Playfair cryptography algorithm document

رمزنگاری پلیفیر یا **مربع پلیفیر** یا **رمزنگاری پلیفیر** ویت استون یک روش رمزنگاری متقارن است و اولین رمزنگاری جانشینی دیاگرام بوده و طرح آن اولین بار در سال **1854** توسط چارلز ویت‌استون اختراع شده است. ولی به دلیل ارتقای آن توسط لرد پلیفیر، نام پلیفیر به آن اطلاق می‌شود.

این روش جفت حروف (دیاگرام یا بیگرام) را به جای حروف در رمزنگاری جانشینی و نه سیستم‌های رمزنگاری ویژنر رمزنگاری می‌کند. شکستن رمز پلیفیر سخت‌تر است زیرا تحلیل فرکانسی که برای رمزهای جانشینی ساده به کار می‌رود، در آن کارایی ندارد. می‌توان بیگرام‌ها را به صورت فرکانسی تحلیل کرد، ولی خیلی سخت‌تر است. با **600** بیگرام احتمالی به جای **26** مونوگرام احتمالی (تک علامت‌ها، در این حوزه معمولا همان حروف الفبا است) به متن رمز بزرگتری نیاز است.

توصیف

رمز پلیفیر از یک جدول **5** در **5** استفاده می‌کند که شامل عبارت یا واژه کلید است. به خاطرسپاری کلیدواژه و **4** قاعده کل چیزی است که برای ایجاد یک جدول **5** در **5** و استفاده از رمز لازم است.

برای تولید جدول کلید، می‌توان اول فضاهای جدول را با حروف کلیدواژه پر کرد و سپس فضاهای باقیمانده را با حرف‌های دیگر الفبا به ترتیب(معمولا با حذف **«J»** یا **«Q»** برای کاهش حرف الفبا به منظور جا شدن در **26** حروف الفبا در جدول)پر کرد. کلید می‌تواند در ردیف‌های بالای جدول از چپ به راست یا در الگوهای دیگر مانند شروع مارپیچی از گوشه‌ی بالا چپ و پایان در مرکز نوشته شود کلیدواژه به همراه قراردادها برای پرکردن جدول **5** در **5** کلید رمز را تشکیل می‌دهند.

برای رمزنگاری یک پیام، می‌توان پیام را به دیاگرام (گروه‌های دو حرفی) تقسیم کرد به طوری که مثلا **«Hello World»** به **« HE LL OW OR LD»** تبدیل می‌شود. این دیاگرام‌ها با

استفاده از جدول کلید جایگزین می‌شوند. چون رمزنگاری از جفت حروف استفاده می‌کند، به پیام‌هایی با تعداد حرف فرد معمولا یک حرف غیر رایج مانند **«X»** اضافه میشوند تا دیاگرام نهایی را کامل کنند. دو حرف از دیاگرام در گوشه‌های مقابل هم در یک مستطیل در جدول کلید قرار می‌گیرند. برای انجام جانشینی، قاعده‌های زیر را بر حروف در یک متن ساده اعمال کنید:

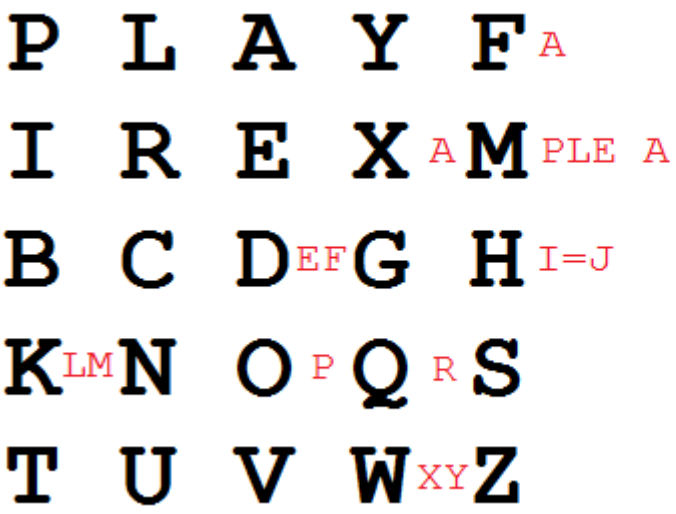
1. اگر هر دو حرف شبیه هم بودند (یا تنها یک حرف باقی مانده)، یک **X** را پس از حرف اول اضافه کنید. جفت جدید را رمزگذاری کرده و ادامه دهید. بعضی از انواع پلیفیر از **«Q»** به جای **«X»** استفاده میکنند.
2. اگر حروف در همان ردیف جدول شما ظاهر می شوند ، به ترتیب آنها را با حروف سمت راست خود جایگزین کنید (اگر حروف اصلی در سمت راست ردیف قرار داشت ، از حرف سمت چپ ردیف استفاده کنید).
3. اگر حروف در همان ستون جدول شما ظاهر می شوند ، به ترتیب آنها را با حروف زیر خود جایگزین کنید (اگر به حروف اصلی در قسمت پایین ستون قرار داشت ،از حرف بالای ستون استفاده کنید).
4. اگر حروف در یک ردیف یا ستون نیستند ، حرف اول را با حرفی که در سطر حرف اول و ستون حرف دوم است جایگزین میکنیم. حرف دوم را با حرفی که در سطر حرف دوم و ستون حرف اول است جایگزین میکنیم.

برای رمزگشایی، از برعکس سه قاعده‌ی آخر استفاده کنید و از قاعده‌ی اول بدون تغییر آن استفاده کنید(**«X»** و **«Q»** های اضافی را حذف کنید به دلیل اینکه وقتی پیام کامل شد هیچ معنی خاصی ندارند.)

چندین نوع جزیی دیگر از رمز پلیفیر اصلی وجود دارد.

مثال

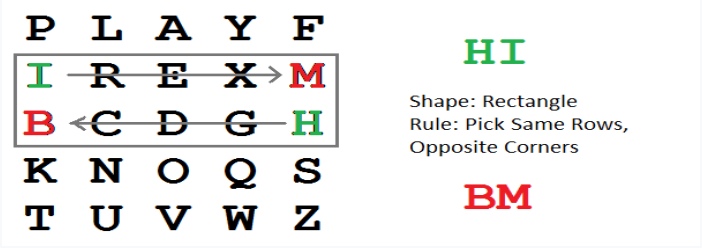
با استفاده از **"playfair exmaple"** به عنوان کلید(با فرض اینکه **I** و **J** قابل تعویض هستند)، جدول به صورت زیر در می‌آید:(حروف قرمز رنگ حذف میشوند):

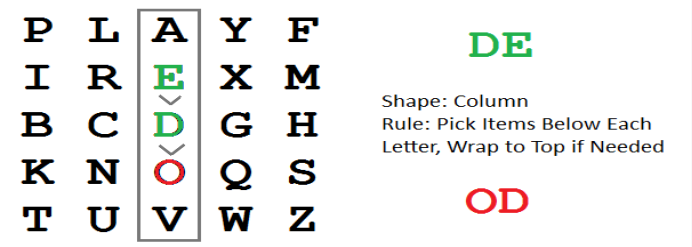
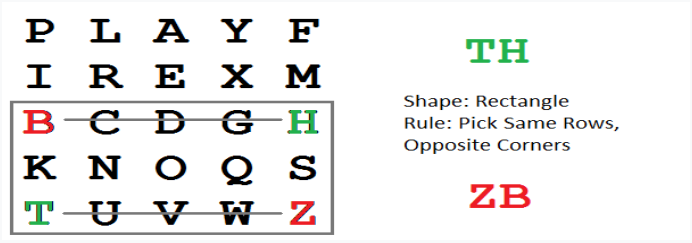
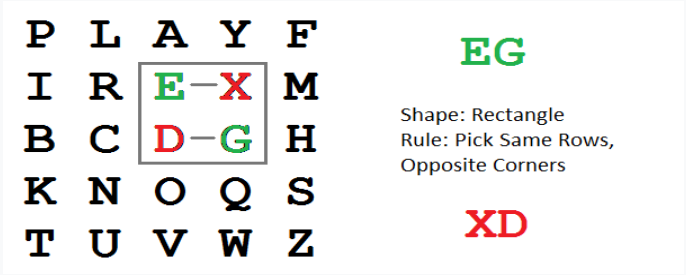
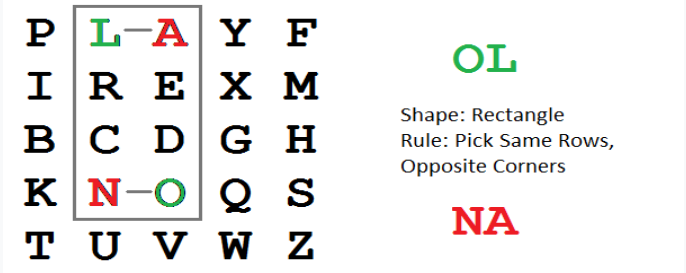


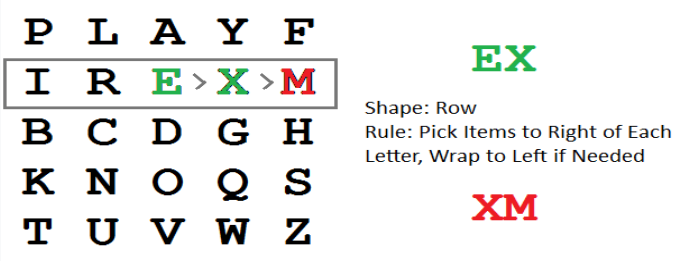

```
P L A Y F
I R E X M
B C D G H
K N O Q S
T U V W Z
```

رپیام "Hide the gold in the tree stump" را رمزنگاری میکنیم(توجه داشته باشید حرف "X" که برای جدا کردن تکرار "E" در کلمه "tree" استفاده می شود) :

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

1جفت HI یک مستطیل تشکیل می دهد ، آن را با BM جایگزین کنید	

2جفت DE در یک ستون است ، آن را با ODجایگزین کنید	
3جفت TH مستطیل را تشکیل می دهد ، آن را با ZB جایگزین کنید	
4جفت EG یک مستطیل تشکیل می دهد ، آن را با XD جایگزین کنید	
5جفت OL یک مستطیل تشکیل می دهد ، آن را با NA جایگزین کنید	
6جفت DI مستطیل را تشکیل می دهد ، آن را با BE جایگزین کنید	
7جفت NT مستطیل را تشکیل می دهد ، آن را با KU جایگزین کنید	

8جفت HE مستطیل را تشکیل می دهد ، آن را با DM جایگزین کنید	
9جفت TR مستطیل را تشکیل می دهد ، آن را با UI جایگزین کنید	
10جفت EX (X درج شده برای تقسیم EE) در یک ردیف قرار دارد ، آن را با XM جایگزین کنید	
11جفت ES مستطیل را تشکیل می دهد ، آن را با MO جایگزین کنید	
12جفت TU در یک ردیف است ، آن را با UVتعویض کنید	
13جفت MP مستطیل را تشکیل می دهد ، آن را با IF جایگزین کنید	

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

بنابراین پیام **"Hide the gold in the tree stump"** تبدیل می شود **"BMODZ BXDNA BEKUD MUIXM MOUVI F"**

فرض کنید شخصی بخواهد رمزنگاری **OR** را رمزگذاری کند. پنج مورد کلی وجود دارد:

1)

```
* * * * *
* O Y R Z
* * * * *
* * * * *
* * * * *
```

Hence, OR → YZ

2)

```
* * O * *
* * B * *
* * * * *
* * R * *
* * Y * *
```

Hence, OR → BY

3)

```
Z * * O *
* * * * *
* * * * *
R * * X *
* * * * *
```

Hence, OR → ZX

4)

```
* * * * *
* * * * *
* O R C *
* * * * *
* * * * *
```

Hence, OR → RC

تحلیل رمز

اگر متن کافی وجود داشته باشد رمز پلیفیر مانند اغلب رمزهای کلاسیک می‌تواند به راحتی کرک شود. اگر متن ساده و متن رمز معلوم باشند، دستیابی به رمز بسیار ساده است. وقتی تنها متن رمز معلوم باشد، تحلیل رمز شامل جستجو در فضای کلید برای یافتن تعداد تطبیق بین تعداد وقوع حرف در دیاگرام و تعداد وقوع حرف در پیام اصلی است .

تحلیل رمز در پلیفیر شبیه تحلیل رمز رمزهای **4** مربعی و دو مربعی است، هرچند سادگی نسبی سیستم پلیفیر باعث ساده‌تر شدن شناسایی رشته‌های متن ساده می‌شود. یک دیاگراف پلیفیر و معکوس آن(مانند **AB** و**BA**)به الگوی حروفی مشابه در متن ساده رمزگشایی می‌شوند(مانند **RE**و **ER**). در زبان انگلیسی، کلمات زیادی وجود دارند که شامل این دیاگراف‌های معکوس هستند مانند **REceivER** و**DEpartED** . شناسایی دیاگراف‌های معکوس نزدیک در متن

رمز و تطبیق دادن آن به یک فهرست از واژه‌های شناخته شده که شامل اینطور کلمات است،راهی ساده برای تولید متن اصلی برای شروع ساخت کلید است.

یک رویکرد متفاوت برای مقابله با رمز پلیفیر استفاده از روش **shotgun hill climbing** است. این با یک مربع تصادفی از حروف شروع می‌شود. تغییرات جزیی ایجاد میشوند (یعنی تغییر حروف، ردیف یا منعکس‌کردن کل مربع) تا بررسی شود که متن به وجود امده از مربع، شباهت بیشتری به متن اصلی استاندارد دارد یا خیر. اگر مربع جدید یک بهبود در نظر گرفته شود، آنگاه پذیرفته شده و سپس جهش می‌یابد(همان تغییرات جزئی ایجاد میشوند) تا یک نامزد بهتر پیدا شود. در نهایت، متن اصلی چیزی بسیار شبیه یافت می‌شود. این فراتر از شکیبایی انسان معمولی است، ولی کامپیوترها می‌توانند از این الگوریتم برای رمزگشایی رمزهای پلیفیر با یک متن نسبتا کوچک استفاده کنند.

جنبه‌ی دیگر در پلیفیر که آن را از رمزهای دومربعی و چهارمربعی جدا می‌کند این است که هیچ وقت شامل یک دیاگرام دو حرفی مشابه مانند **EE** نیست. اگر دیاگرام‌های دوحرفی مشابهی در متن رمز وجود نداشته باشد و طول پیام به اندازه‌ی کافی بلند باشد تا این احتمال را از نظر آماری بامعنی کند، به احتمال زیاد روش رمزنگاری یک پلیفیر است.

یک راهنمای خوب برای ساخت یک کلید برای یک رمز پلیفیر در فصل **7** کتاب «راهکاری در سیستم‌های جایگذاری پلی‌گرافیک» یافت می‌شود که توسط ارتش ایالات متحده تولید شده است.
تحلیل رمز دیگر برای رمز پلیفیر در فصل **11** در کتاب **Helen Fouché Gaines, *Cryptanalysis / a study of ciphers and their solutions***یافت می‌شود .

تحلیل دقیق رمز پلیفیر در فصل **28** در کتاب **Dorothy L. Sayers** با عنوان ***Have His Carcase***یافت می‌شود. در این داستان، نشان داده شده که یک پیام پلیفیر از نظر گرافیک رمزی ضعیف بوده و کارگاه به راحتی می‌تواند کل کلید را با استفاده از تنها چند حدس برای تغییر فرمت پیام حل کند (در این مورد، پیام با نام یک شهر و سپس با تاریخ آغاز می‌شود).

کتاب سایرس شامل یک توصیف دقیق از مکانیک رمزنگاری پلیفیر و دستورالعمل گام به گام تحلیل رمز است.

ارتش، نیروی دریایی و پلیس آلمان از سیستم پلیفیر دوگانه به عنوان یک رمز متوسط در جنگ جهانی دوم استفاده کردند، ولی چون آن‌ها رمزها را در جنگ جهانی اول توانسته‌اند که بشکنند، از روش مربع دوم استفاده کردند که حرف دوم در هر بی‌گرام در آن انتخاب شد و در کلیدواژه توزیع شد و به صورت تصادفی جانشین حرف پیام شده است. ولی به دلیل طرفداری آلمان از پیام‌های **pro forma**، آن‌ها در **Bletchley Park** رمزگشایی شدند. چند عدد قبل از پیام‌ها اضافه شدند. چون اعداد آلمانی از **1 (eins)** تا **12 (zwölf)** شامل تمامی حرف در مربع‌های پلیفیر دوگانه به غیر از **8** مورد هستند، شکستن ترافیک **pro forma** نسبتا آسان بود.

کاربرد در جدول‌های مدرن

جدول‌های متقاطع رمزدار و مدرن مانند جدول لیسنر گاهاً از روش رمزهای پلیفیر استفاده می‌کنند. معمولا بین **4** تا **6** پاسخ باید به شبکه‌ی کد وارد شود و عبارت کلید در پلیفیر برای حل نهایی مهم است.

رمز، خود را به پازل‌های جدول متقاطع وام می‌دهد، زیرا متن اصلی با حل یک مجموعه از سرنخ‌ها به دست می‌آید، ولی متن رمزدار با حل موارد دیگر به دست می‌آید. حلگرها می‌توانند جدول کلید را با جفت‌کردن دیاگرام‌ها بسازند (گاهی اوقات امکان دارد تا کلیدواژه را حدس زد ولی هیچ وقت ضرورت ندارد).

استفاده از رمز پلیفیر به عنوان بخشی از مقدمه‌ی جدول متقاطع توضیح داده می‌شود. این کار را برای حلگرهایی مسطح می‌کند که قبلا با رمز سروکار نداشته‌اند. ولی روش استفاده از رمز همیشه یکسان است. از الفبای **25** حرفی شامل **Q** و کاربرد همزمان از **I** و **J** استفاده می‌شود. جدول کلید همیشه سطر به سطر پر می‌شود.