ATBASH ŞİFRELEME TEKNİĞİ

Bir metni şifrelemek veya şifresini çözmek için İbrani alfabesi temelli basit bir yöntemdir. Bilinen en eski şifreleme yöntemlerinden biridir. Bu şifrelemede her harfin alfabedeki sırasını tersine çevirerek şifreleme işlemi yapar.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
Z	V	Y	Ü	U	T	R	P	Ş	S	Ö	O	N	M	

Örnek: Yukarıdaki tabloya göre;

“melisa” kelimesini “ktlohz” şeklinde şifreler.

POLYBIUS ŞİFRELEME TEKNİĞİ

Harflerin iki rakamlı sayılara dönüştürülmesini sağlayan ve böylece şifreleme amacıyla kullanılan bir karedir.

	1	2	3	4	5
1	A	B	C/Ç	D	E
2	F	G/Ğ	H	I/İ	J
3	K	L	M	N	O/Ö
4	P	R	S/Ş	T	U/Ü
5	V	Y	Z		

Bu durumda “ALİ ATA BAK” cümlesi yukarıdaki Polybius Karesi yardımıyla yazıldığında söz konusu cümlenin şifrelenmiş sayısal karşılığı “11 32 24 11 44 11 12 11 31” olacaktır.

Ancak, Polybius Karesi’nin alfabetik düzeninde bir değişiklik yapılmadığı sürece bu türden bir şifrelemeyi herkes kolayca çözebilir. Bu nedenle Polybius Karesi’nin şifrelemesi, “parola” olarak belirlenen bir kelime yardımıyla güçlendirilmektedir. Söz konusu parola, Polybius Karesi’nde ilk başa yazılır. Burada dikkat edilmesi gereken üç kural vardır:

1. Paroladaki her bir harf, karede yalnızca bir kez kullanılmalıdır.

2. Parola yazıldıktan sonra geri kalan harfler, karede alfabetik sırayla yazılmalıdır.
3. Parolada kullanılmış olan harfler, karede bir kez daha kullanılmamalıdır.

Örneğin, parolası “MATEMATİK” olan bir Polybius Karesi yapılırsa, bu kare şuna benzeyecektir:

	1	2	3	4	5
1	M	A	T	E	I/İ
2	K	B	C/Ç	D	F
3	G/Ğ	H	J	L	N
4	O/Ö	P	R	S/Ş	U/Ü
5	V	Y	Z		

Bu “MATEMATİK” parolalı tabloda “ALİ ATA BAK” cümlesi yazılmak istenirse bu cümlenin Polybius Karesi’ndeki şifrelenmiş sayısal karşılığı “12 34 15 12 13 12 22 12 21” olacaktır.

ZIGZAG ŞİFRELEME TEKNİĞİ

Zigzag şifreleme(Rail Fence Cipher) var olan karakterlerin belirli bir permütasyon kullanılarak yer değiştirmesi prensibine dayanan bir transposition şifreleme formudur. Adını şifreleme yönteminin biçiminden dolayı bu şekilde almıştır.

Şifrelenecek olan metin(plain text) aşağı doğru ve diagonal olarak hayali raylara doğru iner. En alttaki hayali raya geldiğinde tekrar yukarı doğru çıkar ve en üste ulaştığında tekrar aşağı doğru inmek şeklinde açık metin(plain text)’in uzunluğuna göre bu şekilde devam eder.

Örnek

Açık mesaj (Plain Text) İSTANBULTİCARETÜNİVERSİTESİ

Satır Sayısı : 3

İ . . . N . . . T . . . R . . . N . . . R . . . E . .

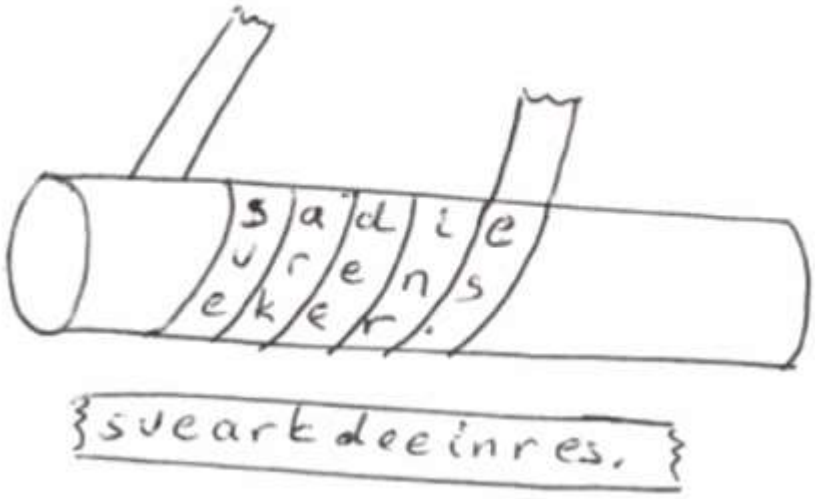
. S . A . B . L . İ . A . E . Ü . İ . E . S . T . S .

. . T . . . U . . . C . . . T . . . V . . . İ . . . İ

Şifrelenmiş Metin (Crypted Text): İNTRN RESAB LİAEÜ İESTS TUCTV İİ

SCYTALE CRYPTEX ŞİFRELEME TEKNİĞİ

Bilgisayar bilimlerinde, veri güvenliği konusunda kullanılan ilkel bir yer değiştirme şifrelemesidir (transposition cipher). Sistem çalışma şekli açısından simetrik şifrelemedir (symmetric cipher) ve iki tarafında elinde doğru anahtar bulunduğunda (gönderen ve alan) çalışmaktadır. Basitçe bir çubuğun etrafına bir mesajın sarılması ile elde edilen mesaj şifreli mesajdır.



Yukarıdaki şekilde sarmal şifrelemesi ile okunaklı olan (soldan sağa ve yukarıdan aşağıya) bir mesajın açılmış hali gösterilmektedir.

Mesaj “svearkdeeinres.” Olarak şifrelenmiştir. Bu mesajın doğru çaptaki bir çubuğun etrafına sarılması ve yukarıdaki şekilde okunması ile mesajın açık hali (plain text) anlaşılabilir. Yukarıdaki örnekte mesajın açık hali “sadievrenseker.” olarak okunabilir.

Bu şifreleme sisteminde doğru çaptaki çubuk anahtar olmaktadır.

Burada cipher (şifreleyici) şeridin sarıldığı baston oluyor, mesajı gönderen ve alan kişi aynı ebatlarda bastona sahipse mesaj kusursuz biçimde karşı tarafa ulaşıyor. Çok güçlü bir şifreleme yöntemi değil tabiki ama bundan 3000 yıl öncesini düşünürsek kırılması epey zor bir yöntem.

Programcılık açısından ise orta zorlukta bir dizi işlemi gerektirir. Diyelim ki kodu oluşturacak sargı sayısı 10 olsun, her bir satır için 10 karakter saklayacaktır. İkinci

satırın ilk harfi kodlama yağıldığında tüm metnin ikinci harfi olacaktır. Bu şekilde düşünüldüğünde 2 boyutlu dizinin tek boyutlu hale getirilmesi işlemi yapılıyor demektir.

B	U	B	İ	R	Ş	İ	F	R	E
L	İ	M	E	S	A	J	D	I	R

Alt satırdaki karakterler üst satırdaki karakterlerin arasına geçiş yapacaktır;

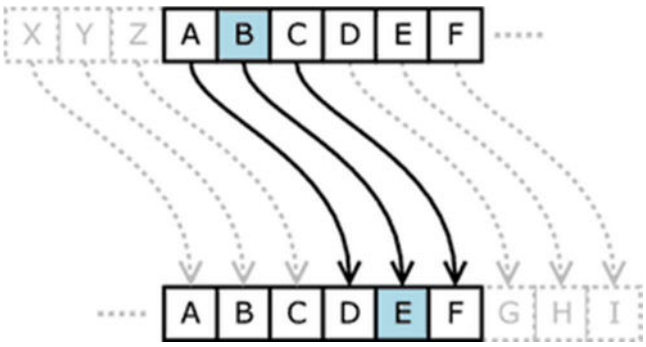
Yukarıdaki;

BUBİRŞİFRELİMESAJDIR kelimesi

BLUİBMİERSŞAİJFDRIER olarak şifrelenir.

SEZAR ŞİFRELEME TEKNİĞİ

En eski şifreleme yöntemlerinden bir tanesi de Romalı'ların geliştirmiş olduğu şifreleme yöntemidir. Harflerin sırasını kaydırma yöntemi ile yapılır. Kodu çözecek olan kişi kaydırma sayısını biliyorsa iletilen mesajı rahatlıkla çözebiliyor. Örneğin üç harf atlamalaı bir şifrelemede "abi" kelimesi "del" ile kodlanır.

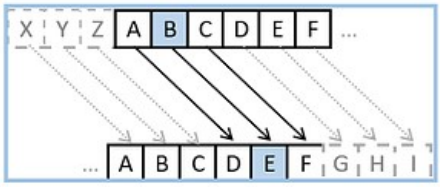


3 harf kaydırmalı Sezar şifreleme

Öte yandan, Sezar Şifresi(Cevrimsel alfabe) kırmak görece kolay olmaktadır: Bir filolog, bir dilde en çok geçen harfleri bulabilir. O harfler ile mesajda en sık geçen harfleri karşılaştırarak hangi harfin hangi harf ile değiştirildiğini bulabilir. Bu adımların ardından, mesaj çözülmüş olur. Sezar Şifresi Hakkında:

- Kaba kuvvet (brute-force) saldırısıyla çok kolay çözülür. ÇünküŞifreleme/Şifre çözme yöntemi gizli değildir.
- Sadece 25 (Latin alfabesi harf sayısı) farklı deneme yeterlidir. (Anahtar uzayı 25 elemanlıdır.)
- Düz metin (plaintext) ve formatı gizli değildir.
- Harf değiştirme şifrelemelerinde toplam 26! farklı şifre tablosu vardır.

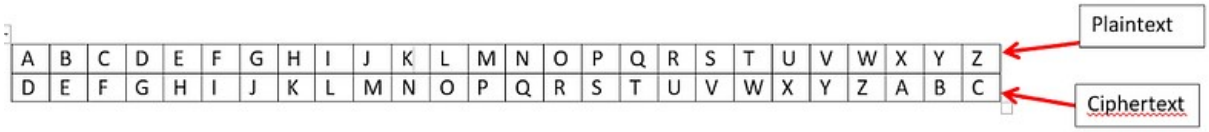
Genel olarak 26 harfli ingiliz alfabesi için çözüm;



SHIFT +3

This Caesar cipher has a shift of 3 characters.

The letter 'A' becomes a 'D'. The letter 'B' becomes 'E'.



HOMOFONİK ŞİFRELEME TEKNİĞİ

- Sezar şifresi (Ceaser's cipher) gibi mono alfabetik şifreleme yöntemlerinin frekans analizi (frequency attack) karşısında aciz kalmasının karşısında homofonik yer değiştirme şifresinde bu zaaf kısmen de olsa ortadan kalkmaktadır. Şifreleme yönteminin temel çalışma prensibi şifrelenecek metnin ait olduğu alfabedeki harflerin kullanım sıklıklarına dayanmaktadır. Her bir harf frekansına en yakın tam sayı kadar ayrı sembol ile ifade edilmektedir. Kriptolama işlemi ise her harf kendisine karşılık gelen bir veya birden fazla sembolden herhangi birisinin rassal olarak seçilmesiyle gerçekleşmektedir.
- Tablo 1.1 İngiliz Alfabesindeki Harflerin Kullanım Sıklıkları ve Homofonik Şifreleme Sonucu Kaç Değişik Sembolle Gösterileceği

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

- Plaintext: ANKARA
- Ciphertext: 47 91 04 47 35 53
- Veya
- Ciphertext: 09 18 04 53 35 78
- Her harf kriptolanma aşamasında Tablo 1.2 'de ilgili sütundan rassal bir değer seçilmesi ile gerçekleşmektedir. Bu şekilde alfabede A ve E gibi sık kullanılan harfler ciphertext'te birden fazla şekilde sembolize edilecek, dolayısıyla ciphertext'teki frekans değerleri bozuntuya uğrayacaktır

TRANSPOSİTİON KOLON DEĞİŞTİRME ŞİFRELEME TEKNİĞİ

- Yerine Koyma Yöntemleri (Substitution Methods): Gizli anahtar şifreleme tekniğinde kullanılan bu şifreleme yönteminde açık metindeki karakterlerin yerine, başka bir alfabenin karakterleri veya sayısal değerler koyulur. (Mullins ve Moore 2002)

- Yer Değiştirme Yöntemleri (Transposition Methods): Yine gizli anahtar şifreleme tekniğinde kullanılan bu yöntemde açık metin karakterlerinin pozisyonları yeniden düzenlenir. Orijinal

karakterler konumlarını kaybederler, fakat kimlikleri değişmez. Picket Fence Columnar ve Double Fİve şifreleme algoritmaları bu yöntemlere örnek olarak gösterilebilir. .(Highland 1997)

Columnar tranposition şifreleme yönteminde amaç karakterlerin kimliklerini değiştirmeden pozisyonlarını değiştirmektir. Şifre kullanılarak veya sadece satir sütün değişikliği yapılarak uygulanabilir. Columnar transposition şifreleme yönteminde bir C değeri ile şifrelenecek metin tabloya sokulurken tabloda olacak sütün sayısı belirlenir. Örneğin şifreleme yapacağımız metin COLUMNARTRANSPOSITIONCIPHER olsun. C=5 dersek şifreleme yaparken oluşturacağımız tablo şu şekilde olur.

1. Key kullanmadan şifreleme:

   Bu metnimizi key kullanmadan Columnar Şifreleme Yöntemi uygulayarak şifreleyecek olursak;

   CNASNEOANICRLRSTIUTPIPMROOH

   cipher textini elde ederiz. C=5 oldugu için şifrelenmiş metni düzenleyecek olursak, şifrelenmiş metnimizin en son hali şu şekilde olur;

   CNASN EOANI CRLRS TIUTP MROOH

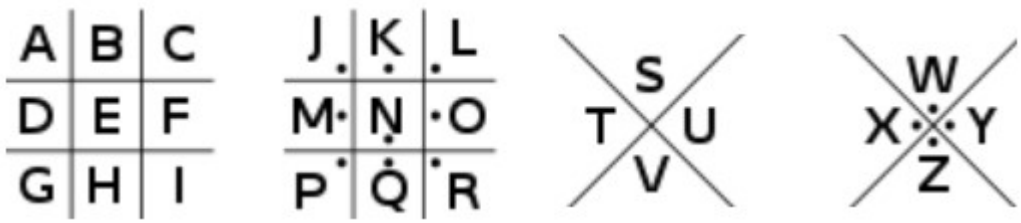
HILL ŞİFRELEME TEKNİĞİ

Bu şifreleme yöntemi, blok şifreleme yöntemi kullanılarak oluşturulur. Metinler, bloklara ayrılarak her biri ayrı ayrı şifrelenir. Metinlerin, karakterlerle değer biçimde çarpılması sonucunda yeni karakterler elde edilir.

PIGPEN ŞİFRELEME TEKNİĞİ

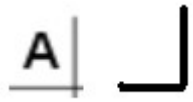
Pigpen şifrelemesi (pigpen cipher) 18. Yüzyılda freemason (özgür masonlar) tarafından kullanılan bir sistemin ismidir. Bu sistemde her harf bir sembol ile gösterilir. Yani sistemde herhangi bir hesaplama gerekmeksizin klasik Latin alfabesindeki semboller farklı sembollerle değiştirilir.

Sembollerin üretildiği şekiller aşağıda verilmiştir:



Yukarıdaki şekillerin içerisine yerleştirilen semboller, yerleştirildikleri şekil itibariyle farklı sembollerin üretilmesi için kullanılırlar.

Örneğin A harfinin yerleştiği geometrik şekil ters L sembolüdür:



Yukarıda, harfin yerleştiği geometrik yapı ve sembol sırayla gösterilmiştir. Benzer şekilde V harfinin bulunduğu sembol aşağıda verilmiştir:

Görüldüğü üzere her şeklin, harfe bakan kısmının alınması ile bir sembol tablosu oluşur:

Yukarıdaki bilgiler ışığında örneğin “sadi evren seker” dizgisini (String) şifreleyecek olursak aşağıdaki şekilde bir sonuç elde edilir:

Görüldüğü üzere şifreleme işlemi sırasında yapılan tek işlem, Latin alfabesindeki harfleri gösteren sembollerin bire bir değiştirilmesidir. Sistem açılırken de benzer bir uygulama yapılır ve şifrelenmiş metnindeki semboller, Latin harflerine dönüştürülür.

Bu sistemin bir şifreleme sistemi olarak kabul edilmemesinin altında yatan sebep ise, sistemde herhangi bir hesaplamanın bulunmayışıdır. Örneğin kirchoff prensibine göre, bir sistemin şifreleme sistemi olabilmesi için sistemin tamamen bilinmesine rağmen güvenlik sağlayabilmesidir. Bu sistemde ise, sistemi bilen birinse karşı bir güvenlik söz konusu değildir. Sistemin çalışması bilindikten sonra bilen kişi bütün şifreli mesajları rahatlıkla açabilir.

FREKANS ANALİZİ ŞİFRELEME TEKNİĞİ

Frekans analizi, bir alfabede harflerin kullanım sıklığına göre yapılan değerlendirmedir. Yani şifrelenmiş metinde en çok kullanılmış harf belirlenir ve bu harf kullanılan dilde en çok kullanılan frekansı en yüksek harfle eşleştirilerek, düz metin bulunmaya çalışılır. ⎪ Bu şifreli metin frekans analizi ile çözülmeye çalışıldığında dildeki frekans ile örtüşecektir.

VIGENERE POLI ALFABETİK ŞİFRELEME TEKNİĞİ

• Polialfabetik şifrelemede ise, anahtara bağlı olarak her harf alfabede birden fazla harfle eşleşmektedir. • Bu tip şifreleme, mono alfabetik yöntemlerden farklı olarak, bir harf değiştirilince her seferinde aynı harfe dönülmez. • Bu işlem,”VigenereTablosu” olarak bilinen bir tablo ile gerçekleştirilir. • Bu yaklaşımla bir mesajın şifrelenebilmesi için, bir anahtar kelimeye ihtiyaç vardır. •

Bunun bir örnek verelim. “EİMZA KULLANMALIYIZ” cümlesi şifrelenecek mesajmızın olsun. “HEMEN” kelimesini ise, anahtar kelime olarak seçilsin. Bu harflere karşılık olarak, anahtar kelimenin yardımıyla Tablodan yeni harfler

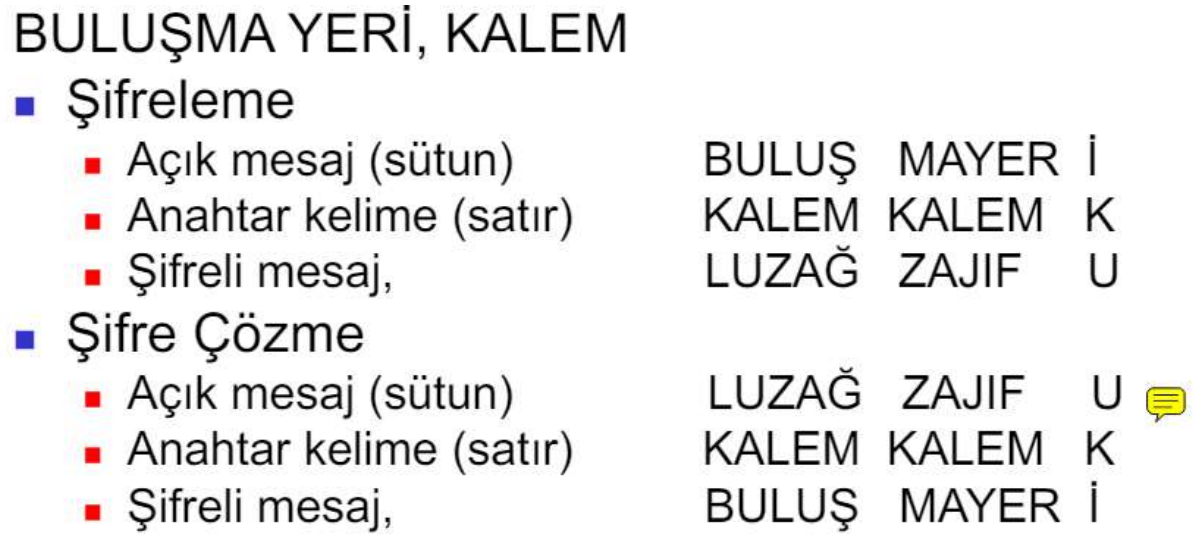
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Açık Mesaj	EİMZA	KULLA	NMALI
Anahtar kelime	HEMEN	HEMEN	HEMEN
Şifreli Mesaj	LNBDN	ŞİAPN	ÜRMPV

- Elde edilen şifrelenmiş mesajın şifrelerinin çözümü için, aynı anahtar “HEMEN” kullanılmalıdır. Deşifreleme işlemi ise, aşağıda verilen adımlarda gerçekleştirilir ve bu işlemler sonucunda şifrelenmiş olan karakterler tekrar geri elde edilebilir.

Şifreli Mesaj	LNBDN	ŞİAPN	ÜRMPV
Anahtar kelime	HEMEN	HEMEN	HEMEN
Açık Mesaj	EİMZA	KULLA	NMALI

- Böylece, başlangıçta şifrelenen açık metin yukarıda verildiği gibi tekrar geri elde edilebilir.



BINARY ŞİFRELEME TEKNİĞİ

Binary Şifreleme Tekniği temelde veri iletimi sırasında veri kaybını önleme amacıyla geliştirilmiş bir kodlama tekniğidir. Bilgisayar dilinde şifrelenmiş bir metnin şifresini çözerken (decrypt) bu metodu kullanmak gerekir. Temelde matematikteki ikili sayı sistemine dayanır.

Veri iletimi sırasında veri kaybını önlemek amacıyla geliştirilmiş bir kodlama tekniğidir. Bir çoğumuz bunu Base64 şifreleme yöntemi olarak biliriz ama **Base64 bir şifreleme yöntemi değil, bir kodlama yöntemidir**.Peki nasıl çalışır bu kodlama yönetmi ?

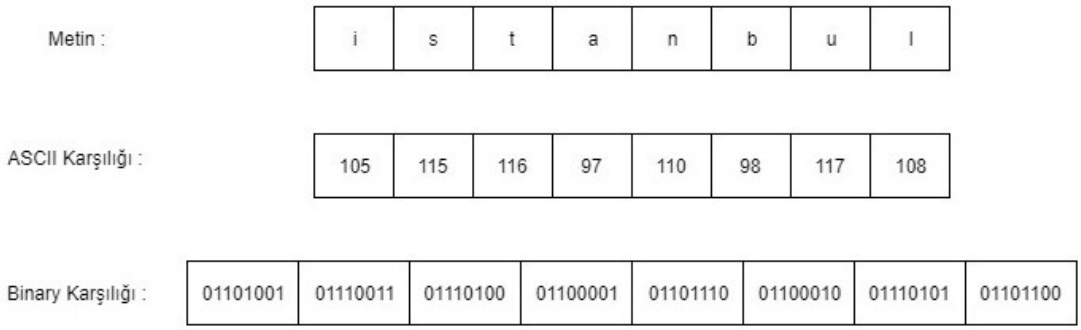
Kodlanmak istenen veri öncelikle karakter karakter ayrılır. Daha sonra her bir karakterin 8 bit uzunluğundaki binary karşılığı bulunur.Bulunan 8 bitlik ifadeler yan yana yazılır ve tekrar 6-bitlik gruplara bölünür . Her bir 6-bitlik grubun Base64 alfabesindeki karşılığı yazılır ve kodlama işlemi tamamlanır.Kod çözme işlemi(Decode) içinde aynı işlemlerin tersi uygulanır.

Örnek

Kodlanacak Metin : istanbul

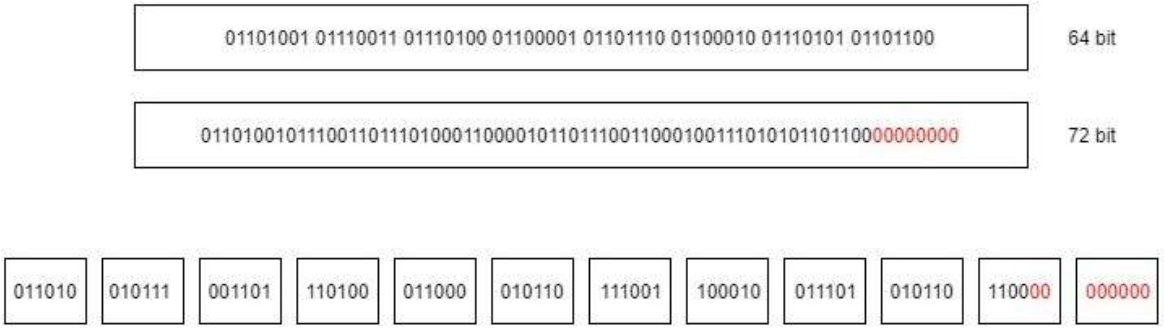
***Aşama-1**: Binary Karşılığını Bul*

Öncelikle **“istanbul”** kelimesinin herbir karakterinin ASCII karşılığını bulacağız , daha sonrada bulduğumuz herbir decimal değerin 8-bitlik binary karşılığını hesaplayacağız , dolayısıyla istanbul kelimesinin binary karşılığını bulmuş olacağız.



***Aşama-2**: 6-bitlik kısımlara ayır*

Şimdide bulduğumuz binary değerini 6-bitlik kısımlara ayıracağız.Bu aşama algoritmanın en önemli aşaması diyebilirim.Çünkü 6-bit kısımlara ayırma işlemi yaparken eğer değerimizin uzunluğu 6 nın katı değil ise 6'nın katı olana dek sonuna 8 bit uzunluğunda '00000000' değerini ekleyeceğiz. "istanbul" kelimsenin herbir harfinin binary karşılığını yan yana yazdığımız zaman uzunluğu 64 bit oluyor.Fakat 64 altının katı olmadığı için sonuna 8 bit uzunluğunda 0 ekliyoruz ve 72 bit oluyor yani 6 nın katına ulaşmış olduk.Bakın burası çok önemli ,66 da altının katı ama yapmadık , 72 yaptık çünkü 6 nın katına ulaşma işlemini 8 bit 0 ekleyerek yapmamız gerekiyor. Örneğin uzunluğumuz 80 bit olsaydı iki kez 8 bit ekleyecektik ve 96 ya tamamlayacaktık. Kısacası uzunluğumuzu 24 ün katına tamamlamaya çalışıyoruz.

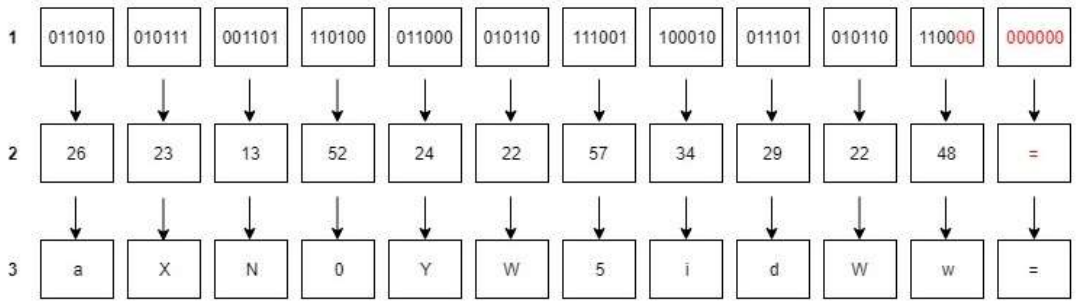


***Aşama-3**: Base64 alfabesindeki değerlerini bul*

Bu aşamada 2. aşamada bulduğumuz 6-bitlik grupların Base64 alfabesindeki karşılığını bulacağız.Önce 6-bitlik grupların decimal karşılığını hesaplaycağız , daha sonra Base64 alfabesindeki hesapladığımız decimal değere karşılık gelen karakteri bulacağız.Ama burada dikkat etmemiz gereken bir kısım var .Eğer sondaki 6-bitlik gruplar bizim eklediğimiz 0 lardan oluşuyor ise onların yerine ' **=** ' yazıyoruz.Bu önemli bir nokta çünkü biz eğer base64 ile kodlanmış metini tekrar eski haline döndürmek istediğimiz zaman ' = ' işaretlerinin sayısına bakarak bu metini kodlamak için kaç tane 8-bit lik sıfır eklendiğini biliriz.

Base64 Alfabesi

0	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	27	28	29	30	31
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
32	33	34	35	36	37	38	39	40	42	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4	5	6	7	8	9	+	/



Metin **: istanbul**

Base64 ile kodlanmış hali : **aXN0YW5idWw=**

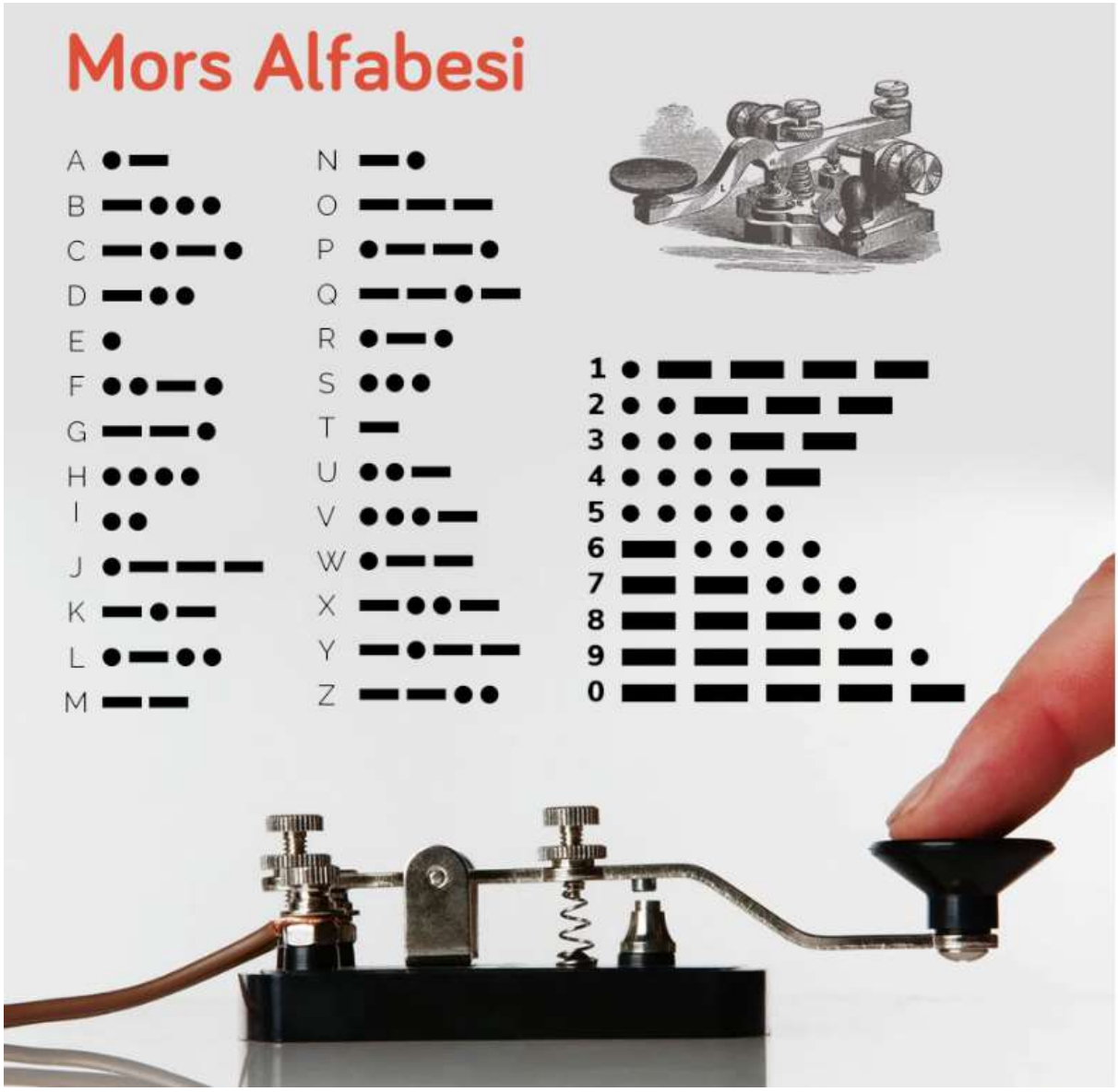
Metini geri döndürmek(Decode) içinde aşağıdan yukarıya doğru aşamalar tekrar uygulanır:

- Herbir karakterin Base64 alfabesinde karşılık gelen sayıyı bul
- Bulunan herbir sayının binary karşılığını bul
- Binary değerleri yana yana yaz ve 8-bit gruplara ayır
- Eğer sonradan eklediğimiz bitler varsa çıkar (8-bitlik 0 lar varsa)
- Herbir 8-bitlik grupların decimal değerlerini bul
- Decimal değerlere göre ASCII tablosunda karşılık gelen değeri yaz

MORS ALFABESİ ŞİFRELEME TEKNİĞİ

Mors Alfabesi ya da Mors Kodu, alfabedeki harfleri çizgiler ve noktalar ile ifade etmeye dayalı basit bir şifreleme metodudur. Çizgi ve noktaları seslerle de ifade edebilmek bu alfabeye bir şifreleme metodu olarak değer kazandırmaktadır.

-... .. .-.. .. -- .-.. . / -.- .- .-.. .. -.



Harflerin Mors Kodu Tablosu

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 _ _ . .

Sayıların Mors Kodu Tablosu

1 . – – – – –

2 . . – – – –

3 . . . – –

4 . . . . _

5 . . . . .

6 – . . . .

7 – – . . .

8 – – – . .

9 – – – – .

0 – – – – –