# الگوریتم رمزنگاری سزار

* فرآیند رمزگذاری

رمزگذاری سزار به صورت زیر تعریف می شود:

C = ( P + K ) mod 26

P علامت اختصاری متن ساده است. C  نیز علامت اختصاری متن رمزشده قلمداد می شود. K  نیز علامت اختصاری کلید است. Mod عملگر پیمانه گیری رایانه ای تعریف شده است، بدین معنی که باقیمانده تقسیم هر نتیجه ای که از جمع P و K بدست می آید، بر 26 گرفته شده و C را تشکیل می دهد.

حال الگوریتم را روی عبارت "Attack at dawn" و با کلید K=’E’ بررسی می کنیم :

Plain Text = “ Attack at dawn “

Key = ‘E’

در این الگوریتم به هر یک از حروف یک عدد نسبت داده می شود. مثلا برای حروف A تا Z اعداد صفر تا 25.سپس عملیات رمزگذاری حرف به حرف  انجام می گیرد:

1. C= ( P + K ) mod 26= ( ‘A’ + ‘E’ ) mod 26= ( 0 + 4 ) mod 26= 4= ‘E’

2. C= ( ‘t’ + ‘E’ ) mod 26= ( 19 + 4 ) mod 26= 22= ‘W’

…

11. C= ( ‘w’ + ‘E’ ) mod 26= ( 22 + 4 ) mod 26= 26 mod 26= 0= ‘A’

12. C= ( ‘n’ + ‘E’ ) mod 26= (16 + 4 ) mod 26= 20= ‘U’

Cipher Text = “EWWEGO EW HEAR”

* فرآیند رمزگشایی

فرآیند رمزگشایی دقیقا عکس فرآیند رمزنگاری است الگوریتم رمزگشایی به صورت زیر تعریف می شود**:**

P = ( C – K ) mod 26                             (3-2)

رمز سزار از دسته رمزهای تک حرفی[4] به حساب می آید، بدین مفهوم که الگوریتم رمزنگار یک تک حرف به عنوان ساده متن دریافت کرده و با یک تک حرف به عنوان کلید، آنرا به یک تک حرف رمزمتن تبدیل می نماید. این خاصیت از نقاط ضعف بزرگ الگوریم مذکور است.