1-) Kriptoloji kelimesi , final anahtar kelimesi kullanılarak Auto Key Chipher ile şifrelenmesi durumunda , şifreli metin aşağıdakilerden hangisidir ?
A)PZVPEYCWYB
B)DXTDEYBWYB
C)PXTDEABWFG
D)KEQDAACXOP
E)DXCWQECZUY

2-) Auto Key Chipher ile şifrelemede kullanılan matematiksel fonksiyon hangisidir?
A)e(x) = x . z mod26
B)e(x) = x - z mod26
C)e(x) = x + z mod26
D)e(x) = x / z mod26
E)e(x) = x % z mod26

3-)Aşağıdakilerden hangisi rsa şifreleme algoritması methodlarından değildir?
A-DecryptValue
B-EncryptValue
C-StringValue (doğru cevap)
D-ToString
E-ToXmlString

4-) LegalKeySize algoritmasının özelliği nedir ?
A-anahtar değişimi algoritmasının ismini belirtir.
B-şifreleme ve deşifreleme için kullanılacak anahtarların kaç bitten oluşacağını gösterir.
C-bu algoritma tarafından desteklenen geçerli anahtarlar bit olarak büyüklüğünü gösterir. (doğru cevap)
D-imzalama için kullanılacak algoritmanın adını gösterir.
E-iki nesnenin birbirine eşit olup olmadığını test eder.

5-)
p=8101 ve a=6 ise
a x = 7531 (mod p) probleminde x'i pohlig-hellman algoritmasını uygulayarak bulunuz.
A)6688 B)6671 C)6689 D)6686 E)6690

6-) Ayrık logaritma probleminin çözümü için bir alternatif sunan ve çinli kalanlar teoremini kullanan algoritma aşağıdakilerden hangisidir?
A) Pohlig-Hellman
B)Miler-Robin
C)El-Gamal
D)Sovolay-Strassen
E)Shank's

7-)AES algoritması, 128 bitlik veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreleyen bir algoritmadır. 192 bitlik anahtar kullanımında algoritmadaki döngü sayısı kaçtır?

A)10 B)11 C)12 D)14 E) 16

8-)

1-Anahtar bit uzunluğu kısa
2-S box'ların sabit olması
3-Şifrelenecek her blok için aynı anahtarın kullanılması
Yukarıdakilerden hangisi veya hangileri DES'in kırılma nedenlerinden değildir?

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

9-) Index Calculus çözme yöntemine göre n sayısının n-1 sayısının çarpanlarının toplamı m ise ve bu çarpanlardan elde edilen en yakın sayı da k ise mod n için kaç deneme yapılırak şifre çözülür ?

A-) m B-) m*n+k C-) m +(n-k) D-) n*(m-k) E-) m*k-n

10-) Index calculus algoritması kaç adımda problemi çözer?

A-)2 B-)3 C-)4 D-)5 E-)6

11-)

I.n
II.b
III.p
IV.q
V.a

RSA Cryptosystem'de yukarıdaki değişkenlerden hangisi ve hangileri private olmalıdır?

A-Yalnız I B-I ve II C-II,III ve IV D-III,IV ve V E-Hepsi

12-)p=11, q=17, b=3 ve x=6 değerleri için RSA Cryptosystem'de şifrelenmiş veriyi ($y=e_k(x)$) bulunuz.

A-23 B-29 C-31 D-37 E-41

13-)RSA Cryptosystem ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A-a ve b, mod(φ(pxq))'ya göre aralarında asal olmalıdır.
B-a ve p, mod(n)'ye göre aralarında asal olmalıdır.
C-a ve q, mod(φ(bxp))'ye göre aralarında asal olmalıdır.
D-a ve b, mod(pxq)'ya göre aralarında asal olmalıdır.
E-b ve n, mod(φ(axq))'ya göre aralarında asal olmalıdır.

14-)

int k,q,k>0,q odd (n-1)=2^kq
if a^q=1(mod n) return("maybe prime")
for j=0 to k-1 do
if(a^2*q mod n=n-1) return("maybe prime")
return ("composite")

15-) Algoritma hangisine aittir?
a) Solovay Strassen
b)Miller Rabin
c) Shanks Algoritması
d)Diffie Helman Anahtar Değişim Protokolü
e)Pohlig-Hellman Algoritması

16-)Aşağıdakilerden hangisi Miller Rabin testinin diğer testlerden daha iyi olma nedenlerinden biri değildir?

a)Fermat testi, Carmichael sayılarını bulmakta zayıf kalmaktadır.
b)Solovay&Strassen testi, çalışma zamanı olarak daha fazladır.
c)Solovay&Strassen testi, Jacobi sembol hesaplamaları yüzünden uygulanması daha zordur.payıyla daha gerçeğe yakın sonuçlar sunmaktadır.
d)Miller&Rabin testi en kötü şartlarda bile (worst case) en fazla diğerleri kadar çalışma zamanına ihtiyaç duymaktadır.
e)Miller Rabin testi olası((probabilistic) asallık testidir.

17-)Aşağıdakilerden hangisi kriptografik hash fonksiyonudur?
A-DES
B-IDEA
C-MD5
D-RSA
E-DES

18-)Aşağıdakilerden hangisi en güçlü hash fonksiyonu olarak değerlendirilmektedir?
A-SHA-1
B-MD5
C-SHA-256
D-SHA-128
E-SHA-512

19-)g sayıda harfe sahip bir alfadebeki x metnini, K anahtarıyla şifrelerken e(x) = (x+K)modg, şifrelenmiş y metnini çözerken çözerken de d(y) = (y-K)modg formüllerini kullanan temel şifreleme algoritması aşağıdakilerden hangisidir?

A) Affine Cipher
B) Hill Cipher
C) Shift Cipher
D) substitution Cipher
E) Vigenere Cipher

20-) Harf sayısı 26 olan bir alfabede x metninin harflerinin sayısal karşılıkları sırasıyla 7, 4, 11, 11, 14'tür. Shift Cipher ile K=15 anahtarıyla şifrelersek, şifrelenmiş metnin harflerinin sayısal karşılığı sırasıyla aşağıdakilerden hangisi olur?
A) 13, 5, 8, 2, 6
B) 17, 14, 14, 14, 0
C) 19, 22, 0, 0, 3
D) 21, 18, 25, 25, 2
E) 22, 19, 0, 0, 3

21-)"HELLO WORLD" metnini verilen anahtara göre substitution cipher algoritmasından geçirirsek elde edeceğimiz şifreli metin ne olur?

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

A.EGXXF NFQXZ
B.EOXXG VGDXZ
C.EOIIM VMDIZ
D.CGIIT NTDIZ
E.CJIIT VTGIZ

22-)Çalışma uzayımız İngiliz alfabesinin karakterleri olmak üzere substitution cipher de anahtarımız ne olur.

A. 25
B. 26!
C. 25!
D. 26
E. 12 x 26

23-) Shanks Algoritmasının çözüm aradığı denklem aşağıdakilerden hangisidir?

A-√((a-1) mod p)
B- √(a mod p)
C-√(a mod (p-1))
D-√((a+1) mod p)
E-√(p mod a)

24-) Shanks Algoritmasının çözüm aradığı ayrık logaritma denkleminde yer alan "a" değerinin alabileceği değer aralığı hangisinde doğru olarak verilmiştir?

A- $0 \leq a \leq p-1$
B- $0 \leq a \leq p-2$
C- $0 \leq a \leq p+1$
D- $0 \leq a \leq p+2$
E- $0 \leq a \leq p$

25-) Eliptik Eğri Şifrelemesi ile ilgili olarak aşağıda verilen bilgilerden hangisi yanlıştır?

A)Temelini Eliptik Eğri Ayrık Logaritma Problemi oluşturmaktadır.
B)Victor Miller ve Neal Koblitz tarafından ilk kez Kripto Sistem için temel alınması önerilmiştir.
C)Çalışma hızı ve hafıza ihtiyacı bakımından RSA ile karşılaştırıldığında daha yavaş çalışmakta olduğu ve daha çok hafıza ihtiyacı duyduğu görülmektedir.
D)Sıkça kullanılan Açık Anahtar Kripto Sistemleri arasında bulunmaktadır.
E)En önemli özelliği diğer açık anahtar şifreleme sistemlerinin güvenliğini daha düşük anahtar değerleriyle sağlayabilmesidir.

26-) Eliptik eğrilerde ayrık logaritma kullanımına ilişkin olarak $y2 = x3 + 9x + 17$ şeklinde F23 için tanımlanan bir eliptik eğride Q = (4,5) noktası için P = (16,5) noktasına göre ayrık logaritma logP(Q) nedir?
(logP(Q): P tabanında Q logaritmasının değeri)

A)13 B)9 C)19 D)16 E)20

27-) Tanımlanırken çarpımsal bir grupta ayrık logaritmayı hesapladığı ve FP* sonlu cismi için Çinli Kalanlar Teoremine dayanarak uyarlandığı belirtilen algoritma aşağıdakilerden hangisidir?

A)Bebek ve dev adımlar
B)Index Calculus
C)Shanks
D)Pohlig hellman
E)Elliptic Curve

28-) Pohlig Hellman Algoritması ile 7531=6x (mod 8101) şeklinde verilen denklem çözülmek istendiğinde x' in hangi durumu için denk oldukları görülebilir?

A)6689
B)3789
C)6300
D)1234
E) 5240

29-)Çalışma uzayının x^3 +x+1 olduğunu kabul edin.Finite fielde göre (x^2 +x)(x^2) çarpım sonucunun bu uzaya göre tersi nedir?
A-x^2
B-x^2 +1
C-x^2 +x
D-1
E-x

30-) Finite Field'a göre aşağıdakileden hangisi polinom uzayı olarak seçilemez?
A-x^3 +x+1
B-x^3 +x^2 +1
C-x^2 +5
D-x^4 +x 3 +5
E-x^3 +1

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

A) q=n*p dir.
B) RSA ya göre daha yüksek anahtar değeri taşır.
C) Temel birimler eliptik eğri üzerindeki noktalardır.
D) y2=x3+ax+b ye dayanır.
E) İşleyişi RSA'ya benzerdir

32-) Aşağıdakilerden hangisi Eliptik Eğri Şifreleme(ECC)'nin RSA ve DiffieHellman'dan farklarından biri değildir?
A)Daha hızlı çalışır.
B)Kırılması daha zordur.
C)Daha çok bellek kullanır.
D)Aynı anahtar boyutu için RSA ve DiffieHellman'a göre daha güvenlidir.
E)163 bit ECC şifreleme 1024 bit RSA şifreleme ile denktir.

33-) Asal çarpanlarına ayırma zorluğuna dayanan şifreleme algoritması hangisidir?

A-) Shift Chipper
B-) Gold Wasser
C-) El-Gamal
D-) Miller Robin
E-) RSA

34-) El-Gamal yönteminde şifrenin çözülme zorluğu neye dayanır?

A-) Private keyin çözülme zorluğuna
B-) Discrete logaritma probleminin çözülme zorluğuna
C-) Şifreleme protokolünde kullanılan anahtar sayısı
D-) Şifreleme protokolünde kullanılan bit sayısı
E-) Hiçbiri

35-) Permutation Cipher ile şifrelenmiş TÜRKİYEM kelimesinin şifrelenmiş metni KTÜRMİYE olduğuna göre, k anahtarı aşağıdakilerden hangisidir ?
A - 4123
B - 3214
C - 1342
D - 2314
E - 2143

36-)KRİPTOLOJİ kelimesinin Permutation Cipher ile 51432 anahtarı ile şifrelenmiş metni aşağıdakilerden hangisidir ?
A - TKPİRİOJOL
B - TPKRİİJOLO
C - RKTİPLOİOJ
D - RPKİTLJOOİ
E - PRTİKJLİOO

37-) Shift Chiper'da "KHAN" kelimesi key "k=19" ile şifrelendiğinde sonuç ne olur?
A-DASG
B-DAUG
C-DBTG
D-EBUHC
E-DATG

38-) Shift Chiper yöntemi için aşağıdakilerden hangisi yanlıştır?
A-Şifreleme matris yoluyla yapılmaz.
B-Şifrelenecek metin ile oluşan şifre aynı karakter sayısına sahiptir.
C-Şifreleme denklemi:ek(x)=(y-k) mod 26'dır.
D-Şifre çözme denklemi:dk(y)=(y-k) mod 26'dır.
E-Basit bir şifreleme yöntemi değildir.

39-) Shift Chiper'da "KHAN" kelimesi key "k=19" ile şifrelendiğinde sonuç ne olur?
A-DASG
B-DAUG
C-DBTG
D-EBUHC
E-DATG

40-) Shift Chiper yöntemi için aşağıdakilerden hangisi yanlıştır?
A-Şifreleme matris yoluyla yapılmaz.
B-Şifrelenecek metin ile oluşan şifre aynı karakter sayısına sahiptir.
C-Şifreleme denklemi:ek(x)=(y-k) mod 26'dır.
D-Şifre çözme denklemi:dk(y)=(y-k) mod 26'dır.
E-Basit bir şifreleme yöntemi değildir.

41-) Index Calculus çözme yöntemine göre n sayısının n-1 sayısının çarpanlarının toplamı m ise ve bu çarpanlardan elde edilen en yakın sayı da k ise mod n için kaç deneme yapılırak şifre çözülür ?

A-)n*k B-) n*m+k C-) m +(n-k) D-) n*(m-k) E-)n+(m-k)

42-) Index calculus algoritması kaç adımda problemi çözer?
A-)3 B-)7 C-)5 D-)4 E-)6

43-)DES algoritmasında parity(kontrol) bit uzunluğu kaç bittir?
A-9
B-12
C-8
D-16
E-10

44-) Triple DES algoritmasında Key uzunluğu kaç bittir?
A-56
B-112
C-192
D-128
E-168

45-) Diffine –Helman Anahtar değişim protokolünde p=17 ve α=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}

46-) Diffine –Helman Anahtar değişim protokolünde p=17 ve α=3 ise Alice 15' i seçiyor Bob ise 13' ü. Buna göre aralarındaki ortak anahtar aşağıdakilerden hangisidir?

A- 10
B- 9
C-12
D-11
E- 6

47-) Diffine –Helman Anahtar değişim protokolünde p=17 ve α=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}

48-) Diffine –Helman Anahtar değişim protokolünde p=17 ve α=3 ise Alice 15' i seçiyor Bob ise 13' ü. Buna göre aralarındaki ortak anahtar aşağıdakilerden hangisidir?
A- 12
B- 9
C- 10
D- 11
E- 6

49-)Aşağıdaki algoritmalardan hangisi hash algoritması değildir?
A-MD5
B-SHA-1
C-DES
D-SHA2
E-MD6

50-)Aşağıdakilerden hangisi hash fonksiyonun uygulamalarından değildir?
A-Dosyanın bütünlük kontrolü
B- Saklanan şifrelerin güvenliği
C- Uzun mesajları imzalamak
D- Mesaj doğrulama kodları
E- Bir dosyanın boyutunu küçültme

51-) Diffine –Helman Anahtar değişim protokolünde p=17 ve α=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}

52-) Diffine –Helman Anahtar değişim protokolünde p=17 ve α=3 ise Alice 15' i seçiyor Bob ise 13' ü. Buna göre aralarındaki ortak anahtar aşağıdakilerden hangisidir?
A- 10
B- 9
C- 5
D- 7
E- 6

53-)Aşağıdakilerden hangisi AES'de kullanılan işlem basamaklarından biri değildir?
A-ShiftRow Dönüşümü
B-MixColoumn Dönüşümü
C-ByteSub Dönüşümü
D-ChangeKey Dönüşümü
E-AddRound Dönüşümü

54-)Aşağıdakilerden hangisi asimetrik şifreleme özelliklerinden biri değildir?
A-Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.
B-Anahtarı kullanıcı belirleyebilir.
C-Anahtar uzunlukları bazen sorun çıkarabilir.
D-Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması gerçekleşebilir.
E-Asimetrik şifreleme algoritmalarında anahtar ile şifre çözme anahtarı aynıdır.

55-)$3.x \equiv 4 \bmod 7$ ise x aşağıdakilerden hangisidir?
a- 3 mod 7
b-5 mod 7
c- 6 mod 7
d- 2 mod 7
e- 4 mod 7

56-) Shift Cipher yöntemine için aşağıdaki ifadelerden hangisi yanlıştır?
a-İlkel şifreleme yöntemidir.
b-Şifrelenmek istenen metindeki karakterler anahtar kadar kaydırılır.
c-Şifreleme denklemi : $ek(x) \equiv (x+k) \bmod 26$ 'dır.
d-Şifre çözme denklemi: $dk(y) \equiv (y-k) \bmod 26$ 'dır.
e-Anahtar olarak 4x4 boyutunda kare matris kullanır.

57-) Z5 'nin quadratic residueleri aşağıdakilerden hangisinde tam olarak verilmiştir?
a-(1,4)
b-(2,4)
c-(3,5)
d-(0,2)
e-(2,3)

58-) 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^(-115)
C- 2^(-112)
D- 2^(-121)
E- 2^(-118)

59-)Aşağıdakilerden hangisi bir Olası (probabilistic) Asallık Testi değildir?

A-Fermat
B-Slovay&Strassen
C-Euler

D-Frobenius
E-Miller&Rabin

60-) Aşağıdakilerden hangisi Index-calculus yöntemindeki 4. adımda B.α^r ifadesini S deki elemanların çarpımı cinsinden yazılamadığında yapılan adımdır?
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.

61-) Index Calculus Yöntemi çözüm basamakları toplam kaç basamaktan oluşur?
A)4 B)2 C)5 D)3 E)1

62-) Aşağıdakilerden hangisi Diffie Hillman şifreleme yönteminin özelliklerinden değildir?
A- Açık anahtar şifrelemesi kullanır
B- Ayrık logaritma zorunluluğu bulunmaktadır
C- İkiden fazla kişi anahtarı değiştiremez <-- cevap
D- RSA bu algoritmadan sonra tasarlanmıştır
E- Taraflar birbirlerini hususi anhtarlarını bilmezler

63-)STREAMCIPHER plain texti BUFHEGFCDATM keyi kullanılarak stream cipher şifreleme yöntemine göre şifrelenirse elde edilen cipher text aşağıdakilerden hangisidir?

A- CNWELHSSKXHD
B- TNWLESHKSHXD
C- YCNELESKHSHX
D- WNLETSHKXDHS
E- UNLWEHSKSHDX

64-) KRIPTOLOJI plain texti TCRMLCAFHK keyi kullanılarak stream cipher şifreleme yöntemine göre şifrelenirse elde edilen cipher text aşağıdakilerden hangisidir?

A- DTZBEQLTQS
B- BZTEBQLQTS
C- MZTQLQTEBT
D- ATZCEBQTEQ
E- CTZEBQLQTS

65-) Hangisi AES algoritmasını oluşturan döngülerin sayısıdır?
A)9
B)4
C)7
D)8
E)10

66-)AES algoritmasında bir döngü kaç bitle başlar ve kaç bitle sonlanır?

A)128-256
B)128-512
C)128-128
D)256-256
E)256-512

67-)
1) ElGamal
2) Diffie-Hellman
3) Dijital imza
Yukarıdakilerden hangileri ayrık logaritma kullanımı yapan şifrelemedir ?
A-Sadece 1
B-1,2
C-1,2,3
D-Sadece 2
E-Sadece 3

68-) Ayrık logaritma için hangisi yanlıştır ?
A-Açık anahtar paylaşımı için araştırmalar sonucunda modül yapısınının matematiksel özelliğini kullanılması ile oluşturulan bir sistemdir.
B-En önemli örnekleri ElGamal, Diffie-Hellman ve Dijital imzadır.
C-Ayrık logaritma problemi logg b 'nin genel çözümünü hesaplayan hızlı ve verimli bir algoritma bilinmemektedir.
D- Polinom zamanda çözülemez.
E-Ayrık logaritma ile yapılan şifrelemelerin kırılması kolaydır.

69-)Aşağıdakilerden hangisi Euler fonksiyonu için yalnıştır?

A-Phi fonksiyonu olarak da bilinir.
B-Bir tam sayının o sayıdan daha büyük ve o sayı ile aralarında asal olan sayma sayı sayısını belirten fonksiyondur.
C-RSA kriptografi sisteminde de kilit rol oynamaktadır.
D-Totient fonksiyonu olarak da bilinir.
E-İsviçreli matematikçi Leonhard Euler tarafından bulunmuştur.

70-)24 sayısının totient fonksiyonu φ (24) aşağıdakilerden hangisidir?
A-3
B-9
C-8
D-7
E10

71-) El Gamal şifreleme yöntemi aşağıdakilerden hangisini ya da hangilerini kullanır?
|-PublicKeyCryp
||-PrivateKeyCryp
|||-PermutationCipher

A-Yalnız | ****
B-Yalnız ||
C-Yalnız |||
D-|,||

E-|-||-|||

72-) Plaintext=""kural"" ,Anahtar =(32514), Ciphertext=?
A-lakru
B-alkur
C-rulka ****
D-uralk
E-lakur"

73-) Hangisi simetrik sifreleme ve Des modlarından degildir?
A.)CBC
B:)ECB
C:)PCBC
D:)OFB
E:)AES

74-) AddRoundKey'de kaç bitlik anahtar kullanılır?
A.) 32
B)128
C)64
D)256
E)1024

75-) Aşağıdakilerden hangisi DES(Data Encryption Standard)'in özelliklerinden biri değildir?
A-Blok şifreleme yapar.
B-Simetrik şifreleme algoritmasıdır.
C-Açık anahtar şifrelemeye örnektir.
D-DES-3 DES'e göre daha güçlü bir algoritmadır.
E-Brute Force ataklarına karşı güvensizdir.

76-) Aşağıdakilerden hangisi RSA için yalnıştır?
A-Açık anahtar şifrelemeye örnektir.
B-RSA için bir ortak anahtar bir de özel anahtar gerekir.
C-Simetrik şifreleme algoritmasıdır.
D-Sayısal imza teknolojisinde kullanılabilir.
E-Çarpanlara ayırma probleminin zorluğuna dayanır.

77-) ""defend"" kelimesini k = (5,7) olarak Affine Cipher'a göre şifreleyiniz. Şifrelenmiş metin aşağıdakilerden hangisi olur?
A- wbgbuw
B- xchcvx
C- defend
D- uzezsu
E- Şifrenelenemez.

78-) Bir metin Affine Cipher ile şifrelenmeye çalışılıyorsa ve kullanılan alfabede 26 harf varsa key ikilisi (a,b) kaç farklı değer olabilir?

A- 12, 26
B- 26, 26
C- 26, 12
D- 12, 12
E- mod26, mod26

79-)Aşağıdakilerden hangisi yanlıştır ?
A)DES bruto force ile kırılmıştır.
B)Simetrik şifreleme yöntemlerinde aynı anahtar ile hem şifreleme hem de çözümleme yapılır.
C)Simetrik anahtar şifrelemede , verilerin daha güvenli gönderilmesi için public anahtar şifreleme ortaya çıkmıştır.
D)DES 64 bit olarak tanımlanmıştır , ama 50 bitlik anahtar kullanılmıştır.
E)DES kırıldıktan sonra AES kullanılmaya başlanmıştır.

80-) Hash algoritması ile ilgili hangisi doğrudur ?
I)Algoritmanın ürettiği sonucu tekrar asıl metne dönüştürmek mümkün değildir.
II)Hash algoritması md5 veya sha olabilir.
III)Bilgisayar ağlarında , internet trafiğinde ya da kimlik doğrulamada kullanılabilir.
IV)Keyfi uzunluktaki bir mesajdan 128 bit uzunluğundaki bir mesaj ortaya çıkar.
A) I,II,III B)II,III,IV C)Yalnız 2 D)II ve III E)Hepsi

81-)ϕ(143) Euler Fonksiyonu göre nedir ?
A-90
B-150
C-110
D-130
E-120

82-)3 des algoritmasında kullanılan anahtar kaç bittir?
A-64
B-168
C-128
D-108
E-56"

83-) Bir algoritmayı kırmak için bulunan en iyi algoritma aşağıdakilerden hangisidir?
A-Brute Force
B-One Time Pad
C-RSA
D-DES
E-AES

84-) Private Key kriptografi ile ilgili aşağıdakilerden hangisi yanlıştır?
A-Anahtar çift taraflıdır
B-Anahtarı karşı tarafa yönlendirmek zordur.

C-Anahtar açıktır ve herkesin erişimine açıktır
D-Şifreleyen taraf ile şifreyi çözen taraf aynı anahtarı kullanır.
E-Simetrik şifreleme tekniğidir.

85-)Aşağıdaki protokollerden hangisi kriptografiyi kullanmaz?
A-HTTPS
B-SSH
C-TELNET
D-SFTP
E-IPSEC

86-)Aşağıdakilerden hangisi açık anahtar şifreleme algoritması değildir ?
A-Des
B-Twofish
C-Aes
D-Rsa
E-Rc6

87-)Aşağıdakilerden hangisi asimetrik şifrelemenin özelliklerinden birisi değildir?
A)Diffie Helman anahtar değişim protokolünden çıkmıştır.
B)Ayrık logaritma problemine dayanır.
C)Şifreleme anahtarı ile şifre çözme anahtarı birbirinden farklıdır.
D)Şifrelemeyi yapan anahtara açık anahtar denir.
E)Asimetrik şifreleme güvenlik açısından simetrik şifrelemeye göre daha zayıftır.

88-)α, ß ve p bilinmesine rağmen problemin çözülememesi aşağıdakilerden hangisini tanımlar?
A)Rsa Cryptosystem
B)Shanks Algoritması
C)Ayrık Logaritma problemi
D)Jacobi Symbol
E)Miller-Robin

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

90-)..... 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) vignere cipher
b)aes
c)affline cipher
d)hill cipher
e) 3 des

91-)DES algoritmasında 1 den 16 ya kadar dönen döngüde Ri' lerin elde edilmesi için kullanılan formül aşağıdakilerden hangisidir

a) R i = L i – 1 ⊕f(Ri-1 , K i)
b) R i = L i – 1 ⊕f(K i)
c) R i= L i – 1
d) R i =R i - 1
e) R i = R i - 2

91-)z13 'de aşağıdakilerden hangisi quadratic residue'dur?

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

92-) Asal çarpanlara ayırma zorluğuna dayanan şifreleme algoritması hangisidir ?

A-) EL-GAMAL
B-) AES
C-) RSA
D-) 3-DES
E-) Miller Rabin

93-) Alfabe : a b c d e f g h
Anahtar : f d e a c h g b
Yukarıda verilenlere göre "baba dede" nin Substitution Cipher ile şifrelenmiş hali nedir?

A) ecec fcfc
B) cdcd acac
C) efef ghba
D) fdac gfcf
E) dfdf acac

94-)4x≡9 mod14 denkliğini sağlayan x değerlerini bulunuz.

.

a-) x≡2 mod14
b-) Çözümü yoktur
c-) x≡3 mod14
d-) x≡4 mod14
e-) x≡5 mod14

95-)P(x1, y1) ve Q(x2, y2) noktalarını içeren bir eliptik eğride, bu noktaların birbirine eşit olmadığı durumlarda aşağıdaki eğim formüllerinden hangisi kullanılır?

A) (y2-y1)/(x2-x1)
B) (y1-y2)/(x2-x1)
C) (x2-x1)/(y2-y1)
D) (x2-x1)/(y1-y2)
E) (x1-x2)(y1-y2)

96-) (2508/1115) Jacobi kullanarak Legendre sembolünü hesaplayınız.

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

97-) Jeromi sembolunde (2|n) = -1 ise ve n = 3 ya da aşağıdaki değerlerden hangisi olabilir?
A-)5mod(8)
B-)6mod(8)
C-)7mod(8)
D-)4mod(8)
E-)3mod(8)

98-) Shift Chiper'da "KHAN" kelimesi key 'k=19' ile şifrelendiğinde oluşan mesaj nedir?
A-) NAHK B-) XYZA C-) EATH D-) EBUHC E-) DATG

99-) Ciphertext="gizet", key=(1,4), plaintext?
A-)cevap B-)deniz C-)kitap D-)kural E-)kalem

100-) Diffine –Helman Anahtar değişim protokolünde p=17 ve α=3 ise Alice 15' i seçiyor Bob ise 13' ü. Buna göre aralarındaki ortak anahtar aşağıdakilerden hangisidir?
a) 10 b) 9 c) 12 d) 11 e) 6

101-)Aşağıdaki yöntemlerden hangisi ayrık logaritma probleminin çözümünde kullanılabilir?
A-) Pohlig-Hellman
B-) Euclid
C-) Çinli Kalanlan Teoremi
D-) Shanks Algoritmas
E-) Fermat Teoremi

102-)X=2(Mod3), x=4(mod7), x=6(mod10) denklem sistemini sağlayan en küçük pozitif x sayısı elde ediniz.
a)120
b)180
c)240
D)320
e)116

103-) Aşağıdakilerden hangisi asimetrik şifreleme algoritmalarından biridir?
A) RC4
B) RSA **
C) 3-DES
D) DES
E) AES

104-) 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

105-) 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

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

107-)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.

108-) Sezar şifreleme sisteminde, "SEZAR" açık yazısı, Türkçe alfabede, hangi gizli yazıya dönüşür?
A-)RDYZP
B-)BRÜTÜS
C-)SFABS
D-)UĞCÇT
E-)KAVAKLI

109-) Legendre Symbol e göre () işleminin sonucu kaçtır?
A) -1
B) 0
C) 1
D) 37
E) 98
Cevap A

110-) 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

111-)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.

112-) 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

113-) Aşağıdakilerden hangisi simetrik anahtar kullanan algoritmalardan değildir?

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

114-) 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

115-) 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.

116-) 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

117-) 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

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