الگوريتم رمزنگاری سزار

الگوريتم رمز سزار براي اولين بار توسط ژوليوس سزار سردار رومي مورد استفاده قرار گرفت. در اين الگوريتم جايگزيني حروف براساس ترتيب در حروف الفبا انجام ميشود بنابراين برای رمز نمودن متن جايگزيني زير را خواهيم داشت:

رشته مبنا  
ABCDEFGHIJKLMNOPQRSTUVWXYZ

رشته تبديل يافته  
DEFGHIJKLMNOPQRSTUVWXYZABC

در اين تبديل هركدام از كاراكتر ها تبديل به كاراكتري تبديل ميشوند كه در ترتيب حروف الفبا سه مرحله بعد از آن قرار دارند، بعنوان مثال A به D كه اين تبديلات براي تمامي كلمات انجام ميشود.

در حالتي كه متن رمز شده در اختيار قرار دارد اين تبديل برعكس انجام ميشود و ما تبديل زير را خواهيم داشت:

رشته تبديل يافته  
DEFGHIJKLMNOPQRSTUVWXYZABC

رشته مبنا  
ABCDEFGHIJKLMNOPQRSTUVWXYZ

در صورتي كه به كلمات در هر زبان رايج توجه كنيم ميتوانيم اين نكته را دريابيم كه شكل ظاهري حروف، تعداد كاراكتر ها، تعداد حروف در هر كلمه ميتواند داراي معيار خاصي باشد. اين معيارها براساس نوع زبان ميتواند متفاوت باشد.

در رمز نگاري به روش سزار خصوصيات اصلي كلمات تغيير نميكند بلكه با توجه به اينكه نسبت يك به يك بين حروف برقرار است خصوصيات كلمه تغير نخواهد كرد و با اندكي هوشياري ميتوان متن رمز شده را حدس زد.