

KRİPTOGRAFİ YÖNTEMLERİ			
Klasik Yöntemler:	Modern Yöntemler:		
Yerine Koyma:	Simetri:		
Tek Alfabeli	Asimetrik:		
Çok Alfabeli	RSA		
	DES		
	3DES		
	Asim. Şifreleme:		
	RC4		
	SEAL		
	Asimetrik:		
	RSA		
	DSA		
	Diffie-Hellman		

KLASİK KRİPTOGRAFİ YÖNTEMLERİ

Sesaz Şifreleme (Caesar Cipher, M.O. SB), harflerin alfabedeki 3 konum sonrasındaki karşılığı ile değiştirilmesine esasa dayanır.

Anahtar = ve kadar döndürme

Şifrelenen harfin alfabedeki sesaz = [Şifrelencek harfin alfabedeki sesaz + Anahtar sayımı] mod 26

İngilizce Alfabe 26 harf -> 261 farklı şifre tablosu, 25 farklı anahtar sayı

Frekans analizi ile sesaz şifresi çözülebiliyor. En çok kullanılan harf ve kelimeler ile deşifre veya saldırılar yapılabilir.

Vernam Şifrelemesi (Vernam Cipher, One Time Pad, 1917), rastgele verilerden oluşturulan tek kullanımlık bir perit (şifre) anahtar olarak kullanılır.

Harfler iki sisteme girer, birinde kendine karşılık gelen iki kod ile XOR işlemine tabi tutularak şifreli metin oluşur.

Şifreli metin= (Açık metin XOR Anahtar)

Karakteristik iki sisteme girer, birinde kendine karşılık gelen iki kodla tablosu kullanılır

Açık metin = "ay"
Anahtar = 01100001, 01110011
Şifreli metin = 00011011 00001101
Şifrelenmiş kod = 01111000 01110100
Şifrelenmiş metin= "ay"

Açık metinde yer alan her karakter, şifre karşısına denk gelen karakteri modüllerle toplama işlemine tabi tutularak şifrelenir.

Açık metin="haceler", şifre="yolcu"
n(17) = y(26) + m (45 mod 26)
n(18) = x(23) + l (7 mod 26)
n(19) = u(20) + e (17 mod 26)
n(20) = i(9) + m (16 mod 26)
n(21) = t(19) + j (11 mod 26)
n(22) = r(17) + y (23 mod 26)
Şifreli metin="ufelguy"

Deşifre için şifreli metindeki moddan anahtar olarak kullanılan metnin modları çıkarılır.

Enigma Şifreleme

Arthur Scherbius, 1920'li yıllarda elektronekanlık bir şifre makinesi olan Enigma'yı icat etmiştir.

Enigma mekanizması sarıya kırmızı, elektrik bataryası, Enigma rotoru kömür ve karışondan oluşmaktadır.

Her harf karakterinin değiştirilmesi için rotor mekanizması geliştirilmiştir. Her karakter için üretilen yer bulduca farklı olabilmektedir.

1.Dünya Savaşı sırasında Nazi Almanyası tarafından bir mesajın şifrelenmesi ve tekrar çözülmesi amaçla ile kullanılmıştır.

Makine, Alet Turling ve ekibi tarafından geliştirilmiştir.

Operatör hatırlarını, prosedür açıkları ve ele geçen kod kitapları sayesinde çözülmebilmektedir.

Enigma şifreleme, Vigenere tablosunda kullanılan çoklu alfabe yöntemi kullanılır. Böylece tek bir düzlemde, aynı anahtar kullanılsa bile mesajlar şifrelenmemektedir.

Harfin şifrelenmeden önceki hâline aynı harf damamasa, deşifre çalışmaz ve çok sayıda döngü denemesine gerektirmektedir.

Hill Şifresi

Hill sistemi(1917), lineer cebirle dayanmaktadır. Anahtar ve açık metin harflerinin sayısal değerlerinin tablosu yapılır.

Hill şifresi ile açık metin **tane alfabetik karakter için m tane renk kombinasyonu** yapılır m tane alfabetik karakter üretilmektedir.

m=2 Açık metin, n=(LxL) şifrelenmiş metin, y=(y1,y2)
y1=11x1+3x2
y2=4x1+7x2

(y1,y2)=(11x1+3x2) [11 3] Matris gösterimi
[1 3]
Açık metin, x="ay"=[1 4] Anahtar, X=[2 4]
[3 5]

[1 4] [2 4] = [14 24] -> y1(14,24) = "KT"
[3 5]

Şifrenin açılması için matrisin tersinin bulunması gerekir.

büyüklük, playfair

MODERN KRİPTOGRAFİ YÖNTEMLERİ

Claude Elwood Shannon'un "Gizlilik Sistemlerinin Betimlenmesi" (1948), modern kriptografiyi başlatmıştır. Shannon'un çalışmaları, özellikle dağılımlı bir anahtar kullanılarak şifreleme sistemlerini, anahtar olmaksızın kırılması mümkün değildir.

Sonuç olarak bir anahtarla aynı mesajı şifreleyen anahtarlar farklıdır.

Whitfield Diffie ve Martin Hellman, "Kriptografide Yeni Yöntemler" başlıklı makalesi (1976) ile güvenli bir iletişim için anahtarın rolünü tanımlamışlardır.

Kriptografinin en temel sorunlarından biri olan anahtar alışveriş problemi çözülmüştür.

Şifreleme için kullanılan anahtarın dağılımı ve yerinde göre temel olarak iki çeşit şifreleme algoritması bulunmaktadır:

- Simetrik (gizli anahtarlı) şifreleme
- Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Asimetrik (açık anahtarlı) şifreleme

Simetrik şifreleme ve dağılımı şifreleme algoritmasıdır.

Diffie - Hellman Anahtar Dağılımı

Diffie - Hellman Anahtar Dağılımı Algoritması (1976), kriptografik anahtarların dağılımında kullanılan bir yöntemdir. Haberleşme tarafları ortaklaşa güvenli olmayan bir iletişim kanalı üzerinden ortak bir gizli anahtar üretilmesine olanak sağlar.

Ayrıca göndericinin açık ve gizli anahtar bulundur. Açık anahtarlar, büyük asal sayılar olarak seçilir.

Gönderici

1. Rastgele sayıyı üretir.

2. $A = g^a \text{ mod } P$ hesaplar ve Göndericiye gönderir.

3. Alınan değeri $A = g^a \text{ mod } P$ hesaplar.

Alınan

1. Rastgele sayıyı üretir.

2. $B = g^b \text{ mod } P$ hesaplar ve Göndericiye gönderir.

3. Gönderilen değeri $A = g^a \text{ mod } P$ hesaplar.

RSA

RSA Algoritması (1978), Ron Rivest, Adi Shamir, Leonard Adleman tarafından geliştirilmiştir.

Çarpımın ayrı ayrı çarpanlarına tamamlanır.

Anahtar uzunluğu 1024, 2048, 4096 bit olabilir.

Yeni bir anahtar oluşturulduğunda, anahtarın uzunluğu 1024 bit olabilir.

Şifreleme, anahtar dağılımı ve dijital imza oluşturma için kullanılır.

Anahtar oluşturma

1. Rastgele sayıyı üretir ve p ve q sayılarını seçer.

2. $n = p \cdot q$ hesaplar ve n değerini hesaplar.

3. $\phi(n) = (p-1) \cdot (q-1)$ olarak $\phi(n)$ değeri hesaplar.

4. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

5. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

6. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

7. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

8. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

9. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

10. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

11. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

12. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

13. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

14. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

15. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

16. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

17. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

18. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

19. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

20. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

21. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

22. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

23. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

24. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

25. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

26. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

27. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

28. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

29. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

30. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

31. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

32. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

33. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

34. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

35. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

36. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

37. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

38. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

39. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

40. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

41. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

42. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

43. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

44. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

45. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

46. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

47. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

48. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

49. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

50. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

51. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

52. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

53. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

54. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

55. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

56. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

57. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

58. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

59. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

60. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

61. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

62. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

63. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

64. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

65. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

66. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

67. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

68. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

69. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

70. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

71. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

72. e değeri $\phi(n)$ ile 1 sayısına eşit seçilir.

73. d değeri e ile $\phi(n)$ değerini 1 sayısına eşit seçilir.

