Caesar cryptography algorithm document

در رمزنگاری، **رمز سزار** (به انگلیسی:Caesar cipher) که با نام‌های **کد سزار**، **شیفت سزار** یا **رمزشیفت** نیز شناخته می‌شود، یکی از ساده‌ترین و شناخته‌شده‌ترین تکنیک‌های رمزگذاری است. این رمز یک نوع رمز جانشینی است که در آن هر حرف در متن آشکار با حرف دیگری با فاصله ثابت در الفبا جایگزین می‌شود. برای مثال با مقدار انتقال ۳، D به جای A می‌نشیند، E به جای B، و الی آخر. نام این روش از ژولیوس سزار گرفته شده‌است که از آن برای ارتباطات محرمانه خود استفاده می‌کرد.

رمز سزار معمولاً به عنوان یکی از اجزای سیستم‌های رمزگذاری پیچیده‌تر مانند رمز ویژنر استفاده می‌شود. روت۱۳ یک حالت خاص رمز سزار است که از میزان انتقال ۱۳ استفاده می‌کند و با توجه به آن‌که الفبای انگلیسی از ۲۶ حرف تشکیل شده، وارون خودش است. رمز سزار مانند تمام رمزهای جانشینی تک‌الفبایی دیگر به راحتی شکسته می‌شود و با وجود تکنیک‌های مدرن، هیچ‌گونه امنیتی برای ارتباطات فراهم نمی‌کند.

شیوه رمزگذاری:

تبدیل 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 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

$$A \to 0 , B \to 1, \ldots, Z \to 25$$

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

$$E_n(x) = (x + 1)\ mod\ 26$$

به طریق مشابه، رمزگشایی به صورت زیر انجام می‌شود.

$$D_n(x) = (x - n)\ mod\ 26$$

توجه به این نکته ضروری است که تعاریف مختلفی برای عملیات پیمانه 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 رمزهای جانشینی (در برابر رمزهای چند الفبایی) 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.

شکستن رمز

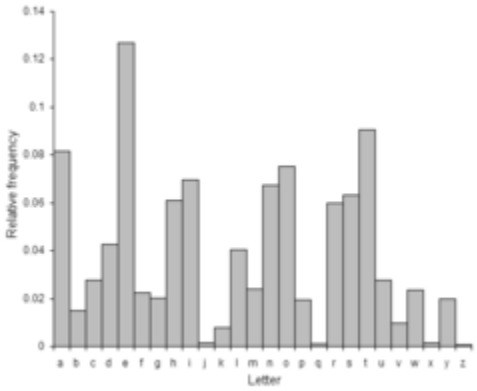
رمز سزار حتی در شرایط حمله متن اصلی به راحتی قابل شکسته شدن است. دو موقعیت زیر می‌توانند در نظر گرفته شوند:

1. حمله‌کننده می‌داند یا حدس می‌زند که نوعی از رمز جانشینی ساده استفاده شده‌است اما مشخصا نمی‌داند که رمز سزار است.
2. حمله‌کننده می‌داند که رمز سزار استفاده شده‌است اما مقدار انتقال را نمی‌داند.

در حالت اول استفاده از تکنیک‌های معمول شکستن رمزهای جانشینی مانند تحلیل فراوانی به سادگی نتیجه‌بخش است. در حین استفاده از این تکنیک‌ها، حمله‌کننده به راحتی متوجه نظم موجود در سیستم جانشینی و استفاده از رمز سزار خواهد شد.

شکستن رمز در حالت دوم ساده‌تر از حالت اول است. از آنجا که تعداد ممکن انتقال‌ها محدود است (در زبان انگلیسی ۲۶ حالت ممکن) اعمال حمله جستجوی فراگیر و آزمایش تمام حالات ممکن به سرعت انجام می‌شود برای مثال همان‌طور که در جدول نشان داده شده، بخشی از متن به همراه تمام انتقال‌های ممکن نوشته می‌شود و ردیف حاوی متن بامعنی به راحتی قابل تشخیص است. در این روش کافی است که زیر هر حرف از متن رمز شده، تمام حروف الفبا به ترتیب نوشته شوددر مثال جدول زیر متن رمز شده **EXXEGOEXSRGI** است و به سادگی می‌توان تشخیص داد که کلید رمز استفاده شده برابر با ۴ بوده.

میزان انتقال رمزگشایی	متن آشکار احتمالی
۰	exxegoexsrgi
۱	dwwdfndwrqfh
۲	cvvcemcvqpeg
۳	buubdlbupodf
۴	attackatonce
۵	zsszbjzsnmbd
۶	yrryaiyrmlac
...	
۲۳	haahjrhavujl
۲۴	gzzgiqgzutik
۲۵	fyyfhpfytshj



توزیع فراوانی حروف در یک متن معمولی زبان انگلیسی به راحتی قابل تشخیص و پیش‌بینی است. رمز سزار این توزیع را به چپ یا راست منتقل می‌کند اما شکل آن را تغییر نمی‌دهد. میزان انتقال به راحتی با مشاهده نمودار فراوانی قابل تشخیص خواهد بود.

روش دیگر حمله جستجوی فراگیر با کمک تحلیل فراوانی است. در این روش با مقایسه فراوانی حروف در متن رمز و فراوانی حروف در متون عادی زبان مورد استفاده و جابجایی دو نمودار می‌توان میزان انتقال را پیدا کرد. برای مثال در زبان انگلیسی **E** و **T** پراستفاده‌ترین و حروف **Q**

و **Z** کم‌استفاده‌ترین حروف هستند این روش توسط کامپیوتر هم قابل پیاده‌سازی است. برای این کار کافی است با استفاده از آزمون مربع کای، توزیع داده شده با توزیع مورد انتظار مقایسه شود .

معمولاً فقط یک متن آشکار محتمل برای یک متن رمز وجود دارد، اما برای رمزهای بسیار کوتاه ممکن است تعداد پاسخ‌های محتمل بیشتر از یکی باشد. برای مثال متن رمز **MPQY** می‌تواند به **aden** یا **know** برگردد. به‌طور مشابه **ALIIP** می‌تواند **dolls** یا **wheel** باشد و **AFCCP**را می‌توان به **jolly** یا **cheer** رمزگشایی کرد. به حداقل طول متن رمز شده که لازم است تا متن اصلی به صورت یکتا قابل شناسایی باشد فاصله یکتایی گفته می‌شود .

استفاده چندباره از رمز سزار بر روی یک متن به امنیت بیشتر منجر نمی‌شود. زیرا دو بار رمزگذاری با انتقال‌های **A** و **B** معادل یک بار رمزگذاری با کلید **A+B** است. به زبان ریاضی می‌توان گفت مجموعه رمز سزار با کلیدهای متنوع، تحت ترکیب یک گروه تشکیل می‌دهند.