

رمزنگاری جابه‌جایی

در رمزنگاری کلاسیک، رمزنگاری جابجایی (به انگلیسی Transposition cipher): روشی است که با جابجا کردن حروف عمل رمز کردن را انجام می‌دهد و با اجرای برعکس آن رمزگشایی صورت می‌گیرد. از دید ریاضی یک تابع یک به یک بر روی مکان حروف کار رمز کردن را انجام می‌دهد و معکوس آن برای رمزگشایی استفاده می‌گردد. رمزهای جابجایی ترتیب حروف را عوض می‌کنند ولی آن‌ها را تغییر نمی‌دهند. در ادامه نمونه‌هایی از رمزنگاری جابه‌جایی معرفی شده‌اند.

رمز rail fence

در این نوع سیستم ابتدا حروف را به صورت سطری در جدولی به ابعاد مشخص قرار می‌دهیم و سپس اقدام به خواندن ستونی آن می‌کنیم.

پیاده سازی در cryptool:

ابتدا در قسمت Transposition Cipher >> Classical >> Cryptography >> templates را باز می‌کنیم.

در قسمت Plaintext متن اصلی Sepide Omidvar را وارد می‌کنیم. در قسمت Key کلید را نظر می‌گیریم و طول کلید عمق جدول قرار گیری حروف من اصلی خواهد بود. در اینجا کلید sep با طول کاراکتری ۳ در نظر گرفته شده است و عمق جدول هم ۳ خواهد بود. با زدن کلید start متن رمز شده Si iaedOdrpemvSi ia خواهد بود.

