# ŞİFRELEME TİPLERİ ve ÇÖZÜMLEMELERİ



ÇAĞRI ESER

## **TANIM**

Geçmişten günümüze kadar gelmiş olan ve çoğu hala günümüzde kullanılmakta olan bir çok şifreleme türleri bulunmaktadır.Bu şifreleme türleri zamanla kırılması ile birlikte yeni teknikler geliştirilmiştir.Bu tekniklerin geliştirilmesi ise geçmiş yıllarda kullanılan şifreleme teknikleride göz ardı edilmemiştir.Bunlar genel olarak karıştırma,karmaşıklaştırma veya farklı aritmetik yöntemler ile geliştirme çalışmaları yapılmıştır.Bu makalede ise şifreleme tiplerinin ve modelleri hakkında araştırma çalışması yapılmıştır.

# **Modern Cryptography**

#### Circular Bit Shift

Hexadecimal,Decimal,Binary,ASCII olarak verilebilir. 2≤B≤32, 1≤N<B olarak Brute Force yapılabilir.

Shift by ±N bits, N= ve Block Size [B] (in bits) değerlerini almaktadır.2 Sayısal değer alır.

## Crypt()

MD5 Mode (\$1\$), Password ve Salt değer alır.

Örnek:

Pass=Merhaba Salt=Merhaba

MD5 crypt( \$\,\\_)\$1\$Merhaba\$OgeLyMkayk\$0.Ss/z9fQi.

## Blowfish (bCrypt) Mode (\$2\$)

Cost (Log2) between 04 and 31 olarak bir değer alır sayısal olarak 4 olur 5 olur. Ayrıca Salt (20 alphanum. chars) değeride almaktadır.

\$2y New algorithm (non ambiguous) \$2b New algorithm (variant) \$2aNew algorithm (ambigu) \$2x Old algorithm

Çeşitleri bulunmaktadır.

## SHA-2 Mode (SHA256 \$5\$ or SHA512 \$6\$)

256 ve 512 olarak ayarlanabilir. Ayrıca iterations ( yineleme ) ayarlanabilir durumda yapılabilir.

Salt : Merhaba Pass : DenemeSifre

Default Number of iterations

Sonuç:

\$6\$Merhaba\$e1fAujpWwiiLTUTXcVVYW3JrWbITZQEPkxFNsGTxUAWZsjBkbAFjE3eGSlstPbLPzdbk0QQIUe1H5xWWzJPJ10

İterations & rounds 3000 yapıldığı durum

\$6\$ rounds = 3000\$ Merhaba\$ Cv2PJYYbjkZ15rTWlrtv/0JwB4iqHc..EN4AaOQK6R/oQuJaInI84bxXYfj9z7q66kfXV1ScHyP48m1ETtQGJ.

#### **BlowFish**

Modları: ECB,CBC,CTR,OFB,CFB,PCBC

Padding: pkcs5padding, pkcs7padding, nopadding

In-Format - Out Format: String, Hex, Base 64

Tipinde olabilir. Ayrıca bir adet Password alarak metin çözümlemesi yapılabilir.

## BlowFish Araçları

http://blowfish.online-domain-tools.com/ https://www.lddgo.net/en/encrypt/blowfish

https://sladex.org/blowfish.js

#### RC4

Bir adet key değeri bulunmaktadır ve steam olarak moduda yer alır.Çıktılar base64 veya Hex değerlerinde olabilir.Binary biçimindede yer aldığı görülmektedir.

Hex: 24d4b760de5029faa85fb342f551083b Base64: JNS3YN5QKfqoX7NC9VEIOw==

https://cryptii.com/pipes/rc4-encryption https://www.lddgo.net/en/encrypt/rc4

https://encode-decode.com/rc4-encrypt-online/

## **RSA**

RSA, güvenliği tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanan bir tür açık anahtarlı şifreleme yöntemidir. 1978'de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından bulunmuştur.

## XOR

Klasik XOR şifrelemesidir.XOR olarak belirli bir değer ile birleşmesi sonucu oluşan değerler bütünüdür.Hexadecimal,ASCII,Decimal olarakta belirtilebilir.

0.0 = 1

0.1 = 1

 $1 \ 0 = 1$ 

 $1 \ 1 = 0$ 

Değerlerini almaktadır.

https://xor.pw/

https://www.dcode.fr/xor-cipher

# **Poly-Alphabetic Cipher**

# Alberti Cipher

Disk 1 : Small Ring, Disk 2 : Large Ring olmak üzere iki adet değer bölümü bulunmaktadır.

Initial Shift 0 Periodic increment 1 Period length 4

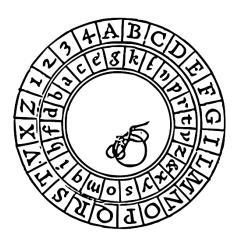
3 Adet ise Sayısal değerler bölümü bulunmaktadır.

Disk 1: ABCDEFGILMNOPQRSTVXZ1234 Disk 2: usqomkhfdbacegilnprtxz&y

0,1,4

OMQCMK-DECODE





Alberti Cipher Diskine ait görüntüler.

# Çözümleme

https://goto.pachanka.org/crypto/alberti-cipher-disk/https://www.dcode.fr/alberti-cipher

# **Alphabetical Ranks Added**

Şifrelenen veriler genelde sayısal bir değer alır.

Merhaba, 1

Şifrelenmiş hali : 13 18 36 44 45 47 48 olur. 1 ve 0 olarak iki adet değer almaktadır.

## **Autoclave Cipher**

American Cryptogram Association üyeleri tarafından kullanılmıştır. 1586 yılında Blaise de Vigenère tarafından oluşturulmuştur.2 türü bulunmaktadır key-autokey ve text-autokey isimleride buradan almaktadır.Vigenere Cipher ile ortak noktası bulunmaktadır.Birde alfabe bulunur genelde ABCDEFGHIJKLMNOPQRSTUVWXYZ kullanılır.

Plaintext: Merhaba

Key:TEST

Ciphertext: Fijamfr

Cözümleme:

https://www.dcode.fr/autoclave-cipher

https://en.metools.info/enencrypt/autokey206.html

https://crypto.interactive-maths.com/autokey-cipher.html

## **Beaufort Cipher**

Beaufort classic (key-txt) German variant (txt-key) olmak üzere 2 tip bulunmaktadır.Bir adet key ile şifreleme yapılabilir.Alfabede bulunmaktadır.

Plaintext: Merhaba

Key: Key

Result: Yahdexk Çözümleme :

https://www.boxentriq.com/code-breaking/beaufort-cipher

https://www.dcode.fr/beaufort-cipher

## **Bellaso Cipher**

5 Adet değer almaktadır. Bunlar;

PlainText: Merhabalar Keyword CHIAVE Alphabet ABCDEFGHILMNOPQRSTVX Number of alphabets to generate 10 Shift between each alphabets 1 Key to generate alphabets IOVE

Sonuç:

**ILCVPQPEPC** 

Şifrelenecek veri , Anahtar kelime , alfabe , oluşturulacak alfabe sayısı , alfabe arası geçiş numarası ve yaratılan alfabe anahtarı .

Çözümleme:

https://www.dcode.fr/bellaso-cipher

## Chaocipher

Left Disk Alphabet (Şifre Metni) ve Right Disk Alphabet (Düz Metin) olmak üzere iki adet disk bulunmaktadır.Örnek;

Left Disk Alphabet : XLEMFHIWOVNYRUDQCJPASGBTKZ Right Disk Alphabet: SGLBIZHJMFTRXAVKNQPDWYCUOE

Şifrelenmiş Veri : Okgmvtw

Çözümlenmesi:

https://www.cachesleuth.com/chaocipher.html

https://www.dcode.fr/chao-cipher

https://mysterytoolbox.organisingchaos.com/Ciphers/cipher/Chao

## **Delastelle Trifid Cipher**

3 Adet 9 kısascası 3^3 = 27 kare blok bulunmaktadır.Bunlarda alfabeye göre bir dizi söz konusudur.Ayrıca 100 'e kadar bir Group Size değeri almaktadır.Tercihen belirtilen key ilede otomatik şifreleme yapılabilir.

#1 #2 #3
DEN HIJ STU
MAB KLO VWX
CFG PQR YZ\_
Key: DENEME
PlainText: merhaba
Result: EHMTKPQ

Çözümleme:

https://www.dcode.fr/trifid-delastelle-cipher, https://cryptii.com/pipes/trifid-cipher

## **Gronsfeld Cipher**

Yalnızca 10 alfabenin kullanılması dışında Vigenère ile aynıdır ve dolayısıyla "anahtar kelime" sayısaldır.

Text: Merhaba Pass: 12345

Alfabe: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Result: Ngulfcc

Tablo:

Plain letter	G	R	0	N	S	F	Ε	L	D
Key (repeated)	1	2	3	4	1	2	3	4	1
Cipher Letter	Н	Т	R	R	Т	Н	Н	Р	Ε

# Çözümleme :

https://rumkin.com/tools/cipher/gronsfeld/ https://www.dcode.fr/gronsfeld-cipher

# **Hill Cipher**

2x2 veya 3x3 Matrixten oluşmaktatır. 2x2 values < 10 + latin alphabet brute force yapılabilir.

Ayrıca Matrix key ile oluşturmada bulunmaktadır.

## Örnek:

Metin: Merhabalar Ben Crypto

3x3 Matrix Key: 20 23 11 5 10 24 25 3 22 Sonuc: Zokvhptghr Jwz ZduyxmKN

2x2 ise 4 adet matrix bulunmaktadır.Bu kaynağa buradan ulaşılabilir.

https://www.cryptool.org/en/cto/hill

Alphabet (26 let. A=0) ABCDEFGHIJKLMNOPQRSTUVWXYZ Alphabet (26 let. A=1) ZABCDEFGHIJKLMNOPQRSTUVWXY Alphabet (27 char. A=0) ABCDEFGHIJKLMNOPQRSTUVWXYZ Alphabet (27 char. A=1) ABCDEFGHIJKLMNOPQRSTUVWXYZ Custom: ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 Sorularda bazen alfabe bu olabilir : abcdefghijklmnopqrstuvwxyz0123456789{ } 4 Çeşit ayarlanabilir ve manuel olarakta alfabe ayarlanabilir. Ayrıyetten Crypto aracı ile 5x5 Matrixe kadarda çıkartılabilir.

## Çözümlemeler:

https://www.dcode.fr/hill-cipher https://asecuritysite.com/cipher/hill

https://planetcalc.com/3327/

https://massey.limfinity.com/207/hillcipher.php

ABCDEFGHIJKLMNOPQRS	TUVWXYZ		Value o alphabet	of the first character
Hill key matrix			Multiplicatio	n variant
<ul><li>Alphabet characters</li><li>Number values</li></ul>		8		tor) * (matrix) * (column vecto
Alphabet characters	Number values		Size of matri	×
			c	1×1
			0	2×2
			0	3×3
			0	4 × 4
Ge	nerate random key		•	5×5
	Reset key		Larc	er matrix
Г	Show details and single step	s of the Hill cipl		No. madia
Encrypt Decryp			options	Cancel

# Jefferson Wheel Cipher ( Jefferson Cylinder )

Jefferson Diski olarakta bilinir.

Jefferson diski , her biri kenarları etrafında düzenlenmiş alfabenin 26 harfine sahip bir dizi tekerlek veya disk kullanan bir şifreleme sistemidir.



İlgili Görseller;

1:	< ZWAXJGDLUBVIQHKYPNTCRMOSFE <
2:	< KPBELNACZDTRXMJQOYHGVSFUWI <
3:	< BDMAIZVRNSJUWFHTEQGYXPLOCK <
4:	<pre>&lt; RPLNDVHGFCUKTEBSXQYIZMJWAO &lt;</pre>
5:	< IHFRLABEUOTSGJVDKCPMNZQWXY <
6:	< AMKGHIWPNYCJBFZDRUSLOQXVET <
7:	< GWTHSPYBXIZULVKMRAFDCEONJQ <
8:	< NOZUTWDCVRJLXKISEFAPYGHBQ <
9:	< XPLTDSRFHENYVUBMCQWAOIKZGJ <
10:	< UDNAJFBOWTGVRSCZQKELMXYIHP <

7:	<pre>&lt; R AFDCE O NJQGWTHSPYBXIZULVKM &lt;</pre>
9:	< E NYVUB M CQWAOIKZGJXPLTDSRFH <
5:	< T SGJVD K CPMNZQWXYIHFRLABEUO <
10:	< R SCZQK E LMXYIHPUDNAJFBOWTGV <
1:	< E ZWAXJ G DLUBVIQHKYPNTCRMOSF <
6:	< BİR MKGHI W PNYCJBFZDRUSLOQXVET <
3:	< T EQGYX P LOCKBDMAIZVRNSJUWFH <
8:	< N OZUTW D CVRJLXKISEFAPYGHBQ <
2:	< O YHGVS F UWIKPBELNACZDTRXMJQ <
4:	< W AORPL N DVHGFCUKTEBSXQYIZMJ <

Çözümleme :

https://www.dcode.fr/jefferson-wheel-cipher

## **Nihilist Cipher**

Kriptografi tarihinde Nihilist şifre, ilk olarak 1880'lerde Rus Nihilistler tarafından çarlık rejimine karşı terörizmi organize etmek için kullanılan, elle çalıştırılan simetrik bir şifreleme şifresidir.

Kare Bloklar ile yapılan bir şifrelemedir ayrıca KEY değeride yer almaktadır. Column-Row veya Row-Column olarak koordinatlarda yer almaktadır.

ABCDEFGHIKLMNOPQRSTUVWXYZ (-J) ABCDEFGHIJKLMNOPQRSTUWXYZ (-V) ABCDEFGHIJKLMNOPQRSTUVXYZ (-W) ABCDEFGHIJKLMNOPQRSTUVWXYZ (-Q) ABCDEFGHIJKLMNOPQRSTUVWXY (-Z)

Bilinen alfabeler yer almaktadır.

Şifreleme yapıldığında sayısal bir veri ortaya çıkmaktadır : 28 26 70 28 30 48 37 58 38 47 38 57 80 58

#### Çözümleme:

https://cryptii.com/pipes/nihilist-cipher https://www.dcode.fr/nihilist-cipher

Vertical shift ,Horizontal shift ,Number of characters per block olmak üzere 3 adet sayısal bir parametre değeri almaktadır.Ayrıca bir alfabe bulunmaktadır.Nihilist ile benzerlik göstermektedir. 5x5 Matrix bulunmaktadır.

#### Alfabeler:

ABCDEFGHIKLMNOPQRSTUVWXYZ (-J) ABCDEFGHIJKLMNOPQRSTUWXYZ (-V) ABCDEFGHIJKLMNOPQRSTUVXYZ (-W) ABCDEFGHIJKLMNOPQRSTUVWXYZ (-Q) ABCDEFGHIJKLMNOPQRSTUVWXY (-Z)

## **Porta Cipher**

13 Alfaden oluşmaktadır.Harf olarak 2 adet harf alır ve buna göre bir şifreleme gerçekleştirmektedir.Jeffersona benzer bir yapısı vardır fakat harf olarak 2 adet alır ve sonra alfabe alınır.

```
Keys | 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 b c d e f g h i j k l m C,D | o p q r s t u v w x y z n m a b c d e f g h i j k l m C,D | o p q r s t u v w x y z n m a b c d e f g h i j k l E,F | p q r s t u v w x y z n o l m a b c d e f g h i j k g G,H | q r s t u v w x y z n o p k l m a b c d e f g h i j k g G,H | q r s t u v w x y z n o p q j k l m a b c d e f g h i j k g h i j k l m a b c d e f g h i j k g h i j k l m a b c d e f g h i j k g h i j k l m a b c d e f g h i j k l m a b c d e f g h i j k l m a b c d e f g h i j k l m a b c d e f g h i j k l m a b c d e f g h i j k l m a b c d e f g h i j k l m a b c d e f g h i j k l m a b c d e f g h i j k l m a b c d e f g h i j k l m a b c d u,V | x y z n o p q r s t u v w x c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y z n o p q r s t u v w x y b c d e f g h i j k l m a b c d y z n
```

Cözümlemesi:

https://www.dcode.fr/porta-cipher

Ayrıca key değeri alarakta şifreleme yapılabilir. https://www.cachesleuth.com/portakey.html

## **Progressive Caesar Cipher**

Aşamalı bir sezar şifrelemesidir.Sayısal değerler girilerek farklı bir yöntem ile şifreleme işlemi gerçekleşmektedir.

3 Adet sayısal parametre alabilmektedir.

Progressive Shifting 1N,2N,3N,...) N= 1 Start at 0: (0N,1N,2N,3N,...) = Click Initial value of the shift = 1

Ayrıca ayarlamalarda yapılabilir : Each character (/c) Each word (/w) Every N characters (/n), N= 3

<u>https://coderdojodc.com/crypto/Encryption\_Tutorial.html</u> Cözümleme :

https://www.dcode.fr/progressive-caesar-cipher

# Ragbaby Cipher

Bir adet alfabe listesi alır veya 26 letters (A-Z),24 letters (Original, without J and X),36 alphanumeric characters (A-Z0-9) değerleri bunlarla birlikte 3 değerden biri seçildiğinde key girmek gerektedir. Eğer alfabe alınacaksa "shift of the first Word" ve "shift for each letter" sayısal değerleri girilmektedir.

Metin: Merhabalar Ben Ragbaby

Şifrelenmiş Hali : Nrblhjjwlk Ftu Bgljjl7

Key: SECRET

List: 36 alphanumeric characters (A-Z0-9)

Çözümleme:

https://thescytale.com/RB\_RagbabyDecoder.html

https://www.dcode.fr/ragbaby-cipher

## **Slidefair Cipher**

Bir key birde alfabe bulunur.Şifrelemeler çiftler halinde olmaktadır.Vigenereye benzerlik gösterir.

Çözümleme :

https://www.dcode.fr/slidefair-cipher

Key: SECRET Metin: Merhaba Sonuç: NFDVZCIR Alfabe:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

**Solitaire Cipher** 

Solitaire kriptografik algoritması, Neal Stephenson'un isteği üzerine Bruce Schneier tarafından , saha ajanlarının elektronik cihazlara güvenmek veya suçlayıcı araçlar taşımak zorunda kalmadan güvenli bir şekilde iletişim kurmak için kullandığı Cryptonomicon adlı romanında kullanılmak üzere tasarlandı.Sıradan bir oyun kağıdı destesiyle hesaplanan manuel bir şifreleme sistemi olacak şekilde tasarlandı

Text: Merhabalar Solitaire

Card Codes: 18, 5, 49, 29, 1, 28, 45, 15, 48, 32, 23, 8, 35, 14, 16, 34, 30, 43, 6, 37, 2, 39, 22, 7, 50, 17,

25, 12, 3, 46, 4, 52, 10, 21, 26, 47, 31, 33, 11, 44, 9, 40, 24, 27, 19, 36, 38, 20, 51, 41, 13, 42

Options: The generated keystream (sequence of cards as numbers from 1 to 52)

Alfabe: ABCDEFGHIJKLMNOPORSTUVWXYZ

Şifrelenmiş Hali : Ejokbdtawx Pwuwjimik

Cözümlenmesi:

https://www.dcode.fr/solitaire-cipher-schneier

## **Trithemius Cipher**

Ascending 0,1,2,3... ve Descenging 0,1,2,3... değerleri bulunur artan ve azalan olarak ayrıca bir adet alfabe yer alır. Initial Shift + 0 Numeral değer yer almaktadır.

Metin: Trithemius Test Ascending 0,1,2,3... Initial Shift + 0 ABCDEFGHIJKLMNOPQRSTUVWXYZ

Sonuç: Tskwljspcb Dpeg

## Çözümlenmesi:

https://www.dcode.fr/trithemius-cipher https://www.cachesleuth.com/trithemius.html https://md5decrypt.net/en/Tritheme-cipher/

## **Variant Beaufort Cipher**

German variant (txt-key) Beaufort classic (key-txt) Vigenere classic (txt+key)

Bir adet key değeri ve ABCDEFGHIJKLMNOPQRSTUVWXYZ alfabesi yer almaktadır. Beaufort Cipher'in Varyant tipinde bir şifreleme tipidir.

Şifrelenmiş bir veri : tYqta Xqnkqjv Rackbqhp

## Çözümlenmesi:

https://www.dcode.fr/variant-beaufort-cipher https://cryptii.com/pipes/variant-beaufort-cipher

## **Vernam Cipher (One Time Pad Vigenere)**

Gilbert Sandford Vernam (3 Nisan 1890 - 7 Şubat 1960), 1914'te Worcester Politeknik Enstitüsü mezunu ve AT&T Bell Labs mühendisiydi; 1917'de katkılı çok alfabetik akış şifresini icat etti ve daha sonra otomatik bir kerelik ped şifresini birlikte icat etti .

Text: VERNAM Key: VERNAM

Alfabe: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Şifrelenmiş Hali: QIIAAY

Çözümlenmesi:

https://www.dcode.fr/vernam-cipher

https://calcoolator.eu/vernam-cipher-encoder-decoder-

## **Vigenere Cipher**

Vigenere şifresi, düz metnin her harfinin farklı bir Sezar şifresi ile kodlandığı alfabetik metni şifreleme yöntemidir; bu şifrenin artışı, başka bir metnin karşılık gelen harfine ( anahtar) göre belirlenir.

Text: Merhaba Key : Key

Alfabe: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Sonuç : Wiprezk

Cözümlenmesi:

https://www.dcode.fr/vigenere-cipher

Ayrıca Auto solve ilede yapılabilir : https://www.guballa.de/vigenere-solver

## **Vigenere Multiplicative Cipher**

Burada ise değerler genel olarak sayısal işlemenktedir.

Örnek:

Text: 12 123 12 312 312 312 312 3123

Key ( Numbers ): 11 5 25

Sonuçlar: 132 615 300 3432 1560 7800 3432 15615

## **Transposition Cipher**

## **ADFGVX Cipher**

Kriptografide ADFGVX şifresi , Birinci Dünya Savaşı sırasında Alman İmparatorluk Ordusu tarafından kullanılan , elle uygulanan bir alan şifresiydi . Kablosuz telgraf kullanarak gizlice mesaj iletmek için kullanıldı . ADFGVX aslında ilk kez 1 Mart 1918'de Alman Batı Cephesi'nde kullanılan ADFGX adlı eski bir şifrenin uzantısıydı . ADFGVX, 1 Haziran 1918'den itibaren hem Batı Cephesinde hem de Doğu Cephesinde uygulandı .



ADFGVX Şeklinde bir Kare blokları 6x6 ve alfabeye görede şekillenmektedir.

#### Alfabeler örnek:

ABCDEFGHIKLMNOPQRSTUVWXYZ (-J) ABCDEFGHIJKLMNOPQRSTUWXYZ (-V) ABCDEFGHIJKLMNOPQRSTUVXYZ (-W) ABCDEFGHIJKLMNOPQRSTUVWXYZ (-Q) ABCDEFGHIJKLMNOPQRSTUVWXY (-Z)

#### Cözümlenmesi:

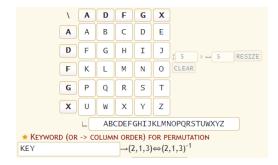
https://www.dcode.fr/adfgvx-cipher https://www.cachesleuth.com/adfgvx.html

## **ADFGX Cipher**

ADFGVX şifresine benzerdir sadece 5x5 kare bloklar yer alır.Permutasyon ayarlamaları diğerinde olduğu gibi bundada bulunmaktadır.

## Çözümlemesi:

https://www.dcode.fr/adfgx-cipher



# **AMSCO Cipher**

Şifreyi oluşturmak için bloğun genişliğini belirleyen bir anahtar seçilir ve ardından anahtarın altındaki bloğa yatay olarak düz metin yazılır. Hem satırlar hem de sütunlar her zaman digraflar ve tek harfler arasında değişir, ardından her sütun şifreyi oluşturmak için dikey olarak okunur. Sütunların okunma sırası anahtar kelimenin sayısal sırasına göre belirlenir.

## 2 Değer vardır options olarak

Split [2,1] : Bigram ve ardından unigram ile başlar Split [1,2] : Unigram ve ardından bigram ile başlar

Diğer Harflerin Kesme Sırası (Other letters cut sequence (repeated and alternated)): 2,3

Hepsi optional bir yapıdadır.

Permutasyon Key'i bulunmaktadır  $(1,3,2) \Leftrightarrow (1,3,2)-1$ : Key

## Şifreleme:

Text: Test Message

Split [1,2] (starts with Unigram then Bigram) Key: Deneme -  $(1,2,4,6,5,3) \Leftrightarrow (1,2,6,3,5,4)-1$ 

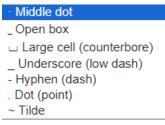
Result: TGEESSATSME

#### Cözümleme:

https://www.dcode.fr/amsco-cipher

## Caesar Box Cipher

Sezar şifreleme tekniğinin farklı versiyonudur.Şifrelenmiş bir kutu, bir dikdörtgen (veya bir kare) veya en azından bir boyut kullanır.



Ayrıca Karakterler yer almaktadır.

Optional'de "Keep punctuation and spaces" değeri tercih meselesidir.

# Örnek Şifreleme:

Metin: Merhabalar Ben Sezar

Box/Square/Rectangle Dimensions: Widht veya Height ikisinden biri

Widht: 7

Sonuç: MLEEAZRRAHBRAELBNLASL

Çözümleme:

https://www.dcode.fr/caesar-box-cipher

## **Columnar Transposition Cipher**

Bir aktarma şifresi (aynı zamanda permütasyon şifresi olarak da bilinir), karakterlerin kendisini değiştirmeden karakterlerin konumlarını ( aktarma ) karıştıran bir şifreleme yöntemidir.

Bir Key Değeri olur buna göre permütasyon ayarlanır.

Write by rows, read by columns (by default) 
Write by rows, read by columns (by default)
Write by rows, read by rows
Write by columns, read by rows
Write by columns, read by columns

Ayrıca 4 adet Mod seçeneği vardır Okuma – Yazma olarak Sütun-Satır olarak ayarlanabilir.

#### Örnek:

Metin: CrackerTest1923

Key: PERMUTEST  $(2,7,4,1,3,8,6,9,5) \Leftrightarrow (4,1,5,3,9,7,2,6,8)-1$ 

Optional: Write by rows, read by columns

Result: RTRC9CSA1TE3EK2

## Çözümleme:

https://www.dcode.fr/columnar-transposition-cipher

https://crypto.interactive-maths.com/columnar-transposition-cipher.html

# **Double Transposition Cipher**

İki adet permütasyon key bölümü ve her birinde Columns / Lines seçenekleri yer almaktadır.

## Örnek:

Metin: Merhabalar Ben Kripto

Permutasyon Key 1 : TEST  $(2,3,1,4) \Leftrightarrow (3,1,2,4)-1$  ( Columns ) Permutasyon Key 2 : 1923  $(1,3,4,2) \Leftrightarrow (1,4,2,3)-1$  ( Lines )

Result: EBRKTMAANPHLEIRABRO

#### Cözümleme

https://www.dcode.fr/double-transposition-cipher

## Rail Fence (Zig-Zag) Cipher

Rail Fence ( Demiryolu Çit ) şifresi ( zikzak şifresi olarak da bilinir ) klasik bir transposition şifresi türüdür . Adını, yatay raylarla inşa edilmiş bir çite benzetilerek şifrelemenin gerçekleştirilme şeklinden almaktadır.

```
W...E...C...R...U...O...
.E.R.D.S.O.E.E.R.N.T.N.E
..A...I...V...D...A...C.
```

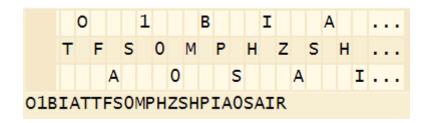
#### WECRUO ERDSOEERNTNE AIVDAC

## Örnek:



START olarak başlangıca dair bir değer belirtilir.

Ayrıca OFFSET olarak N = Numeral bir değer girilir.



Şifrelenmiş bir Rail Fence değeridir.

## Çözümleme:

https://www.boxentriq.com/code-breaking/rail-fence-cipherhttps://www.dcode.fr/rail-fence-cipher

## **Redefence Cipher**

Rail Fence yakınlığı ile bilinir benzer özelliklere sahiptir.

Dept,Offset ve Order gibi değerler belirir bunlarla bir şekil verilmektedir.

## Örnek:

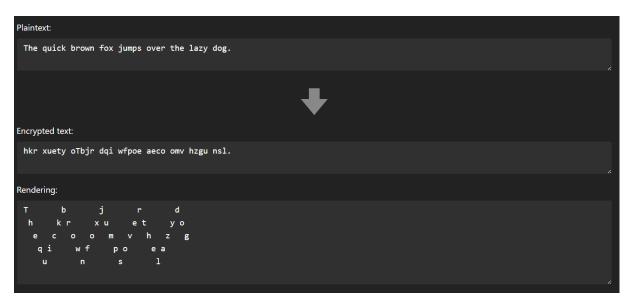
Text: "Merhabalar Ben Redefence"

Depth: 5 Offset: 0 Order: 21435

Alfabe: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Sonuç : elrdfMaehb eRn eraBeeanc

Örnek bir görsel;



## Çözümleme:

https://www.cryptool.org/en/cto/redefence https://www.dcode.fr/redefence-cipher

Ayrıca KEY değeri ilede şifreleme ve çözümleme yapılmaktadır.

## **Route Cipher**

Buradaki fikir, harfleri normal yazı gibi soldan sağa ve yukarıdan aşağıya yazmak değil, daha ziyade bir ızgaradaki yılan gibi veya zig zag gibi önceden tanımlanmış bir yolu takip etmektir .

Yön değerleri bulunmaktadır



Route width (horizontal size) : Yatay – Rota genişliği bulunmaktadır.Burada sayısal bir değer girilmektedir.

Ayrıca Boşluk karakteri için Dot,Underscore gibi özel karakterler düzenlemeside yer alabilir.

## Örnek:

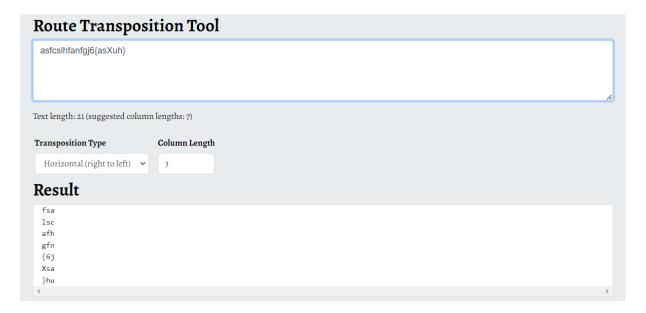
Text: RouteCipherTR

Horizontal Lines from bottom-left (Reading Direction)

Vertical Lines from top-left (Writing Direction)

Route width: 2 Special Chars: Tilde

Result: I~CRETTRUEOHRP



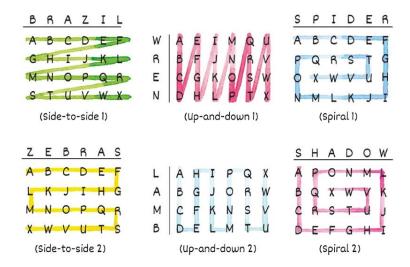
Sadece Column 3 R-L Horizontal ile yapılan bir çözümleme işlemi.

## Çözümleme:

https://www.dcode.fr/route-cipher

https://www.boxentriq.com/code-breaking/route-transposition

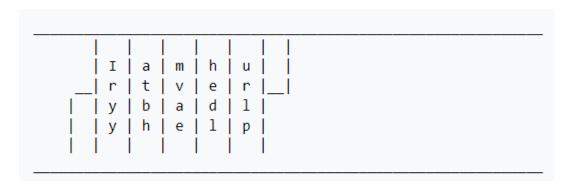
https://www.cachesleuth.com/routetransposition.html



Farklı tipte bir Route Cipher

# **Scytale Cipher**

Bir silindirden oluşan, bir aktarım(Transposition) şifresi gerçekleştirmek için kullanılan bir araçtır . etrafına sarılmış, üzerinde bir mesaj yazan bir parşömen şeridi. Antik Yunanlıların ve özellikle Spartalıların bu şifreyi iletişim kurmak için kullandıkları söyleniyor. askeri kampanyalar. Alıcı , mesajı okumak için parşömenle aynı çapta bir çubuk kullanır.



I am hurt very badly help

## Örnek:

"Merhaba Ben SCYTALE 1923"

Number of letters per turn of band : 3 (Ayrıca "Number of turns of the band" optional yapılabilirdi )

# Şifrelenmiş hali:

## MBAEELRNEHS1AC9BY2AT3

MBA

E E L

R NE

HS1

A C9

BY2

AT3

Böyle daha iyi bir açıklayıcı oldu sanırım.

## Çözümleme:

https://www.cachesleuth.com/scytale.html

https://dencode.com/cipher/scytale

https://www.dcode.fr/scytale-cipher

# **Spiral Cipher**

Route cipher ile benzer özelliklere sahiptir. Keep değerleri : spaces and punctuation & letters only Spiral tipleri bulunmaktadır.

## Örnek:

★ SPIRAL ☐ INWARD FROM TOP-LEFT, CLOCKWISE
○ Inward from top-left, counterclockwise
○ I INWARD FROM TOP-RIGHT, CLOCKWISE
○ I INWARD FROM TOP-RIGHT, COUNTERCLOCKWISE
☐ INWARD FROM BOTTOM-RIGHT, COUNTERCLOCKWISE
○
○ INWARD FROM BOTTOM-LEFT, COUNTERCLOCKWISE
O 🖪 OUTWARD, START BY RIGHT, CLOCKWISE
O 🔁 OUTWARD, START BY RIGHT, COUNTERCLOCKWISE
Olymord, Start by Bottom, Counterclockwise
O 🖪 OUTWARD, START BY BOTTOM, CLOCKWISE
OUTWARD, START BY LEFT, COUNTERCLOCKWISE
Outward, start by left, clockwise
OUTWARD, START BY UP, COUNTERCLOCKWISE
Outward, start by up, clockwise

Şifrelenmiş metin : ar·Tul···ra···kb·eyiahreM

Merhabalar Türkiye: Read in Lines ile şifrelenmiştir yukarıda ki spiral kullanılarak.

#### Cardan Grille

1550 yılında, Fransızca'da Jérôme Cardan olarak bilinen Girolamo Cardano (1501–1576), gizli mesajları yazmak için basit bir ızgara önerdi. Mesajlarının tamamının şifre gibi görünmemesi için mesajlarını sıradan bir mektubun içine gizlemeyi amaçlıyordu.

Örnek şifreleme:

Text : Masked : e

Pattern: denemebirpasswordrastgelebbb

Şifrelenmiş Hali: CCVMKAERHRJHAALBALFHZAOYRBEYCMNXOCARKCADUPAN

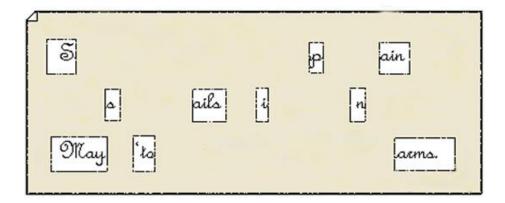
Random yapıldığında ise sonuç böyle olabilir;

Text: SGYMETRYWHABNYASLARVBBENCALWRDJAEYNVLW Mask: XXX X XX XX XX XX XX XX XX XXX

Çözümleme: https://www.dcode.fr/cardan-grille

Six John regards you well and spekes again that all as rightly 'vails him is yours now and ever.

Nay he 'tone for past d'lays with many charms.



Şifreleyici, ızgarayı bir kağıdın üzerine yerleştirir ve mesajını dikdörtgen açıklıklara yazar; bu açıklıklardan bazıları tek bir harfe, bir heceye veya tam bir kelimeye izin verebilir. Daha sonra ızgara kaldırılarak parçalar doldurularak gerçek mesajı gizleyen bir not veya mektup oluşturulur. Cardano, gizli kelimeleri gösterebilecek düzensizlikleri düzeltmek için metnin üç kez taslağının hazırlanmasını önerdi.

# **Ubchi Cipher**

Permutasyon bir key değeri olur bu string ifade ile verilmektedir. Ayrıca Harf verilmektedir çözümleme yapılırken ise harf kadar sayı girilmektedir.

Metin: Merhabalar Ben Sifreleme

Key: SECRET Letters: ABCDEF

Result: IAEEEAEFBDERAAMBMEFRSRLCLHNB

Çözümlemesi:

Cipher: IAEEEAEFBDERAAMBMEFRSRLCLHNB

Remove: 6

Result: MERHABALARBENSIFRELEME

# **Substitution Cipher**

# **Homophonic Substitution Cipher**

# **Homophonic Cipher**

Sayısal bazı değerler ile yapılan şifreleme yöntemidir.Sonuç sayısal bir değer oluşturur.

* ALPI	HABET	
	Letter	Replacement(s)
16	Р	26,44
17	Q	25
18	R	24,49
19	S	10,30,45,99
20	Т	06,96,55
21	U	16,94
22	V	23
23	W	13
24	X	11
25	Υ	08
26	Z	04
27		

Bir alfabe listesi ve Replacements yer alır.

Text: Merhabalar

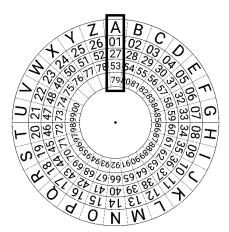
Sonuç: 9364914271531073124

Çözümlemesi:

https://www.dcode.fr/homophonic-cipher

# **Mexican Army Cipher Wheel**

4 Disk pozisyonları vardır.Harfler sayısal değerlerle ilişki kurmaktadır.buna göre bir şifreleme yöntemi geliştirilmiştir.



Örnek Bir Şifreleme:

* MEXICAN ARMY WHE	EL PLAIN	I TEX	XT (?)
Merhabalar			
★ WHEEL 1 POSITION	01 (A)	~	
★ WHEEL 2 POSITION	27 (A)	~	
★ WHEEL 3 POSITION	53 (A)	~	
★ WHEEL 4 POSITION	79 (A)		~
			► ENCRYPT
			LINGINIT

Sonuç : 39054408535401122718 sayısal bir değere bürünür. Çözümleme : <a href="https://www.dcode.fr/mexican-army-cipher-wheel">https://www.dcode.fr/mexican-army-cipher-wheel</a>

# **Modulo Cipher**

Modüler aritmetik ile yapılan bir şifreleme yöntemidir.

Modulo N değeri ve Her sayıda ki rakam sayısı belirtilir.

Örnek:

Text : Merhabalar Modulo N =20

Number of digits in each number: 9 (En fazla 9)

Result : 930166173 145431865 941365078 991982428 114477241 285837582 687164281 281653212

529347701 419968058

#### **Substitution**

#### **ASCII Shift**

ASCII Shift Cipher tekniği genel olarak farklı tiplerde görülebilir.Karmaşık karakterler veya Hexadecimal,Decimal,Octal veri olabilir.Sayısal bir değer ile shift işlemi yapabilmektedir.

Text: Merhaba Ben Cipher

Shift: 64

Result: (ASCII): %2(!"!\�%.\�)0(%2

HEX: 0D 25 32 28 21 22 21 60 02 25 2E 60 03 29 30 28 25 32

1-127 arası bir shift işlemi gerçekleşebilir.

## **Control characters encoding**

Karakter kodlama şifrelemesidir.Sayısal değerler girilerek bunların şifrelenmesi gerçekleşir. Unicode semboller ile veya daaha farklı bir teknik ile gerçekleşebilir.

Örnek:

Merhabalar > 77 101 114 104 97 98 97 108 97 114

Şifrelenecek veri : 77 101 114 104 97 98 97 108 97 114 Options : The associated Unicode Symbol (∿,..., ¬)

Result: BEGANF veya DC3 ETB ENQACK CAN FF

Sort Name olarak yapılır ise result : DC3 ETB ENQACK CAN FF

Cözümlemesi:

https://www.dcode.fr/ascii-control-characters

Alt Codes

Çeşitli emoji karakterleriyle yapılan şifrelemeler

Örnek

Text: Merhabalar

Çözümleme: https://www.dcode.fr/alt-codes-converter

## **Affine Cipher**

Bir alfabedeki her harfin sayısal eşdeğeriyle eşleştirildiği, basit bir matematiksel işlev kullanılarak şifrelendiği ve tekrar bir harfe dönüştürüldüğü bir tür monoalfabetik ikame şifresidir .

3 Adet seçenekte bulunmaktadır;

Bu katsayı için afin kod çözme/desübstitüsyon tablosu Bu katsayı için afin kodlama/ikame tablosu Afin katsayıları modüler ters DISPLAY AFFINE DECODING/DESUBSTITUTION TABLE FOR THESE COEF.

DISPLAY AFFINE CODING/SUBSTITUTION TABLE FOR THESE COEF.

O DISPLAY AFFINE COEFFICIENTS BY MODULAR INVERSE

Bunlar Calculate işlemleri için sadece geçerlidir.

A ve B Kat sayısı seçimi yapılır. Bir adette alfabe dizesi vardır.

Örnek:

Metin: Merhabalar 1923

A: 3 B: 1

Sonuç : f(x)=3x+1 : Lnawbebiba 1923

Çözümleme:

https://cryptii.com/pipes/affine-cipher https://www.dcode.fr/affine-cipher

## **Atbash Cipher**

Atbash şifresi, alfabeyi (veya abjad , hece , vb.) alıp bunu tersine eşleyerek oluşturulan özel bir tek alfabeli şifre türüdür , böylece ilk harf son harf olur, ikinci harf sondan ikinci harf olur.

Merhabalar metni "Nviszyzozi "olarak çevrilmiştir.

## Çözümleme:

https://www.dcode.fr/atbash-cipher

	Aleph	Bet	Gimel	Daleth	Heh	Vav	Zayin	Het	Tet	Yodh	Kaph	Lamed	Mem	Nun	Samech	Ayin	Peh	Tzady	Koof	Reish	Shin	Taw
Plain	א	ב	λ	Т	ה	1	r	n	υ	1	כ	ל	מ	3	0	ע	9	У	ק	٦	ש	ת
	Taw	Shin	Reish	Koof	Tzady	Peh	Ayin	Samech	Nun	Mem	Lamed	Kaph	Yodh	Tet	Het	Zayin	Vav	Heh	Daleth	Gimel	Bet	Aleph
Cipher	ת	ש	٦	7	צ	9	ע	0	3	מ	ל	5	1	ט	n	r	1	ה	т	λ	ב	א

Modern İbrani alfabesinin Atbash şifrelemesi

## **Bacon Cipher**

Bacon şifresi veya Bacon şifresi , 1605'te Francis Bacon tarafından geliştirilen bir steganografik mesaj kodlama yöntemidir.Bir mesaj, içeriğinden ziyade metnin sunumunda gizlenir. Bacon şifresi hem ikame şifresi (düz kodda) hem de gizleme şifresi (iki yazı tipini kullanarak) olarak kategorize edilir .

24 letters, I=J and U=V-24 Harften oluşur ve ayarlamaları mevcuttur.

Letter 1 ve Letter 2 olmak üzere 2 harf değeri girilmektedir.

Örnek:

Metin: Merhaba Cipher

Letter 1 : C Letter 2 : T

Options: 24 letters, I=J and U=V

Result: CTCTT CCTCC TCCCC CCTTT CCCCC CCCCT CCCCC CCCTC CTCCC CTTTC

CCTTT CCTCC TCCC

Çözümleme:

https://www.dcode.fr/bacon-cipher

https://mothereff.in/bacon

## $A-B\ Tablosu$

Letter	Code	Binary	Letter	Code	Binary
Α	aaaaa	00000	N	abbaa	01100
В	aaaab	00001	0	abbab	01101
С	aaaba	00010	Р	abbba	01110
D	aaabb	00011	Q	abbbb	01111
Е	aabaa	00100	R	baaaa	10000
F	aabab	00101	S	baaab	10001
G	aabba	00110	Т	baaba	10010
Н	aabbb	00111	U, V	baabb	10011
I, J	abaaa	01000	W	babaa	10100
K	abaab	01001	X	babab	10101
L	ababa	01010	Υ	babba	10110
M	ababb	01011	Z	babbb	10111

Letter	Code	Binary	Letter	Code	Binary
Α	aaaaa	00000	N	abbab	01101
В	aaaab	00001	0	abbba	01110
С	aaaba	00010	Р	abbbb	01111
D	aaabb	00011	Q	baaaa	10000
Е	aabaa	00100	R	baaab	10001
F	aabab	00101	S	baaba	10010
G	aabba	00110	Т	baabb	10011
Н	aabbb	00111	U	babaa	10100
1	abaaa	01000	V	babab	10101
J	abaab	01001	W	babba	10110
K	ababa	01010	X	babbb	10111
L	ababb	01011	Y	bbaaa	11000
М	abbaa	01100	Z	bbaab	11001

I,J,V ve

U harflerinin kendine göre düzenlerinden dolayı farklılık olabilir.

# **Bazeries Cipher**

Bu şifre iki adet 5x5 kare ızgara kullanır; biri düz bir alfabeyle, diğeri ise bir sayıdan oluşan anahtarlı bir alfabeyle doldurulmuştur. Düz metin harfler birinci ızgarada yer alır ve ikinci ızgarada aynı konumda bulunan harf şifre olarak kullanılır.

Numeric Key değeri girilir ve 2 kare bloklar ile yapılabilir .

"Merhabalar" metninin şifreme hali;

5x5 Bloklar halinde yapılan şifreleme



## **Binary to Characters (Shapes)**

Binary kodlarının şifreleme tekniğidir.

 $\label{eq:Merhaba} \textbf{ Cipher: 01001101\ 01100101\ 01110010\ 01101000\ 01100001\ 01100001\ 01100001\ 01100000\ 01100000\ 01101001\ 01110010}\\ \textbf{ 01101001\ 01110000\ 01101001\ 01110010}$ 

Şifrelenecek Veri: 01001101 01100101 01110010 01101000 01100001 01100010 01100001 00100000 01000011 01101001 01110000 01101000 01101001 01110010

#### Result:

dOqPIdIodo10\\I8po//0IoOOd1000%||ood0qIo80I810oO0818oqIdbIOdo/|\oOO8//%80\\81%11boI0

## **Book Cipher**

Kitap şifresi, bir mesajın düz metnindeki her kelimenin veya harfin, onu başka bir metinde konumlandıran bir kodla ( anahtar) değiştirildiği bir şifredir .

Şifrelenecek Veri: Merhaba Cipher

Metin:

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here', making it look like readable English. Many desktop publishing packages and web page editors now use Lorem Ipsum as their default model text, and a search for 'lorem ipsum' will uncover many web sites still in their infancy. Various versions have evolved over the years, sometimes by accident, sometimes on purpose

Şifrelenmiş Hali: 36, 5, 9, 50, 98, 13, 3, 47, 2, 59, 91, 92, 9

Çözümlemesi ise Metin ve Şifrelenmiş hali bulunan sayılar ile yapılmaktadır.

Cözümlemesi: https://www.dcode.fr/book-cipher

## **Ceaser Cipher**

Harflerin belirli bir düzene göre ötelenmesi ile yapılan sezar şifrelemesidir.Brute force ilede rahatça kırılabilir.

Tarihin ilk kriptolojik fikirleri İngilizce'de transposition and substitution cipher adını taşır. Yani yer değiştirme ve harf değiştirme şifrelemesi. Bu yöntemlerden ilki bir yazıdaki harflerin yerlerini değiştirerek, ikincisi ise harfleri başka harflerle değiştirerek elde edilir. Bu şifrelemeyi kullanan belki de en ünlü teknik Sezar Şifresi'dir: Bu şifrede, her harf o harften birkaç sonraki harf kullanılarak yazılır. Örneğin, 3 harf atlamalı Sezar Şifresi'nde "deneme" yerine "ghqhph" yazılır.

## **Disk Cipher**

Alberti Cipher'a benzer bir yapıdadır.



## Çözümlemesi:

https://www.dcode.fr/cipher-disk

## Consonants/Vowels Rank Cipher

Sesli harf, ses yolunda herhangi bir daralma olmaksızın telaffuz edilen heceli bir konuşma sesidir.

3 Modu bulunmaktadır.

```
Vowels and consonants (A=V1, B=C1, C=C2, ...)
Only Consonants (B=1, C=2, ..., Z=20)
Only Vowels (A=1, E=2, ..., Y=6)
```

Şifrelenmiş örnek veri : C10V2C14C6V1C1V1C2V3C12C6V2C14 (Merhaba Cipher)

#### D3 Code

Verilen stringi sayılar ile ve araya özel karakter koyularak yapılan şifrelemedir. 4 Modu vardır :

```
D=3, E=4, F=5, ..., Z=25, A=26, B=1
D=3, E=4, F=5, ..., Z=25, A=0, B=1
D=3, E=2, F=1, G=26, H=25, ..., Z=7, A=6
D=3, E=2, F=1, G=0, H=-1, ..., Z=-19, A=6
```

Metin: Merhabalar 1923

Varyant: D=3, E=2, F=1, G=26, H=25, ..., Z=7, A=6

Şifrelenmiş Veri : 20+2+15+25+6+5+6+21+6+15+ +1+9+2+3

## **DTMF Frequencies**

Dual-tone multi-frequency signaling (DTMF), telefon ekipmanı ile diğer iletişim cihazları ve anahtarlama merkezleri arasındaki telefon hatları üzerinden ses frekansı bandını kullanan bir telekomünikasyon sinyalizasyon sistemidir.

0123456789'un şifrelemesidir aşağıda ki gibidir. 1336-941 1209-697 1336-697 1477-697 1209-770 1336-770 1477-770 1209-852 1336-852 1477-852

#### **Dice Numbers**

Zar emojileri ile yapılan şifreleme

**□** 6

5

∷ 4

⊡ 3

□ 2

⊡ 1

## Çözümleme:

https://www.dcode.fr/dice-numbers

## **Enigma Cipher**

Enigma makinesi, ticari, diplomatik ve askeri iletişimi korumak için 20. yüzyılın başlarından ortalarına kadar geliştirilen ve kullanılan bir şifreleme cihazıdır. İkinci Dünya Savaşı sırasında Nazi Almanyası tarafından Alman ordusunun tüm kollarında yaygın olarak kullanıldı . Enigma makinesi o kadar güvenli kabul ediliyordu ki, en gizli mesajları şifrelemek için kullanılıyordu

## Modelleri

Enigma I
Enigma I "Norenigma"
Enigma I "Sondermaschine"
Enigma M3
Enigma M4 "Shark"
Enigma D/K
Enigma T "Tirpitz"

Swiss-K Railway Enigma "Rocket I" Zählwerk Enigma A-865 Abwehr Enigma G-111 Abwehr Enigma G-312 Abwehr Enigma G-260

UKW C ve B olmak üzere 2 adet reflektör bulunmaktadır.

ROTOR 1		POSITION	RING
VI	~	- 1 A +	- 1 A + Rotor 1,2,3 olmak üzere ayarları
ROTOR 2	~	POSITION - 17 Q +	bulunmaktadır.Buralarda harf ve sayısal değerlerle ayarlamalar yapılmaktadır.  – 1 A + Makine Tipleri :
ROTOR 3	~	POSITION - 19 S +	Wehrmacht/Luftwaffe 3 rotors Kriegsmarine 3 rotors  - 3 C + Kriegsmarine 4 rotors

Plugboard ayarlamaları mevcuttur bunlar harf şeklindede olabilir farklı ayarlardada olabilir.

Örnek Plugboard;

A-B, R-U bq cr di ej kw mt os px uz gh

## Çözümlemeler:

https://www.101computing.net/enigma-machine-emulator/

https://www.dcode.fr/enigma-machine-cipher

https://cryptii.com/pipes/enigma-machine

#### **Fractionated Morse**

Farklı bir mors kodlaması içermektedir.

Mors alfabesiyle kodlanması vardır. String olarakta ifade yer alabilir.

Test Merhaba
PSHZPTGATVCF
-|.|...|-||--|.|.-|--|.-|

Aralarında | çizgi yer alır.

## **Braille Cipher**

Gardner -Salinas braille kodları, görme engelli kişilerin dokunsal okuması için braille hücrelerini kullanarak matematiksel ve bilimsel gösterimi doğrusal olarak kodlamaya yönelik bir yöntemdir . Gardner-Salinas braille'in en yaygın biçimi, genellikle GS8 olarak adlandırılan 8 hücreli türdür . Ayrıca GS6 adı verilen karşılık gelen 6 hücreli bir form da vardır

```
abcdefgh{}
```

## **Hodor Language**

Hodor kelimeleri ile yapılan şifreleme türüdür.

Merhaba Bu Tuhaf Cipher

Result: HODOR Hodor!? hodor? rhodor. ("HODOR... hodor? rhHODOR Hodor! HODOR HODOR-

hodor!? Hodor- hodor!? hHODOR HODOR! Hodor... Hodor? HODOR. hhodor? r")

Decrpyt: alert("Merhaba Bu Tuhaf Cipher")

Javascript olarak sonuç vermektedir.

## **Javascript KeyCodes**

Javascript KeyCodes verilen metni numeral değerlere çevirmektedir. Alert metni = 65 76 69 82 84 numaralarını almaktadır. Ascii Tabloda Decimaldir.

## **K6 Codes**

Çeşitli varyantlarla ve özel karakterler arayı sokularak yapılan garip bir şifreleme türü.

#### Örnek

Text: abcdefgh{abc}

Varyant: K=6, L=5, M=4, ..., P=1, Q=26, R=25, ..., Z=17, A=16, B=15, ..., J=7

Result: 16+15+14+13+12+11+10+9+{+16+15+14+}

Varyant: K=6, L=7, M=8, ..., Z=21, A=22, B=23, ..., E=26, F=1, G=2, ..., J=5

Result: 22+23+24+25+26+1+2+3+{+22+23+24+}

Varyant: K=6, L=5, M=4, ..., P=1, Q=0, R=-1, ..., Z=-9, A=16, B=15, ..., J=7

Result: 16+15+14+13+12+11+10+9+{+16+15+14+}

Arada ki karakterler değişkenlik göstermektedir.

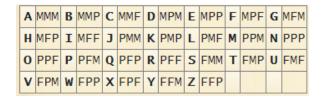
Bunun bide K7 versiyonu vardır oda buna benzerdir pek değişiklik yoktur.

## Çözümlemesi:

https://www.dcode.fr/k7-code https://www.dcode.fr/k6-code

## **Kenny Code**

Kendine ait bir alfabesi vardır ilginç bir şifreleme ile karşımıza çıkmaktadır.



Text : Merhabalar {1}

Result: Ppmmpppffmfpmmmmmpmmmmpmffl

Arada ki özel karakterler kaldırılmaktadır.

## **Keyboard Coordinates**

Keyboard Koordinatları ile yapılan şifreleme yöntemidir.

Text : Merhabalar

QWERTY (US) – Row 3 Column 2 Result : 58 34 35 47 42 56 42

Sonuçlar sayısal verilere dayanmaktadır.

Ayrıca Shift olarakta yöntemi bulunmaktadır. Burada ise string tipindedir.

https://www.dcode.fr/keyboard-shift-cipher, https://www.dcode.fr/keyboard-coordinates

# LSPK90CW Cipher

Özel karakterlerle yapılan şifreleme tekniğidir.

Merhabalar Ben Cipher  $ELL |^{<}][<{AA<{\_|<|^{<}}}AAVVZ |_{|---A_{|}}=[\cdot|/A<$ 

Sonuçlar doğru çıkmamaktadır.Garip bir şifrelemedir.

## A1Z26 Cipher

Alfabeye göre numaralandırılmıştır.

Α	В	C	D	Ε	F	G	Н	Ι	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Text: Merhaba Cipher

Result: 13;5;18;8;1;2;1;0;3;9;16;8;5;18

Cözümlemesi:

https://www.dcode.fr/letter-number-cipher

## **Malespin Slang**

Malespín , 19. yüzyılda El Salvador'da ortaya çıkan ve daha sonra Orta Amerika'nın geri kalanına yayılan bir tür İspanyolca argodur . Şu anda körelmiş durumda ve yalnızca az sayıda kelimeyle varlığını sürdürüyor.

Text : Merhaba Cipher Adam Result : Parhete Comhar Edep

Çözümleme: https://www.dcode.fr/malespin-slang

## **Mono-alphabetic Substitution**

Alfabedeki harflerin 1-1 yazışmaya göre başkalarıyla değiştirildiği bir ikame şifresidir (düz bir harf her zaman aynı şifre harfine karşılık gelir). Yer değiştirmenin tek alfabeli olduğu söylenir çünkü tek bir alfabe kullanılır, bu alfabeye düzensiz denir.

Text: Merhaba Cipher

Alfabe: QWERTYUIOPASDFGHJKLZXCVBNM

Result: Dtkiqwq Eohitk

# **Multiplicative Cipher**

Alfabe ve Key Number değerine göre yapılan şifreleme

Text: Merhaba Cipher

Alfabe: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key Number: 7

Gcpxaha Hcn Oebxcp

Çözümleme: https://www.dcode.fr/multiplicative-cipher

**NATO Phonetic Alphabet** 

Harflerin çeşitli isimlere bürünerek oluşturulan şifreleme yöntemidir.

Α	Alpha	В	Bravo
C	Charlie	D	Delta
E	Echo	F	Foxtrot
G	Golf	Н	Hotel
1	India	J	Juliett
K	Kilo	L	Lima
М	Mike	N	November
0	Oscar	P	Papa
Q	Quebec	R	Romeo
S	Sierra	Т	Tango
U	Uniform	٧	Victor
W	Whiskey	X	X-Ray
Υ	Yankee	Z	Zulu
0	Zero	1	One
2	Two	3	Three
4	Four	5	Five
6	Six	7	Seven
8	Eight	9	Nine
-	Dash		Stop

Merhaba

Mike Echo Romeo Hotel Alpha Bravo Alpha

Çözümlemesi:

https://www.dcode.fr/nato-phonetic-alphabet

## Nak Nak DuckSpeak

Ördek şifrelemesi.

Örnek

Metin: Merhaba Cipher

Result : Nak? nak! Naknak nak? Naknak Nananak Naknak Naknak Naknak Nahak Nahak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak Naknak

Naknak nak? Naknaknak Nananak

Coink-Couink Variant: Couink? coink! Couinkcoink coink? Couinkcoink Couincoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink Couinkcoink

Cözümlemesi:

https://www.dcode.fr/nak-nak-duckspeak

## Navajo Code

Navajo kodu, İngilizce askeri sözcükleri ve harfleri çeviren sözcükleri içeren bir sözlükten oluşur. Şifreleme, Navajo lehçesindeki bir metnin sözcüklerinin veya karakterlerinin değiştirilmesidir.

Örnek:

Metin: abcdefgh

Sonuc: BE-LA-SANA SHUSH MOASI CHINDI AH-JAH CHUO AH-TAD TSE-GAH

## **Keypad Drawing**

Telefon veya bilgisayarlada kullanılan klavyeler ile alakalı şifreleme yöntemidir.Keypad olarak numeral bir şifreleme yöntemidir.

Computer: abcdefghjkl

Computer Sonuc: 14789635 147896532 98423 147862 14789523 147895 987412365 7419635

789521 147593 74123

Phone: abcdefghjkl

Phone Sonuc: \*7412369#8 \*741236589#0 32470# \*7412690 321457\*0# \*741238 3214790#9

147\*369#58 123580\* 147\*538# 147\*0#

Çözümlemesi:

https://www.dcode.fr/numeric-keypad-draw

## **Periodic Table Cipher**

Periyodik tabloya göre yapılan şifreleme türüdür.

1	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18
1	1												2					
1	Н															He		
2	3	4											5	6	7	8	9	10
	Li	Ве							B C N O				0	F	Ne			
3	11	12								13 14 15 16 1				17	18			
3	Na	Mg											ΑŢ	Si	P	S	<b>c</b> 1	Ar
4	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
-	K	Ca	Sc	Ti	٧	Cr	Mn	Fe	Co	Ni	Cu	Zn	Ga	Ge	As	Se	Br	Kr
5	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
,	Rb	Sr	Υ	Zr	Nb	Мо	Tc	Ru	Rh	Pd	Ag	Cd	In	Sn	Sb	Te	Ι	Xe
6	55	56	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86
•	Cs	Ba	Lu	Hf	Ta	W	Re	<b>0</b> s	Ir	Pt	Au	Hg	T1	Pb	Вi	Po	At	Rn
7	87	88	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118
,	Fr	Ra	Lr	Rf	Db	Sg	Bh	Hs	Mt	Ds	Rg	Cn	Nh	F1	Mc	Lv	Ts	Og
				57	58	59	60	61	62	63	64	65	66	67	68	69	70	
					La	Ce	Pr	Nd	Pm	Sm	Eu	Gd	Tb	Dy	Но	Er	Tm	Yb
					89	90	91	92	93	94	95	96	97	98	99	100	101	102
				Ac	Th	Pa	U	Np	Pu	Am	Cm	Bk	Cf	Es	Fm	Md	No	

Metin: Merhaba Cipher

Result: M 68 1 A 56 6 53 15 2 R

Çözümleme:

https://www.dcode.fr/atomic-number-substitution

# **Polybius Square**

Polybius karesi olarak da adlandırılan Polybius şifresi , kare ızgara kullanan bir ikame şifresidir. Düz mesajın her karakterinin yerini, ızgaradaki konumunu tanımlayan birkaç koordinat alır.

## Alfabeler değiştirilebilir:

ABCDEFGHIKLMNOPQRSTUVWXYZ (-J) ABCDEFGHIJKLMNOPQRSTUWXYZ (-V) ABCDEFGHIJKLMNOPQRSTUVXYZ (-W) ABCDEFGHIJKLMNOPRSTUVWXYZ (-Q) ABCDEFGHIJKLMNOPQRSTUVWXY (-Z)

\	1	2	3	4	5	
1	Α	В	С	D	E	
2	F	G	Н	I	K	
3	L	М	N	0	Р	
4	Q	R	S	Т	U	
5	V	W	X	Υ	Z	

Line – Column ve Column-Line olarak ayarlanabilir.

Örnek şifreleme : Merhaba Cipher Result : 32154223111211132435231542

5x5 Kare Bloklarda Line-Column olarak şifrelenmiştir.

Çözümleme :

 $\underline{https://www.dcode.fr/polybius-cipher}$ 

https://cryptii.com/pipes/polybius-square

#### **ROT5** Encoder

ROT5 şifrelemesi bir mesajdaki rakamlara uygulanır (ideal olarak rakamlardan oluşur). Bir rakamın 5 ekleyerek başka bir rakamla değiştirilmesinden oluşur.

Text: 100 120 130 Result: 655 675 685

Çözümleme:

https://www.dcode.fr/rot5-cipher

## **ROT-13 Cipher**

Rot-13 (Rotation 13'ün kısaltması), tersine çevrilebilir ve çok basit olma özelliğine sahip, tek alfabetik ikame şifresine verilen addır. 26 harften oluşan Fransız/Latin alfabesini ve 13'lük ofseti birleştiren Rot-13, bir harfi alfabenin on üç hane aşağısında bulunan başka bir harfle değiştirir. Rot-13 kodlaması, içeriği gizlemek için popülerdir çünkü kolayca geri döndürülebilir, hatta iki kez uygulanırsa orijinal mesaj yeniden görünür.

Text : Merhaba Cipher Result : Zreunon Pycure

Cözümlemesi:

https://www.dcode.fr/rot-13-cipher

#### **Rot-47 Encoder**

Rot -47, tüm görünür ASCII karakterlerini kodlamaya izin veren bir kaydırma şifresidir (Rot13 şifresi yalnızca harfleri kodlayabilir). Rot47, 33 karakteri arasındaki ASCII tablo karakterlerinin bir alt kümesi olan 94 karakterlik bir alfabe kullanır.

Text : Merhaba Cipher Result : |6C9232 r:A96C

Sonuç karmaşık bir ifade içermektedir.

Çözümleme :

https://www.dcode.fr/rot-47-cipher https://dencode.com/cipher/rot47 https://codeverge.com/rot47

# **Rot-1 Cipher**

Rot -1 kodu, alfabenin kaydırılmasına (aynı zamanda döndürme olarak da adlandırılır) dayalı bir ikame şifresidir. Burada alfabede bir harfin hemen ardından gelen harf değiştirilir.

Text : Merhaba Cipher Result : Nfsibcb Djqifs

Çözümleme :

https://www.dcode.fr/rot1-cipher

# Rot8000 Cipher

ROT8000, her karakteri daha sonra Unicode deposunda başka bir yaklaşık 32768 konumla değiştiren tek alfabetik bir ikame yöntemi olan 0x8000 rotasyonunun kısaltmasıdır.

Text: abcdefg123a

Result: 斷籫籬籭蘿籯籰簺簻簼籪

Çözümlemesi: https://www.dcode.fr/rot8000-cipher

Rot Cipher ile alakalı çeşitli şifreleme türleri olabilir aşağıda ki kaynaklardanda çözümlenebilir.

https://www.dcode.fr/rot-cipher https://cyberchef.io/

# **Rozier Cipher**

Rozier şifresi Vigenère şifresinin bir çeşididir. Bir mesajı şifrelemek için, vigenère karesinde düz mesajın harfinin sütununu bulun, anahtarın harfini bulana kadar aşağı inin, ardından anahtarda takip eden harfi bulana kadar yatay olarak hareket edin ve son olarak Şifreli harf olan sütunun harfini okumak için yatay olarak yukarı çıkın.

	Α	В	С	D	Ε	F	G	н	1	J	K	L	М	N	0	Р	Q	R	s	Т	U	٧	W	X	Υ	z
Α	Α	В	С	D	Ε	F	G	Н	Τ	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z
В	В	С	D	Е	F	G	Н	T	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	w	Х	Υ	Z	Α
С	С	D	Ε	F	G	Н	_	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	w	Х	Υ	Z	Α	В
D	D	Ε	F	G	Н	Τ	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С
Ε	Ε	F	G	Н	Τ	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D
F	F	G	Н	-	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С	D	Ε
G	G	Н	Τ	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Ε	F
Н	Н	Τ	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	Ε	F	G
1	_	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С	D	E	F	G	Н
J	J	K	L	M	N	0	P	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С	D	E	F	G	Н	M
K	K	L	M	Z	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J
L	L	М	N	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	Τ	J	K
М	М	N	0	Р	Q	R	S	Т	U	٧	W	Х	Υ	Z	Α	В	С	D	Е	F	G	Н	nte	J	K	L
N	Ν	0	Р	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J	K	L	М
0	0	P	Q	R	S	Ţ	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	1	J	K	L	Ν	N
P	P	Q	R	S	T	U	٧	W	X	Υ	Z	Α	В	С	D	E	F	G	Н	-	J	K	L	M	Ζ	0
Q	Q	R	S	Т	U	٧	W	X	Υ	Z	Α	В	С	D	Е	F	G	Н	$\perp$	J	K	L	M	N	0	Р
R	R	S	Т	$\supset$	٧	W	Χ	Υ	Z	Α	В	С	D	Е	F	G	Ξ	I	J	K	L	М	N	0	P	Q
s	S	T	U	٧	W	Χ	Υ	Z	Α	В	С	D	Е	F	G	Н	-	J	K	L	М	N	0	Р	Q	R
Т	Н	U	٧	8	X	Υ	Z	Α	В	U	D	Ε	F	G	Н	=	J	K	L	Μ	N	0	Р	ď	R	S
U	٥	٧	W	Χ	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J	K	L	Μ	Ν	0	Р	Q	R	S	Т
V	>	W	X	Y	Z	Α	В	C	D	Е	F	G	Ξ	=	J	K	$\perp$	Μ	Ν	0	Р	Q	R	S	T	U
W	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J	K	L	M	N	0	Р	Q	R	S	Т	U	٧
X	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	1	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W
Υ	Υ	Z	Α	В	С	D	Ε	F	G	Н	Τ	J	K	L	М	N	0	Р	Q	R	S	Т	U	٧	W	Х
Z	Z	Α	В	С	D	Ε	F	G	Н	Τ	J	K	L	Μ	N	0	Р	Q	R	S	Т	υ	٧	W	X	Υ

Text : Merhaba Cipher Initial Key : MCH

Result: CJWXFGQHNFMJH

Çözümleme:

https://www.dcode.fr/rozier-cipher

# **Shankar Speech Defect**

Shankar'ın konuşma problemi, karakterin telaffuz kusurunu ortaya çıkarmak için tasarlanmış bir alfabeyle tek alfabeli ikame şifrelemesi olarak kullanılabilir. Harflerin yazışma tablosu şu sekildedir:

XWYAZBCDQEFGHIKLMNOPJRSTUV DFGHJKLMNUOPQRSTIVWXYZBACE

Text : Merhaba Cipher Adam

Result: HZNDXWX YQLDZN XAXH

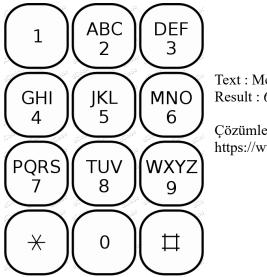
Cözümleme:

https://www.dcode.fr/shankar-speech-defect

# **T9 Cipher**

T9 (9 tuşlu metin), (eski) cep telefonlarında yalnızca sayısal tuşlarla klavye/tuş takımı üzerinde metin yazmak için kullanılan, sözlüğü temel alan bir tahminli metin yöntemidir.

Sonuçlar sayısaldır.



Text: Merhaba Adam Result: 637422202326

Çözümleme:

https://www.dcode.fr/t9-cipher

# **Tap Code**

Alfabedeki 26 harften 25'ini içeren, genellikle 5x5 boyutunda bir harf ızgarası kullanır (bir harf atlanır, genellikle J,k ya da Z). Izgaradaki hücrelerin koordinatları (satır, sütun) 1'den 5'e kadar numaralandırılır ve bu nedenle her hücrenin eşdeğer bir rakam çifti (satır, sütun) vardır.

# Örnek Şifreleme

Text: Merhaba Tap

Alfabe: ABCDEFGHIJKLMNOPORSTUWXYZ (-V)

Result:.....

Kullanılan Özel Karakter : . ( Nokta )

Eğer Karakter # kullanılsaydı sonuç :

Olacaktır.

Çözümlemesi: https://www.dcode.fr/tap-cipher

## **Triliteral Cipher**

Trifid şifrelemesiyle benzer özelliklere sahiptir.

Base3,Frederici,Cardan,Vigenere,Wilkins seçenekleri bulunmaktadır.

Text: Merhaba Cipher (Frederici)

Result: BAAABCCCAACCAABAACAAB ABABBABCAACCABCCCA

Çözümlemesi:

https://www.dcode.fr/triliteral-cipher

#### **Unicode Shift**

Unicode deposunda her karakterin benzersiz bir tanımlayıcısı (kod noktası adı verilen bir sayı) vardır . Bu sayıya bir N değeri eklenerek, Sezar kodu gibi, karakter kaydırma yoluyla bir ikame şifresi oluşturulmasını mümkün kılabilecek farklı bir karakter tanımlanır .

Text : Merhaba Shift : 1000 Result : еэњèщъщ

### Wabun Code

Japonca metinleri iletmek için kullanılan Mors kodunun bir çeşididir .

Text : Merhaba Cipher

Result: -...- R-... C.- P. R

Çözümlemesi:

https://www.dcode.fr/wabun-code

# **Wolseley Cipher**

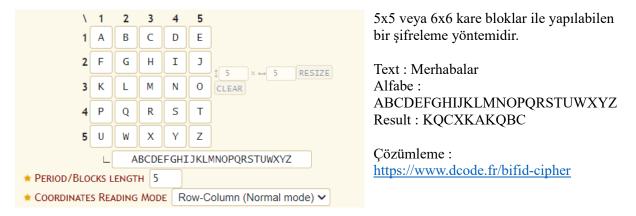
Dengesiz alfabeyle oluşturulan bir anahtara dayanan, tersine çevrilebilir bir substitution şifresidir .



# Polygrammic Cipher

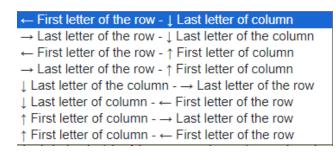
# **Bifid Cipher**

Klasik kriptografide bifid şifre , Polybius karesini transpozisyonla birleştiren ve difüzyonu sağlamak için fraksiyonlamayı kullanan bir şifredir . 1901 civarında Felix Delastelle tarafından icat edildi.



# **Collon Cipher**

Bir ızgara kullanan Collon'un şifresi Polybius'un karesine benzer, ancak koordinatları ızgaranın harfleridir.



Ayarlanabilir modeller.

5x5 Kare blokları kullanmaktadır.

Text: Merhaba Dostum

Model:  $\rightarrow$  Last letter of the row -  $\uparrow$  First letter of column

Alfabe: ABCDEFGHIJKLMNOPQRSTUWXYZ

Length of letter sequences: 3

Result: OETCECJEECABEEOADETTZDEAOC

# **Digrafid Cipher**

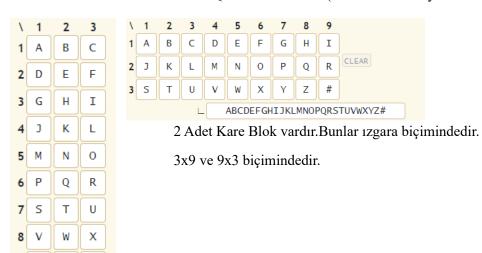
Digrafid şifreleme, 27 karakterli 2 ızgara (3x9 ve 9x3) kullanır.

Alfabe: ABCDEFGHIJKLMNOPQRSTUVWXYZ# (#sembolü alfabeye eklenir).

I

R

CLEAR



Örnek Şifreleme:

Ζ

Υ

Text : Merhaba Izgara Mangal

#

Result: VCNEBCSBUGCRASABNBU#X###

Çözümleme:

https://www.dcode.fr/digrafid-cipher

# **Four Square Cipher**

4 kareli şifreleme, adından da anlaşılacağı gibi, bir kare içine yerleştirilmiş dört kare ızgara (muhtemelen bir anahtar kelimeden oluşturulmuş) ile yapılır.



Örnek şifrelenmiş bir biçimde oluşturulmuş 4 Izgara

### Cözümleme:

https://www.dcode.fr/four-squares-cipher

Ayrıca Three ve Two şifreleme tekniğide vardır.

### Çözümlemeleri:

https://www.dcode.fr/three-squares-cipher

https://www.dcode.fr/two-square-cipher

# Multi-Tap Cipher

Telefon SMS şifreleme tekniğidir.Alfabede ki harflerin sayısal olarak değerlendirilmesidir.Eski telefonlarda SMS yazmak için tuşa tıklanma sayısıda diyebiliriz.

Α	2	В	22
C	222	D	3
E	33	F	333
G	4	Н	44
Ι	444	J	5
K	55	L	555
М	6	N	66
0	666	P	7
Q	77	R	777
S	7777	Т	8
U	88	٧	888
W	9	X	99
Υ	999	Z	9999

Text: Merhabalar Nasılsınız?

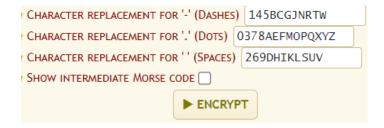
Result: 6 33 777 44 2 22 2 555 2 777 0 66 2 7777 444 555 7777 444 66 444 9999 0 0

Çözümleme :

https://www.dcode.fr/multitap-abc-cipher

# **Pollux Cipher**

Pollux'un şifrelemesi, Mors alfabesini ve Mors alfabesindeki tire ve noktaları başka karakterlerle değiştiren tomogrammik aşırı şifrelemeyi kullanıyor.



Text: Merhabalar

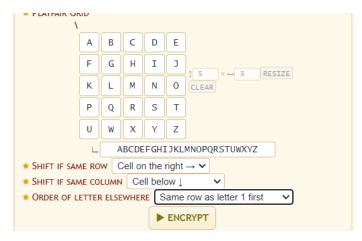
Result: RNDPSQRE28YMQ6AW2T8XA6YW2ERZXLM4VZCP

Cözümleme:

https://www.dcode.fr/pollux-cipher

Playfair Cipher

Playfair şifresi veya Playfair karesi veya Wheatstone-Playfair şifresi , manuel simetrik bir şifreleme tekniğidir ve ilk gerçek digram ikame şifresidir. Bu plan 1854'te Charles Wheatstone tarafından icat edildi, ancak kullanımını teşvik ettiği için Lord Playfair'in adını taşıyor .



5x5 Kare Bloklar yanı ızgara ile yapılan gelişmiş bir şifreleme yöntemidir.

### **Morbit Encoder**

Mors kodunun aşırı şifrelenmesidir ve parçalama yoluyla poligramik ikame eklenir.

Text : Merhaba Ben Darkorbit 9 Harfli Anahtar : AZERTYUIO

Result: 67757129312945173231789258689251728



## **Character Encoding**

### **32-Bit Integers**

Her 32 bitlik bloğun sayı olarak yorumlanmasıyla, bir mesaj bir dizi sayı olarak kodlanabilir.

Text: Merhaba Asker

Result: 1752327501 543253089 1701540673 114

https://www.dcode.fr/32-bit-integers

#### **ASCII85 Encoder**

ASCII85 şifrelemesi farklı türde ve modlarda şifreleme teknikleri vardır. Ayrıca Base85 olarakta bilinmektedir.

## Örnekler;

Text : Merhaba Cipher Options : Original

Result: 9kA?Y@:EXf6YULQAT@

Options: Adobe

Result: <~9kA?Y@:EXf6YULQAT@~>

Options: IP6 – RFC 1924

Result: O=WUuVPat\*LuqhmWpV

Options: ZeroMQ Z85

Result: o>wuUvpAT/lUQHMwPv

Options: BTOA

Result : xbtoa Begin

9kA?Y@:EXf6YULQAT@

xbtoa End N 14 e E 55 S 539 R 1691cc

### Çözümlemesi:

https://www.dcode.fr/ascii-85-encoding

### Crockford base-32 Encoder

Douglas Crockford tarafından tasarlanan base-32, base-32'nin (standart RFC 3548) insan tarafından yazma ve okumayı optimize etmeye ve bir miktar kontrol eklemeye istekli bir çeşididir . Crockford base-32, 32 karakter '0123456789ABCDEFGHJKMNPQRSTVWXYZ', yani 36 alfasayısal karakter kullanır.

Text: Merhaba Cipher

Result: 9NJQ4T31C9GJ0GV9E1M6AWG

# **Base 32 Cipher**

ASCII tablosunun 32 karakteri aracılığıyla ikili dizelerin iletimini kolaylaştırmak amacıyla RFC 4648'de açıklanan bir kodlama standardıdır .

Text: Merhaba Cipher

Result: JVSXE2DBMJQSAQ3JOBUGK4Q=

### **Base45 Cipher**

45 karakterli verileri kodlamak için önerilen bir kodlama standardıdır. Faltstrom ve diğerleri tarafından önerilmiştir. Base45 kodlaması, verilerin 45 tabanına yazılmasından ve aşağıdaki sembol listesinin kullanılmasından oluşur.0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ \$%\*+-./:Bu , alfasayısal modda bir QR kodunda kullanılabilecek 45 karaktere karşılık gelir.

Text : Merhaba Cipher

Result: DZ9%KE0ECOCCMN8L9E5\$C

Cözümleme:

https://www.dcode.fr/base45-encoding

# **Base58 Cipher**

ikili verileri belirli bir 58 karakter kümesinden oluşan bir karakter dizisine dönüştüren bir kodlama sistemidir.aritmetikteki herhangi bir taban gibi, büyük tamsayı sayılarını kodlamak için oluşturuldu; rakamlar için semboller kullanıyor. 58 tabanında, varsayılan olarak 58 sembol sunlardır:123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

Text : Merhaba Cipher Options : Bitcoin BTC

Result: VTJaoCJ6tcPPzF1YNMX

Options: Flickr

Result: usizNci6TBooZf1xnmw

Options: ABC...XYZabc...xyz123456789 Result: ecTjxMTF3mYY9QAhXWg

Options: abc...xyzABC...XYZ123456789

Result: DBsJXmsf3Lxx9paGwvF

Options: Ripple XRP

Result: VTJ2oUJatcPPzErY4MX

# **Base64 Encoder**

Base64, herhangi bir ikili dizeyi metinle kodlamak için 64 karakter kullanan bir bilgisayar kodudur (özellikle e-postalar için kullanılır).

Text: Merhaba Cipher

Result: TWVyaGFiYSBDaXBoZXI=

#### **Base62 Encoder**

Base62, ikili dizelerin kodlanmasına olanak tanıyan 62 karakterden (yani tüm alfasayısal karakterler: 0-9 arasındaki rakamlar, büyük harfler AZ ve küçük harfler az) oluşan bir kodlama yöntemidir. Bu 62 tabanında kullanılan 62 sembol kullanılmaktadır.

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Text: Merhaba Cipher

Result: 8Z6Y0PCqOGosdizesqo

### **Base91 Encoder**

Base91 (veya BasE91), base64'e bir alternatiftir ancak 91 karaktere kadar genişletilmiş bir alfabeye sahiptir: 94 yazdırılabilir ASCII karakteri (0x21'den 0x7E'ye kadar) atlanır-: kısa çizgi (0x2D),\: ters eğik çizgi (0x5C) ve': kesme işareti (0x27). Herhangi bir ikili verinin yalnızca yazdırılabilir karakterlerden oluşan bir karakter dizisine kodlanmasına (ve dolayısıyla kısa mesaj vb. yoluyla iletilmesine) olanak tanır.

Text: Merhaba Cipher

Result: ^OFKu),H\$yD6`E8jXB

#### **Baudot Encoder**

Baudot kodu, telgraf makinesiyle iletişim kurmak için oluşturulan alfabeye verilen addır. Farklı kullanıcılara ve dillere uyum sağlamak için çeşitli varyasyonları bilinmektedir. Alfabe daha sonra ITA2 (International Telegraph Alphabet No. 2) adı altında standartlaştırıldı.

Sonuçlara Binary kodlaması olarak yer alır. 0 ve 1'ler ile sonuçlanır.

Text: Merhaba Asker

Result: 11010 00010 11100 01011 00001 01100 00001 10000 00001 10100 11001 00010 11100

#### Modları:

International Telegraph Alphabet 2 (ITA2)

Baudot original (French/European)

Baudot british (UK)

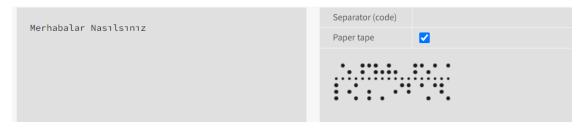
International Telegraph Alphabet 1 (ITA1)

CCITT-1 Internat. Telegraph & Telephone Consultative Committee

Baudot-Murray CCITT2

American Teletypewriter (US TTY)

Alphabet MTK-2 (Russian)



Paper Tape sonuçlar böylede yer almaktadır.

Toplu çözüm için bir diğer kaynak ise : <a href="https://v2.cryptii.com/text/select">https://v2.cryptii.com/text/select</a>

### **UUEncode Encoder**

Uuencode kodlaması, 65 ASCII karakteri (32'den 96'ya kadar) kullanarak herhangi bir ikili dizeyi kodlayabilir.ikili verileri Unix/Linux işletim sistemlerinde varsayılan olarak bulunan ASCII metnine dönüştürmek için kullanılan bir algoritmadır.

Text: Merhaba Asker

Sonuç: -365R:&%B82!!<VME<@```

Çözümleme:

https://www.dcode.fr/uu-encoding

#### Excess-3

Excess-3 kodu (Stibitz kodu olarak da adlandırılır ve bazen XS3 veya XS-3 kısayolu olarak da adlandırılır), eski işlemcilerde 10 tabanındaki bazı hesaplamaları optimize etmek için oluşturulan 4 bitlik ikili ondalık koddur.Sayısal bir şifreleme tipidir.

Text: 1923 80 30 40 50 1234456347

Result:

ŢΪ	t↓					
1923	0100110001010110					
80	10110011					
30	01100011					
40	01110011					
50	10000011					
1234456347	0100010101100111011110001001011 001111010					
#N : 6						

### Çözümleme:

https://www.dcode.fr/excess-3-code

#### **Z-Base32** Encoder

32 karakter kullanırybndrfg8ejkmcpqxot1uwisza345h769yani. Diğerleriyle karıştırılabilecek 4 karakter hariç 36 alfasayısal karakter:0,1,v,2. Alfabenin sırası da değiştirilir (bunun yerine abcdefghijklmnopqrstuvwxyz234567) ortak harfleri (ünlü harfleri) tercih etmek ve kodlanmış mesajları telaffuz edilebilir hale getirmek için. Ayrıca gereksiz karakterler=base32 ve base64 kodlarının sonunda görünen kodlar kaldırılır.

Text: Merhaba Asker

Result: ji1zr4dbcjo1yomupp1zr

Çözümleme:

https://www.dcode.fr/z-base-32-encoding

#### **Chuck Norris**

Chuck Norris'in, 1'i sırasıyla 0 ve 0'ı 00 ve ardından N sıfırla değiştirerek bir dizi ardışık biti kodlama yöntemine göre mesajları tekli kodda kodlamaya yöneliktir.

Text : Merhaba Asker Options : 7-Bit

Options: 8-Bit

https://www.dcode.fr/chuck-norris-code

**Symbols Cipher** 

Wingdings Font



Braille Alphabet



Alien Language \$\(\frac{1}{2}\P\)



Pigpen Cipher



Standard Galactic Alphabet



Mayan Numerals



# **Enochian Alphabet**



Music Staff Notation



Babylonian Numerals



Elder Futhark PNPFR



Egyptian Numerals



Unown Pokemon Alphabet



Templars Cipher



Hylian Language (Breath of the Wild)



Simlish Language



Zodiac Killer Cipher



# Dancing Men Cipher



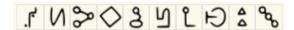
Music Sheet Cipher



7-Segment Display



Gravity Falls Bill Cipher



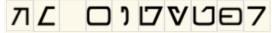
**Dovahzul Translator** 



Iokharic Language



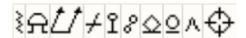
Aurebesh Alphabet



Symbol Font

 $M](\delta\omega \perp X8\%)$ 

Enderwalk Language



Flag Semaphore



# Hexahue



Navy Signals Code



Webdings Font



Futurama Alien Alphabet



Sheikah Language



Gravity Falls Journal 3



Atlantean Language



Rosicrucian Cipher



Theban Alphabet



Cistercian Monk Numerals



Younger Futhark ₱NÞ\RY



Celestial Alphabet



Ogham Alphabet



Clock Cipher



Klingon Language



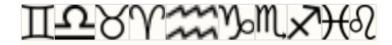
Gerudo Language

6681360188

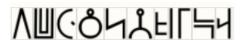
Chinese Code



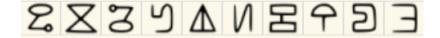
Zodiac Sign



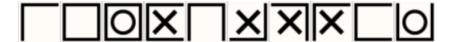
Wakanda Alphabet



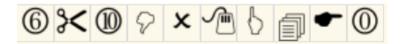
Gravity Falls The Author



Tic-Tac-Toe Cipher



Wingdings 2 Font



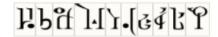
Vulcan Language (Star Trek)



Halo Covenant Language



Hylian Language (Twilight Princess)



French Sign Language



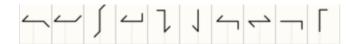
Lunar Alphabet (L. Katz)



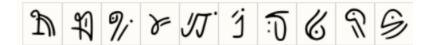
Acéré Cipher



Chappe Code



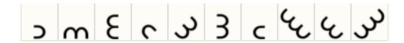
# Amphibia Alphabet



Daedric Alphabet



Dorabella Cipher



Matoran Language



Birds on a Wire Cipher



Tally Marks



Mirror Digits



Kryptonian Alphabet



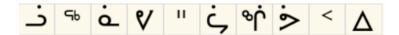
Monklish Alphabet



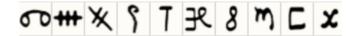
Ancients Alphabet from Stargate



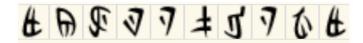
# Inuktitut Language



Mary Stuart Code



Hylian Language (Skyward Sword)



Malachim Alphabet



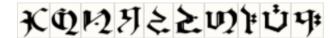
Astronomical Symbol



Friderici Cipher (Windows)



Teyvat Language (Genshin Impact)



Kirby (Forgotten Land) Alphabet



**Dotsies Font** 



Stray Alphabet



# American Sign Language



Hylian Language (The Wind Waker)



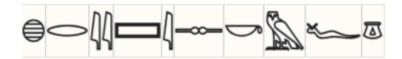
Chappe Alphabet



Goron Language



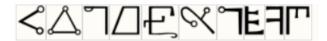
Hieroglyphs (Manuel de Codage)



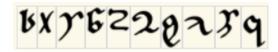
Gnommish Language



Passing the River Alphabet



Lingua Ignota



D'ni Numerals



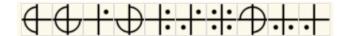
Betamaze Cipher



ITC Zapf Dingbats



Circular Glyphs Alphabet



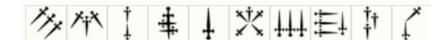
Voynich Cipher



Hymnos Alphabet



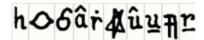
Daggers' Alphabet



Alpha Angle System Branding



Copiale Cipher



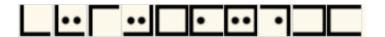
Arthur and the Invisibles Alphabet



Fez Alphabet



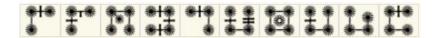
Dada Urka Cipher



Nazcaän Alphabet



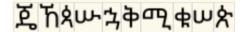
Alphabet of Angels and Genii



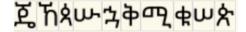
Hylian Language (A Link Between Worlds)



Amharic Language



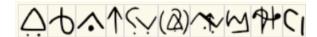
Amharic Language



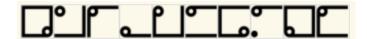
Ballet Alphabet



RataAlada Cipher (Batman)



Nyctography Lewis Carroll



Outer Rim Basic Alphabet



# Mourier Alphabet



**Knots Notation** 



Abyss Language (Genshin Impact)



Tifinagh Alphabet († を出くし。り)



Sumeru Language (Genshin Impact)



Inazuman Language (Genshin Impact)



Deshret Language (Genshin Impact)



Al Bhed Language

