بسم الله الر حمن الرحیم

الگوریتم رمز سزار

یکی از ساده ترین وشناخته شده ترین تکنیک های رمز گذاری است.این رمز یک نوع رمز جانشینی است که دران هر حرف درمتن اشکاربا حرف دیگری با فاصله ثابت در الفبا جایگزین میشود برای مثال با مقدارانتقال3 Dبه جای A مینشیند Eبه جایBوالی اخر.نام این روش از ژولیوس سزار گرفته شده است که از ان برای ارتباطات محرمانه خود استفاده میکرد.رمز سزار معمولا به عنوان یکی از اجزای سیستم های رمزگذاری پیچیده تر مانند رمز ویژنر استفاده میشود. روت 13 یک حالت خاص رمز سزار است که از میزان انتقال 13 استفاده میکند با توجه به ان که الفبای انگلیسی از 26 حرف تشکیل شده وارون خودش است رمز سزار مانند رمزهای جانشی تک الفبایی دیگر به راحتی شکسته می شودو با وجودتکنیک های مدرن هیچ گونه امنیتی برای ارتباطات فراهم نمیکند.

شکستن رمز سزار

رمز سزار حتی در شرایط حمله متن اصلی به راحتی قابل شکسته شدن است . دوموقعیت زیر می توان در نظر گرفته شوند.

1. حمله کننده می داند یا حدس میزند که نوعی از رمز جانشینی ساده استفاده شده است اما مشخصا نمی داند که رمز سزار است.
2. حمله کننده می داند که رمز سزار استفاده شده است اما مقدار انتقال را نمیداند.

در حالت اول استفاده از تکنیک های معمول شکستن رمزهای جانشینی مانند تحلیل فراوانی به سادگی نتیجه بخش است. در حین استفاده از این تکنیک ها حمله کننده به راحتی متوجه نظم موجود درسیستم جانشینی واستفاده از رمز سزار خواهد شد.(توزیع فراوانی حروف دریک متن معمولی زبان انگلیسی به راحتی قابل تشخیص وپیش بینی است. رمز سزار این توزیع را به چپ یا به راست منتقل میکند اما شکل ان را تغییر نمی دهد.میزان انتقال به راحتی با مشاهده نمودار فراوانی قابل تشخیص خواهد بود.)

شکستن رمز در حالت دوم ساده تر از حالت اول است. از انجا که تعداد ممکن انتقال ها محدود است(در زبان انگلیسی26 حالت ممکن)اعمال حمله جستجوی فراگیر وازمایش تمام حالات ممکن به سرعت انجام میشود.

روش دیگر حمله جستجوی فراگیر با کمک تحلیل فراوانی است در این روش با مقایسه فراوانی حروف در متن رمز وفراوانی حروف در متون عادی زبان مورد استفاده وجابجایی دو نمودار می توان میزان انتقال را پیدا کرد. استفاده چند باره از رمز سزاربر روی یک متن به امنیت بیشتر منجر نمی شود.

رمز گذاری

دیل الفبای آشکار به الفبای رمز را می‌توان با هم‌ردیف کردن دو الفبا نمایش داد. الفبای رمز درواقع همان الفبای آشکار است که به میزان مشخصی به سمت راست یا چپ چرخانده شده. برای مثال، رمز سزار با چرخش به چپ میزان انتقال ۳ در جعبهٔ پایین نمایش داده شده. کلید رمز همان مقدار جابجایی است که در این مثال برابر با ۳ انتخاب شده.

آشکار: ABCDEFGHIJKLMNOPQRSTUVWXYZ

رمز: DEFGHIJKLMNOPQRSTUVWXYZABC

رمز سزار را می‌توان به صورت ریاضی با استفاده از همنهشتی نمایش داد. به این منظور ابتدا با استفاده از الگوی ساده زیر، حروف الفبا با اعداد جایگزین می‌شوند.

{\displaystyle A\rightarrow 0,B\rightarrow 1,\cdots ,Z\rightarrow 25}

سپس هر حرف *x* با انتقال *n* به ترتیب زیر رمزگذاری می‌شود:

{\displaystyle E\_{n}(x)=(x+n)\mod {26}.}

به طریق مشابه، رمزگشایی به صورت زیر انجام می‌شود.

{\displaystyle D\_{n}(x)=(x-n)\mod {26}.}

توجه به این نکته ضروری است که تعاریف مختلفی برای  عملیات پیمانه ای وجود دارد. در اینجا نتیجه پیمانه عددی بین ۰ تا ۲۵ است. یعنی اگر *x+n* یا *x-n* در بازه ۰ تا ۲۵ نباشد، باید ۲۶ با نتیجه جمع یا از آن کم شود.

تبدیل حروف آشکار به رمز در تمام متن یکسان است و به این ترتیب رمز سزار در رده رمز جانشینی در برابر  رمز چندالفبایی قرار می‌گیرد.

**مثال**

برای رمزگذاری متن، کافی است که هر حرف از متن آشکار با حرف متناظر آن در الفبای رمز جایگزین شود. در مثال زیر از کلید ۳ برای رمزگذاری استفاده شده.

متن آشکار: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

متن رمز: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

رمزگشایی به روش مشابه و با انتقال به همان میزان در جهت مقابل انجام می‌شود.