Polialfabetik Şifreleme (Vigenere)

- **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

Vigenere Tablosu

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

	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

Polialfabetik Şifreleme (Örnek 1)

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.

Polialfabetik Şifreleme (Örnek 2)

Bu tip şifrelemede, mono alfabetik yöntemlerden farklı olarak bir harf değiştirilince her seferinde aynı harfe dönüşmez. Vigenere tablosu buna bir örnektir.

BULUŞMA YERİ, KALEM

- Şifreleme
  - Açık mesaj (sütun) BULUŞ MAYER İ
  - Anahtar kelime (satır) KALEM KALEM K
  - Şifreli mesaj, LUZAĞ ZAJIF U
- Şifre Çözme
  - Açık mesaj (sütun) LUZAĞ ZAJIF U
  - Anahtar kelime (satır) KALEM KALEM K
  - Şifreli mesaj, BULUŞ MAYER İ

Polialfabetik Şifreleme (Değerlendirme)

- Vigenere tablosu kullanılarak yapılan şifrelemeyi çözmek, yerine koyma veya Sezar şifreleme metotlarından daha zordur, fakat imkansız değildir.
- Kullanılan anahtar uzunluğuna bağlı olarak bu zorluk artmaktadır.

One time pad (Vernam)

- Açık mesaj içinde yer alan her karakter, üretilen dizide karşısına denk gelen karakterle işleme sokularak şifreli mesaj elde edilir.
- Mesajı çözmek için rasgele dizinin bilinmesi gereklidir.
- Tek kullanımlık karakter dizisi
- Bu bir binary stream cipher
- Bu cipher mükemmel bir güvenlik veya gizlilik sağlar.
- Güvenlik rastgele üretilen diziye bağlıdır.

Vernam Şifresi (One Time Pad)

- Bu yaklaşımda, rasgele üretilen tek bir kullanmalık karakter dizisiyle şifreleme işlemi gerçekleştirilir.
- Açık mesaj içinde yer alan her karakter, üretilen dizide karşısına gelen karakterler işleme sokularak, şifreli mesaj elde edilir.
- Mesaj çözmek için rasgele dizinin bilinmesi gereklidir.

Örnek: "EİMZA KULLANMALIYIZ"

Mesaj	***EİMZA***	***KULLANMALIYIZ***
Rasgele dizi	***HNMET***	***KSYROQAZWPGLU***
Şifreli mesaj	***LYBDT***	***VNJFOĞMCKAEUU***

- Bu yöntemde güvenlik rasgele üretilen diziye bağlı olduğundan bu şifreleme sistemi, "mükemmel bir şifreleme yöntemi "olarak da bilinir.
- Burada mükemmeliği sağlayan husus, rasgele dizinin gerçekten rasgele olarak seçilmesi ve anahtar uzunluğu ile aynı olmasıdır

Vernam Şifresi (One Time Pad)

- Mesaj dizini rasgele üretilen bir diziye karşılık gelen harfler ile şifrelenir.
- Şifrenin çözülmesi, bu rasgele anahtarın bilinmesi ile mümkün olur.
- Tek kullanımlık üretilen anahtar ile oluşturulan bu şifreleme mükemmel şifreleme yaklaşımı olarak kabul edilmektedir.

Şifreleme Fonksiyonu

```
      H        E        L        L        O  message
   7 (H)    4 (E)   11 (L)   11 (L)   14 (O) message
+ 23 (X)   12 (M)    2 (C)   10 (K)   11 (L) key
= 30       16       13       21       25     message + key
=  4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z) (message + key) mod 26
      E        Q        N        V        Z  → ciphertext
```

Deşifre Fonksiyonu

```
      E        Q        N        V        Z  ciphertext
   4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z) ciphertext
-  23 (X)   12 (M)    2 (C)   10 (K)   11 (L) key
= -19       4        11       11       14     ciphertext - key
=   7 (H)    4 (E)   11 (L)   11 (L)   14 (O) ciphertext - key (mod 26)
      H        E        L        L        O  → message
```

Vernam Şifresi (One Time Pad)

X = (x1 x2 …….xn) Düz Metin

K = (k1 k2 …….kn) Düz Metin
Uzunluğunda Rasgele Anahtar Dizini

Y = (y1 y2 …….yn) Şifreli Metin

Şifreleme Fonksiyonu

Y = ek(X)= (x1+k1 x2+ k2 …….xn+ kn)
Deşifre Fonksiyonu

X = dk(Y)= (y1+k1 y2+ k2 …….yn+ kn)

Cebirsel İşlemlere Dayalı Şifreler

- Bu yöntemde hesaplama çarpı, bölü, toplam, eksi ve bunun algoritması sembolu:
- B(I)+C

B(I) ASCII'ni karşılığıdır. C sabit. Sadece toplamı kullanarak ne kadar çok algoritma kullanırsak o kadar şifreleme güvenli olur.

Lineer Denklemler:

Y=a+bx

Örneğin: y=a+bx, burada a ve b sabit lineer denklemde de bu bizim iki sabit anahtarımız olur. Eğer desek anahtar 2ve 1/2 ve bu halde

Y=2+1/2x

X burada ASCII'ni karşılar

Metnin aşağıdaki gibi olduğunu varsayalım:

CHANGE KEYS TODAY

Cebirsel İşlemlere Dayalı Şifreler

AÇIK METİN	*ASCII değeri*
CHANGE	67 72 65 78 71 69
KEYS	75 69 89 83
TODAY	84 79 68 65 89

ASCII değeri aşağıdaki operasyonla yeni bir grup parolalı değere dönüştürecektir.

2+1/2(67) =2+33.5=35.5

Bundan sonra açık metnin her harfi için yeni bir değer üretebiliriz. Bu yeni değerler şifreli metin olarak kullanılabilir. Yukarıda geçen metnin şifresi aşağıdaki gibidir:

AÇIK METİN	*PAROLALI METİN*
CHANGE	35.5 38 34.5 41 37.5 36.5
KEYS	39.5 36.5 46.5 43.5
TODAY	44 41.5 36 34.5 46.5

XOR yöntemi

Bu yöntemde;

- **şifreleme ve deşifreleme için aynı anahtar kullanılır.**

Örneğin

Düz Metin	1 1 0 1 0
Anahtar	0 1 0 1 0
Düz Metin	1 0 0 0 0
Anahtar	0 1 0 1 0
Düz Metin	1 1 0 1 0

Playfair Cipher (diagraphic)

P(ON) ⟶ C(ND)

P(CB) ⟶ C(EC)

İki harf bir sütunda ise değiştirilir, alttaki harf ile sağdaki değil

P(EX) ⟶ C(KD)

P(BQ) ⟶ C(HV)

P(TL) ⟶ C(ZT)

Eğer iki harf aynı satırda veya aynı sütunda değil ise yani (diagonal) ise örnek:

P(KQ) ⟶ C(HS)

P(ZR) ⟶ C(WT)

Eğer "I/J" ise

A- I,J,I,J…….. **B- J,I,J,I……..**

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

Playfair Cipher (diagraphic)

- Bu tablo 5*5 bir matristen oluşmuştur.
- İngilizcede I ile J bir kelimede yan yan gelmesi nadirdir.
- Anahtar özelliği:

1. On harfi geçmemelidir.
2. Aynı harfler tekrarlanmamalıdır.
3. Matrisin ilk satırında yazılmalıdır.

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

Anahtar: PALMERSTON

Şifre şeması:

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

Şifreleme:

SF açık metni şifrelemek için; şemada kenarları SF olan bir dikdörtgen çiziniz ve SF için diğer köşeler olan "oc" alınız. Sıra seçimi ise aynı satırda olduğundan!

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

İkililer aynı satırda iseler
İlk sağındakiler ile değiştiriniz;
Harf sonda ise aynı satırın
başına geçiniz. (devirsel)

Örnek: BD ⟶ cf yada CG ⟶ db

Aynı sutünda iseler örneğin; AI ⟶ sw
yada LX ⟶ tl .

Eğer ikili aynı harften oluşuyorsa biri X olarak
değiştirilir. Örneğin; BALLOON kelimesi
BA LX LO ON değişim yapılır ve şifrelenir:
cp tl mt nr (şifreleme de j kullanılmaz sadece i
vardır!)

Örnek1:

Repeated letters in the same chunk are usually separated by an X. The message, "HELLO ONE AND ALL" would become "HE LX LO ON EA ND AL LX". Since there was not an even number of letters in the message, it was padded with a spare X.

- Using "playfair example" as the key (assuming that I and J are interchangeable), the table becomes (omitted letters in red):

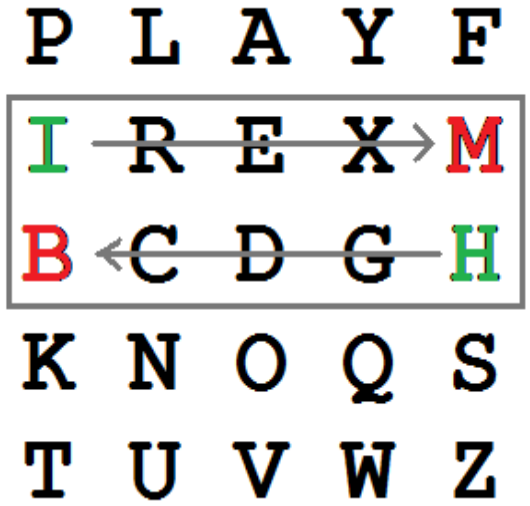
P L A Y F A
I R E X A M PLE A
B C D EF G H I=J
K LM N O P Q R S
T U V W XY Z

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

Encrypting the message "Hide the gold in the tree stump" (note the null "X" used to separate the repeated "E"s) :

- HI DE TH EG OL DI NT HE TR EX ES TU MP

1. The pair HI forms a rectangle, replace it with BM



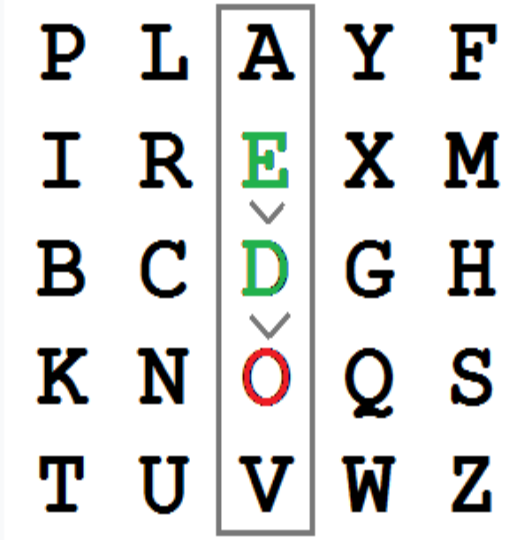
HI

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

BM

- HI DE TH EG OL DI NT HE TR EX ES TU MP

2. The pair DE is in a column, replace it with OD



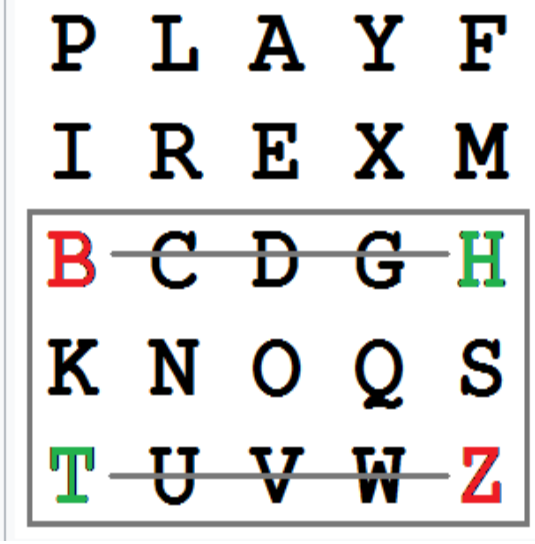
DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

- HI DE TH EG OL DI NT HE TR EX ES TU MP

3. The pair TH forms a rectangle, replace it with ZB



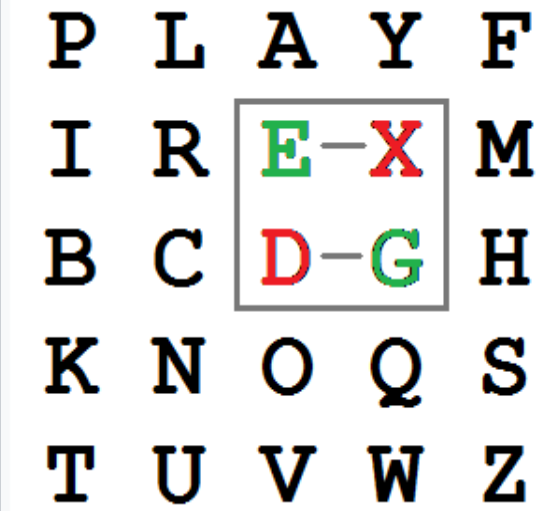
TH

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

ZB

- HI DE TH EG OL DI NT HE TR EX ES TU MP

4. The pair EG forms a rectangle, replace it with XD



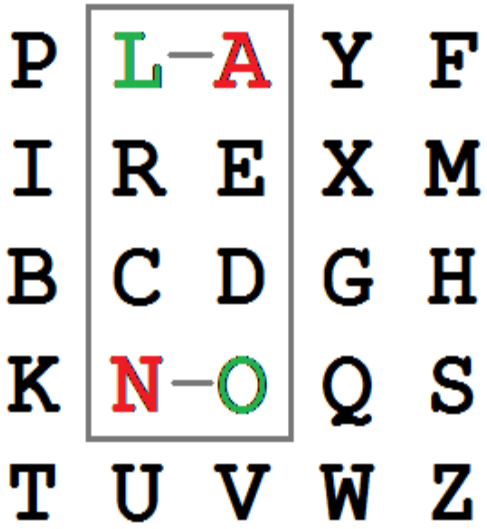
EG

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

XD

- HI DE TH EG OL DI NT HE TR EX ES TU MP

5. The pair OL forms a rectangle, replace it with NA



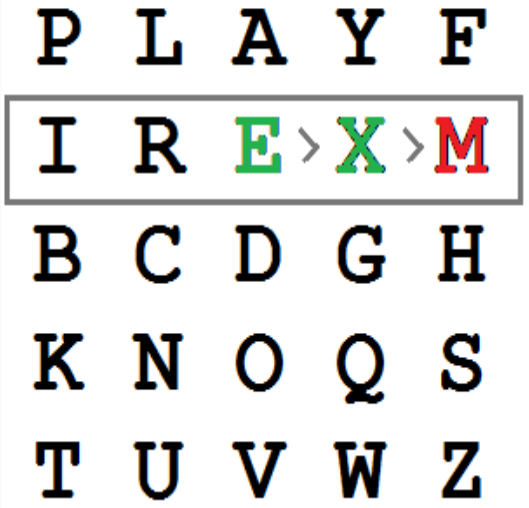
OL

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

NA

- HI DE TH EG OL DI NT HE TR EX ES TU MP

6. The pair DI forms a rectangle, replace it with BE
7. The pair NT forms a rectangle, replace it with KU
8. The pair HE forms a rectangle, replace it with DM
9. The pair TR forms a rectangle, replace it with UI
10. The pair EX (X inserted to split EE) is in a row, replace it with XM



EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

XM

11. The pair ES forms a rectangle, replace it with MO
12. The pair TU is in a row, replace it with UV
13. The pair MP forms a rectangle, replace it with IF

BM OD ZB XD NA BE KU
DM UI XM MO UV IF