امیرحسین شریف ۹۴۱۴۳۰۱۶ رمز play fair

## مقدمه

رمز play fairیکی از رمز های کلاسیک می باشد که توسط ویت استون در سال ۱۸۵۴ ساخته شد و اولین رمز متقارن و جانشینی دیاگرامی بوده ، ولی دوست ایشان که لرد پلی فیر(lord play fair)، آن را ارتقا بخشید و استفاده از آن بسیار تبلیغ کرد. به این دلیل به آن رمز play fair گفته می شود.

در صنایع نظامی قبل ظهور دستگاه های رمز نگاری دیجیتالی از این روش استفاده می شد.

این رمز جفت حروف را رمز نگاری می کند که در زمان خودش،حمله تحلیل فرکانسی برای آن موثر نبود،به علت این حمله تحلیل فرکانسی برای رمز های جانشینی ساده به کار می رفت و برای این رمز کاربردی نداشت. شکستن رمز play fair سخت تلقی می شد،به دلیل این که رمز های جانشینی ساده از ۲۶حروف انگلیسی استفاده که برای شکستن آن! ۲۶ وجود داشت ولی با این روش رمز نگاری حدود ۶۰۰ یا ترکیب دوتایی باید چک می شد که از این نظر این رمز جالب توجه است.

## روش رمز گذاری و رمز گشایی رمز play fair

برای رمز گذاری و همچنین رمز گشایی، رمز play fair از یک جدول استفاده می شود،برای این که بتوانیم قوانین رمز گذاری و هم چنین رمز گشایی نشان دهیم از یک مثال می کنیم. لازم به ذکر است،متن اصلی را با X و کلید را K و متن رمز شده را با Y نمایش می دهیم.

مثال : فرض کنید می خواهیم کلمه یا متن اصلی words را با کلید Apple با استفاده از رمز play fair رمز گذاری کنیم.

در ابتدا اگر کلید مورد نظر دارای حروف تکراری بود،یکی از آن ها نگه داشته و بقیه را حذف در این مثال کلید Apple دارای ۲، حرف P می باشد که یکی از آن ها حذف می کنیم در نهایت کلید می شود.

K = Aple

حال متن اصلی را در نظر گرفته و دو حرف،دو حرف جدا می کنیم،اگر روی کاغذ انجام می دهید،می توانید زیر هر دو حرف خط بکشید،اگر تعداد حروف متن اصلی فرد باشد،به انتهای آن حرفی دلخواه، به جز حروف متن اصلی و حروف کلید بگذارید، در این جا حرف دلخواه اضافه کرده زیرا words دارای ۵حرف می باشد و حرف دلخواه اضافه شده به انتها t می باشد.

X = wordst

حال جدولی ۵*۵ می کشیم و در ابتدا از چپ به راست حروف کلید می نویسیم در آن جدول،وبعد از نوشتن آن،حرف باقی مانده انگلیسی به ترتیب از ادامه آن نوشته انتها و فقط حروف i/j به این شکل و در یک خانه از جدول می نویسیم. دقت شود هیچ حرفی دوبار نمی نویسیم در این جدول.

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

حال می خواهیم رمز گذاری انجام بدهیم.

X = WORDST

حال دو حرف اول کلمه یعنی WO در جدول پیدا می کنیم. این دو حرف چون هر دو حرف سطر و ستون آن دو متفاوت است که به این شکل عمل که در همان سطر حرف W آن قدر به جلو حرکت می کنیم که هم ستون حرف دوم که در اینجا O است، بشود که در این جدول می شود حرف Z و این حرف در Y می نویسیم. برای O مشابه همین کار فقط به عقب حرکت می کنیم تا هم ستون با حرف W بشود، که آن حرف می شود K.

قانون اول در رمز گذاری play fair : اگر دو حرف دارای سطر و ستون های متفاوت بودند،در هر سطر دو حرف حرکت می کنیم تا به ستون دیگری برسند و آن حرف که در سطر هر یک دو حرف و هم ستون دیگری است را یادداشت می کنیم.

حال دو حرف بعدی R,D می باشد که در یک ستون می باشند، که در اینجا به این صورت عمل می کنیم که حروف پایینی خود در جدول جایگزین می کنیم.یعنی Rمی شود W و D می شود،K.

پس قانون دوم: اگر دو حرف هم ستون بودند با مقدار پایینی خود جایگزین می شوند.

حال دو حرف بعدی را که ST می باشند،چون در یک سطر می باشند، با حرف سمت راست در جدول جایگزین می کنیم.به این ترتیب S می شود، T و T می شود،U.

قانون سوم : اگر دو حرف در یک سطر یا ردیف باشند با حرف سمت راست جایگزین می شود.

حال رمز گذاری ، به پایان رسیده و متن رمز شده Y به این شکل است :

Y = ZKWKTU

برای رمز گشایی نیز باید از کلیدی که در اینجا استفاده کرده و با استفاده از جدولی که در بالا وجود دارد و قوانین گفته شده مقدار پیام رمز شده را به متن اصلی برگرداند و مقدار X را بازیابی کرد. فقط قانون دوم و سوم را باید برعکس انجام داده شود.

## چند نکته در مورد رمز play fair

۱- این را می توان به عنوان یکی از قانون های نیز در نظر گرفت،اگر تعداد حروف متن اصلی فرد بود و پس از جدا کردن که در بالا گفته شد،دو حرف مثل یک دیگر بودند از یک جدا کننده که معمولا حرف QیاX می باشد،استفاده می شود برای مثال اگر متن اصلی helloباشد،اگر دوتا دو حروف جدا شوند،LL کنار هم می افتند و این که تعداد حروف این کلمه ۵ است پس یک x در بین دو LL می گذاریم که می شود ۶تعداد حروف و بعد مراحل را رمز نگاری را انجام می دهیم.اگر پس از اضافه کردن جدا کننده ، تعداد حروف متن اصلی فرد شد،طبق نوشته ای که در بالا گفته شد یک حرف به انتهای آن با شرایط گفته شده،اضافه می کنیم.

۲- در قوانینی که در بالا گفته شد،برای قوانین دوم و سوم فرض کنید که جدول چرخشی است یعنی اگر برای رمز گذاری در سطر هردو حرف بودند و یکی از آن ها Q بود ، اگر بخواهیم سمت راست برویم می شود اولین حرف سمت چپ و این قانون برای پایین هم وجود دارد،یعنی اگر پایین تر حرف که هر دو حرف دریک ستون قرار گرفته باشد،مثلا Xحرف پایین آن می شود،اولین حرف بالا یعنی L و برای رمز گشایی هم این ها دستورات صادق هستند،یعنی در جدول چرخشی عمل می کنیم. یعنی قوانین برعکس شده نیز که برای رمز گشایی استفاده می شوند نیز به صورت چرخشی عمل می کنیم.
۳- اگر برای رمز گذاری به خانه جدول l/L رسیدید می توانید هر کدام که را مد نظر را بود انتخاب کنید.
۴- اگر در رمز گشایی در به خانه l/L رسیدید و حرف I را قرار دادید و متن اصلی نامفهوم بود از L استفاده کنید و برعکس.
۵- اگر بعد از رمز گشایی مقدار Xبازیابی شده و کاملا مفهوم است و حرفی اضافه نیز در آن وجود دارد می توانید آن را حذف کنید اگر در انتهای آن باشد.
۶- اگر از حرف X یا Q به عنوان جدا کننده استفاده شده باشد،پس رمز گشایی می توانید جای آن را خالی بگذارید تا مقدار بازیابی شده مفهوم یا متن اصلی درست بدست آید.
۷- در این جا از رمز گذاری play fairاز جدول ۵*۵ استفاده شده،می توان از جدول ۶*۶ نیز استفاده شود.

## نحوه ی پیاده سازی در Cryp tool

در این نرم افزار یک آیتم برای رمز گذاری play fair وجود دارد،متن یا فایل متنی را به عنوان ورودی گرفته و با استفاده جدول play fair آن را رمز نگاری می کند.تنظیمایتی که برای Play fair در نرم افزار وجود دارد،این ها می باشد،می توانید جدول ۵*۵ یا ۶*۶ را بگذارید،می توانید pair separator یا همان جدا کردن دوتا حرف های کلمه ی ورودی باشد،جدا کننده برای دو حرف مثل هم در ورودی بگذاریم . نکته ای در اینجا وجود دارد این است که برای اطمینان از این رمز درست

متن اصلی رمز نگاری می کند با یک کلید یکسان رمز نگاری و رمز گشایی که قابل تنظیم روی آیتم play fair در نرم افزار می توان مقایسه و چک کرد.اگر در کلمه ای که  می خواهیم رمز نگاری بشود j وجود داشته باشد و اگر از جدول ۵*۵ استفاده شود، آن مقدار بازیابی شده را به جای آن i می گذارد در نرم افزار و اگر ۶*۶ باشد،j می گذارد. دیگر این که می توان در آیتم  play fair کلید در درون خود آیتم تنظیم کرد،دیگر نیازی نیست حتما آن را از بیرون به آن داده شود و حتی می توان حروف را نیز می توان تغییر داد.

## نتیجه گیری

رمز پلی فیر(play fair)، در زمان قبل از ظهور سیستم های رمز نگاری دیجیتال،یک رمز امن برای کاربرد های نظامی موثر بود.چون حملات تحلیل فرکانسی بسیار زمان بر می بود و نمی توانستند به سرعت رمز بشکنند،اما در حال حاضر این رمز با استفاده کامپیوتر ها و سیستم های دیجیتال در کم تر یا حدود ۱ ثانیه شکسته می شوند. پس در حال حاضر استفاده از این روش رمز نگاری نا امن است و منسوخ شده است.

## منابع


Wikipedia

ویدیو های آموزشی درس رایانش امن