit olarak değişebilir.

KONU ADI :RSA Şifreleme / Şifreleme çeşitleri

142)Aşağıdakilerden hangisi tarihten günümüze kadar, bazı şifreleme tekniklerinden değildir ?

A)Sezar şifrelemesi
B)Rotor makinesi (Enigma)
C)kriptoanaliz (cevap)
D)Açık anahtarlı şifreleme
E)Veri gizleme teknikleri

143)RSA kriptosisteminde anahtar oluşturma algoritması için aşağıdakilerden hangisi yanlıştır ?

A) A'nın açık anahtarı d ; A'nın gizli anahtarı ise (n, e) olur.
B) $n = pq$ ve $\varphi = (p - 1)(q - 1)$ değerlerini hesaplanır.
C) $1 < e < \varphi$ ve gcd $(e, \varphi) = 1$ olacak şekilde rastgele bir e sayısı seçilir.
D) Öklid algoritması kullanılarak, $1 < d < \varphi$ ve $ed \equiv 1 \pmod{\varphi}$ koşulunu sağlayan d sayısı hesaplanır.
E) ˙İki tane farklı rastgele ve yaklaşık aynı uzunlukta olan p ve q asal sayıları seçilir.

144) Anahtar oluşturması: p = 7 ve q = 19 sayıları kullanılarak yapılan RSA kriptosisteminde gizli anahtar aşağıdakilerden hangisidir? (e = 5)

A) d = 65
B) d= 48
C) d= 58
D) d= 45
E) d= 85

KONU ADI :Karışık

145) Aşağıdakilerden hangisi simetrik anahtar kullanan algoritmalardan değildir?

A-)DES
B-)Blowfish
C-)RSA
D-)3DES
E-)AES

146) gcd(658,1764) işleminin sonucu kaçtır?

A-) 14 B-) 16 C-) 44 D-)34 E-)28

147) Z7 nin quadratic resudie(QR) ve nonquadratic resudie(NQR) değerleri nelerdir?
A) QR=2,3,4 ve NQR=1,5,6
B) QR=1,5,6 ve NQR=2,3,4
C) QR=1,3,5 ve NQR=2,4,6
D) QR=1,2,6 ve NQR=3,4,5
E) QR=1,2,4 ve NQR=3,5,6

KONU ADI : Slovay-Strassen

148) Aşağıdakilerden hangisi Slovay-Strassen testinin özelliklerinden değildir ?

A-)Miller Rabin testine göre daha yavaştır.
B-)Açık anahtar kriptografisinde kullanılmış ilk testtir.
C-)Güçlü asallık testi olarak bilinir.
D-)Slovay-Strassen Algoritmasında n-sayısının asallığını bulmak için Jacobi Semboli kullanılmaktadır.
E-)Olası asallık testlerinden biridir.

149)Aşağıdaki Slovay Strassen algoritma adımlarından hangisi yanlıştır?

A-) Eğer j¹J(a,n) ise n kesin olarak asaldır ve testi geçer.
B-)Eğer gcd(a,n)¹1 ise o zaman n asal değildir ve testi geçemez.
C-) j°$a^{(n-1)/2}$ (mod n) hesaplanır.
D-) J(a,n) hesaplanır.
E-)n'den daha küçük rasgele a-sayısı seçilir.

150)Slovay Strassen testi, olası asallık testlerinden hangisine daha çok benzerdir?

A-)Fermat Testi
B-)Miller-Rabin Testi
C-)Lehmann Testi
D-)Frobenios Testi
E-)Bileşik Testler

KONU ADI :Elliptic

151)Aşağıdakilerden hangisi ECC (Elliptic Curve Cryptography) için doğru bir ifade değildir?

A-)Asimetrik şifreleme algoritmalarından bir tanesidir
B-)1985'te Neal Koblitz ve Victor Miller tarafından geliştirilmiştir.
C-)RSA algoritmasına göre şifrenin kırılması çok daha kolaydır.
D-)Bant genişliği DSA(Digital Signature Algorithm) ve RSA'ya göre daha azdır.
E-) RSA'ya göre daha düşük anahtar değerleriyle güvenliği sağlamaktadır.

152)ECC (Elliptic Curve Cryptography) şifreleme algoritmasını diğer açık anahtar şifreleme algoritmalarından ayıran en büyük özelliği aşağıdakilerden hangisidir?

A-) Daha düşük anahtar uzunluğu kullanması
B-) Bant genişliğini daha fazla kullanması
C-)Büyük sayılarla işlem yapması
D-) Asimetrik şifreleme yapıyor olması
E-)Hız açısından yavaş olması

153) Elliptic Curve Kriptoloji için; E: $y^2 = x^3 + ax + b$; (x,y) IR x IR; ->point at infinity, P->(x1,x2); P + = + P eşitliği aynı zamanda aşağıdakilerden hangisine eşittir?

A-)x1
B-)x2
C-)a
D-)b
E-)P

KONU ADI : Ciphers

154)Z29 da S= 2 3 matrisi kullanılarak Hill Cipher ile şifrelenen x metninin
4 5
ciphertexti “AUPD” ise plaintexti aşağıdakilerden hangisidir?

A) GECE
B) MVAİ
C) GREİ
D) GZEİ
E) AIKM

155) Z26 da Affine Cipher ile şifrelenmiş metnin ciphertexti “GCRWI” ise plaintext aşağıdakilerden hangisidir ?

A) MONEY
B) HONAY
C) MIRKS
D) MEDAM
E) MANTH

156) Z29 da K= “KALEM” anahtari kullanılarak Vigerene Cipher ile şifrelenmiş metnin Ciphertexti “OÜBÇM” ise plaintexti nedir?

A) DOZİN
B) DUREK
C)DANİZ
D)DERAN
E)DÜNYA

KONU:ALGORİTMALAR

157) Miller Rabin Algoritması'nda n=41 için,
(2^k).m formülüne göre m sayısının özelliği nedir? Değerini bulunuz.
A) M, asal sayı olmalı ve m=3
B) M, tek sayı olmalı ve m=5
C) M, çift sayı olmalı ve m=4
D) M, tek sayı olmalı ve m=5
E) M, tek sayı olmalı ve m=7

158) RSA algoritmasında n=p.q formülündeki p ve q değerleri için hangisi doğrudur?
A) İkisi de asal değildirler.
B) Birinin asal olması yeterlidir.
C) Aralarında asal olmalıdırlar.
D) Her ikisi de asal olmak zorundadır.
E) Hiçbiri

159) Z7 nin quadratic resudie(QR) ve nonquadratic resudie(NQR) değerleri nelerdir?
A) QR=2,3,4 ve NQR=1,5,6
B) QR=1,5,6 ve NQR=2,3,4
C) QR=1,3,5 ve NQR=2,4,6
D) QR=1,2,6 ve NQR=3,4,5
E) QR=1,2,4 ve NQR=3,5,6

KONU ADI :Karışık

160)GCD(256,186)=? öklide göre hesaplayınız.
A)18 B)12 C)14 D)15 E)11

161)11 ve 7 ün aralarýnda asal olup olmama testini gcd hesabıyla yaparak 1 'in yanındaki son çarpanı bulunuz.
A)2 B)4 C)3 D)1 E)5

162)Aşağıdakilerden hangisi cipher türlerinden değildir?
A)Hill B)Affine C)Combination D)Stream E)Permutation

CEVAP ANAHTARI

1. A
2. A
3. E
4. A
5. A
6. E
7. E
8. B
9. C
10. A
11. E
12. C
13. E
14. C
15. C
16. C
17. E
18. A
19. D
20. A
21. C
22. E
23. D
24. E
25. B
26. D
27. C
28. E
29. A
30. A
31. C
32. A
33. A
34. A
35. A
36. E
37. A
38. A
39. E
40. C
41. C
42. D
43. B
44. C
45. A
46. A

47. A
48. A
49. E
50. E
51. E
52. E
53. E
54. A
55. E
56. A
57. E
58. E
59. E
60. A
61. C
62. A
63. A
64. A
65. A
66. C
67. E
68. D
69. D
70. A
71. A
72. E
73. A
74. C
75. C
76. A
77. E
78. E
79. E
80. A
81. A
82. C
83. C
84. A
85. B
86. A
87. A
88. A
89. E
90. C
91. E
92. B
93. A
94. D

95. A
96. A
97. A
98. A
99. A
100. C
101. A
102. D
103. E
104. A
105. E
106. A
107. B
108. A
109. E
110. E
111. C
112. A
113. C
114. E
115. A
116. A
117. E
118. E
119. E
120. E
121. D
122. D
123. C
124. B
125. C
126. C
127. E
128. E
129. C
130. E
131. C
132. E
133. A
134. B
135. C
136. A
137. C
138. A
139. D
140. E
141. E
142. C

143. A
144. A
145. C
146. A
147. E
148. C
149. A
150. B
151. C
152. A
153. E
154. A
155. A
156. E
157. B
158. D
159. E
160. E
161. B
162. C