رمزنگاری جانشینی

در **رمزنگاری جانشینی** هر حرف یا گروهی از حروف با یک حرف یا گروهی دیگر از حروف جابجا میشوند تا در نتیجه شکل پیام بهم بریزد.

یکی از قدیمی ترین رمزهای شناخته شده به روش رمز جانشینی، روش رمزنگاری سزار است که ابداع آن به ژولیوس سزار نسبت داده میشود.

یک حالت عمومی و ساده از رمزنگاری سزار آن است که هر حرف الفبا از متن اصلی با حرفی که در جدول الفبا k حرف بعدتر قرار گرفته جابجا شود. (روش Shift by k)

در این روش کلید رمز متن، عدد انتقال یعنی k خواهد بود و بر اساس آن روف یک متن به صورت چرخشی با حرف kام بعد از خودش جایگزین میشود.

البته این روش امروزه بسیار مبتدی به نظر میرسد و به راحتی قابل رمزگشایی است.

بهبود این روش آن است که هر حرف در متن اصلی با یک حرف دلخواه جانشین شود؛ بدان معنا که 26 حرف جدول الفبا به حروف دیگری در همان جدول نگاشته شود.

هر **سیستم رمزنگاری** که در آن یک سمبول با سمبول دیگر جایگزین یمشود اصطلاحاً “سیستم جانشینی تک حرفی” (Monoalphabetic Substitution) گفته میشود که در آن کلید رمز یک رشته 26 کاراکتری است و نگاشتی از جدول الفبا را مشخص میکند.

در نگاه اول این سیستم رمزنگاری مطمئن به نظر میرسد زیرا اگرچه رمزشکن روش عمومی جانشینی حروف را میداند ولی نمیتواند از جایگشت 26 حرف (معادل با 4 \* 10 به توان 26 حالت) موفق به یافتن کلید رمز شود.

بنابراین بر خلاف رمز سزار، آزمایش تمام حالات مختلف کلید غیر ممکن است زیر اگر هر یک از حالات کلمه رمز در یک نانو ثانیه آزمایش شود، بررسی تمام حالات کلید توسط چنین سیستمی 10 به توان 10 سال به طور خواهد انجامید.