رمزنگاری جابه‌جایی

در رمزنگاری کلاسیک، رمزنگاری جابجایی (به انگلیسیTransposition 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 رمزکردن 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 می کنیم.

پیاده سازی در cryptool:

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

در قسمت Plaintext متن اصلی Faeze Karami را وارد می کنیم. در قسمت Key کلید را نظر میگیریم و طول کلید عمق جدول قرار گیری حروف من اصلی خواهد بود. در اینجا کلید two با طول کاراکتری ۳ در نظر گرفته شده است و عمق جدول هم ۳ خواهد بود. با زدن کلید start متن رمز شده e riFzKaaeamخواهد بود.