**الگوریتم رمز playfair**

این الگوریتم رمزنگاری در سال 1854 میلادی توسط چارلز واتسون ابداع شد همانگونه که در سایت ویکی عنوان شده است دلیل نامگذاری این الگوریتم به نام پلایفیر، استفاده از نام استفاده کننده آن لرد پلایفیر میباشد.

این الگوریتم توسط ارتش انگلیس درجنگ جهانی اول و دوم مورد استفاده قرار گرفت. رمزنگاری در این روش به وسیله جایگشت دوحرفی با استفاده از یک ماتریس 5×5 صورت می پذیرد. این الگوریتم روشی مشابه با الگوریتم رمزنگاری ویگنر دارد ولی از آن پیچیده تر است. با این حال می بایست این نکته را مد نظر قرارداد که با کامپیوترهای امروزی تحلیل و شکستن این الگوریتم به آسانی صورت می پذیرد.

**روش رمزنگاری**

در این روش در ابتدا از یک جدول 5×5 برای استفاده شده و بر اساس کلید انتخابی حروف درون جدول ساخته شده و متن مورد استفاده برای رمزنگاری براساس ترکیب موجود در جدول به رمز در می آید. مراحل انجام کار با ذکر مثال به شرح زیر انجا می شود

**مرحله اول - ساخت جدول 5\*5**

جدول 5×5 به عنوان ابزاری برای رمزنگاری استفاده میشود . تعداد حروف زبان انگلیسی 26 حرف است. برای انطباق حروف زبان انگلیسی با جدول 25 حرفی معمولا حرف Q را حذف کرده و یا حروف I,J را یکسان درنظر میگیرند. کلید مورد استفاده برای رمزنگاری انتخاب شده و به ترتیب از چپ به راست در جدول جایگذاری می شود. در جایگذاری حروف از تکرار جلوگیری شده و پس از جایگذاری سایر حروف باقیمانده در جدول جایگزین می شود. برای مثال فرض کنید بخواهیم از کلمه chronology بعنوان کلمه کلیدی استفاده کنیم جدول 5×5 را به شرح زیر پرخواهیم نمود .

C H R O N

L G Y A B

D E F I K

M P Q S T

U V W X Z

**مرحله دوم - فرایند رمزنگاری**

پس از تشکیل جدول که توضیح آن درمرحله اول ارائه شد نوبت به رمزنگاری می رسد. برای این امر متنی مورد نظر را به صورت ترکیبی دو حرفی تفکیک میکنیم به عنوان مثال برای متن انگلیسی زیر

This particular cipher

فاصله بین حروف را حذف نموده و با دسته بندی حروف به شرح زیر قالب اولیه رمزنگاری را ایجاد میکنیم

th is pa rt ic ul ar ci ph er

برای رمزنگاری اقدامات زیر انجام می شود.

1. درصورتی که تعداد حروف فرد باشد اخرین حرف باقیمانده را با حرف z ترکیب و دو حرفی مورد نظر را ایجاد میکنیم

2. در صورتی که حرف تکراری در بین جمله وجود داشته باشد مابین دو حرف تکراری حرف x را جایگزین میکنیم

3. درصورت پشت سر هم قرار گرفتن دو حرف درکار هم در جدول در ترکیب افقی حرف سمت راست ودر ترکیب عمودی حرف پائین جایگزین می شود.

4. درصورتی که حروف در یک سطر و ستون نباشند با تشکیل یک مربع حرف موجود در گوشه مخالف حرف را جایگزین حرف موجود خواهیم نمود.

متن بدست امده از فرایند رمزنگاری به شرح زیر است

pn sx sg nq do cd yo od vg fh

**رمزگشائی**

برای رمزگشایی از متن کافی است تمامی فعالیت هایی که انجام شده است را به صورت معکوس انجام دهیم