رمز playfair

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 ۱۸۵۴ 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 ۶۰۰ [۱]بیگرام احتمالی به جای ۲۶ مونوگرام احتمالی (تک علامت‌ها، در این حوزه معمولا همان حروف الفبا است) به متن رمز بزرگتری نیاز است.

رمز پلیفیر از یک جدول ۵ در ۵ استفاده می‌کند که شامل عبارت یا واژه کلید است. به خاطرسپاری کلیدواژه و ۴ قاعده کل چیزی است که برای ایجاد یک جدول ۵ در ۵ 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 ۲۶ 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 ۵ در ۵ 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:

۱. 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.

۲. 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).

۳. 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).

٤. 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).

پیاده سازی در **Cryptool**:

ابتدا در قسمت templates>>Cryptography>>Classical>>Playfair Cipher را باز میکنیم.

در قسمت Plaintext متن اصلی Faeze را وارد می کنیم. در قسمت Key phrase کلید را Karami در نظر میگیریم. و با زدن کلید start متن اصلی در فرمت FAEZEX در می آید و متن رمز شده MFIVGV خواهد بود.