

رمز جانشای تک الفبایی

رمزنگاری جانشینی

رمزنگاری جانشینی روشی برای رمزنگاری است که در آن هر واحد از متن اصلی بر طبق یک سیستم معین با رمز شده آن جایگزین می شود. یک واحد ممکن است یک حرف باشد (که معمولاً این طور است) یا دو حرف، سه حرف یا حتی ترکیبی از آنها و شکل های مشابه آن باشد. رمزگشایی آن با کمک عکس عمل جاگذاری انجام پذیر است.

این روش با رمزنگاری جابجایی قابل مقایسه است. روش جانشینی بدون تغییر مکان حروف خود آنها را تغییر می دهد ولی رمزنگاری جابجایی حروف را تغییر نمی دهد و فقط آنها را با هم جابجا می کند.

یکی از ساده ترین مثال های این روش رمز سزار می باشد.

رمزنگاری جانشینی انواع مختلفی دارد. اگر رمزنگاری بر روی یک حرف انجام شود به آن رمزنگاری جانشینی ساده گویند. به این نوع رمزنگاری روی گروه های بزرگتری از حروف، پلی گرافیک گویند. یک رمزنگاری تک حرفی از جانشینی ثابت بر روی کل پیام استفاده می کند. در حالیکه رمزنگاری چند حرفی از چندین جانشینی در موقعیت های مختلف در یک پیام استفاده می کند، به طوریکه یک واحد از متن اصلی به یکی از چندین احتمال در متن رمز شده نگاشته می شود و برعکس.

جانشینی ساده

جانشینی یک حرف (جانشینی ساده) را با نوشتن حروف الفبا با یک ترتیب خاص به منظور نشان دادن جانشینی، می توان نمایش داد. به این، جانشینی الفبایی گویند. ممکن است حروف الفبای رمز، شیفت داده شوند یا معکوس شوند (که به ترتیب رمز سزار و اتباش (Atbash) را ایجاد می کنند) یا در یک مدل پیچیده تر پیش روند که در این صورت به آن الفبای ترکیبی (mixed alphabet) یا الفبای بی ترتیب (deranged alphabet) گویند. به طور سنتی، الفبای ترکیبی ممکن است ابتدا توسط نوشتن یک کلیدواژه، حذف حروف تکراری از آن، سپس نوشتن تمامی حروف باقی مانده در حروف الفبا با ترتیب معمولی آنها ساخته شود.

پیاده سازی در Cryptool:

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

در قسمت Plaintext متن اصلی Sepide Omidvar را وارد می کنیم. در قسمت Source Alphabet کلید را حروف و کاراکتر های زبان انگلیسی و نگاشت کاراکتر ها را به یک کاراکتر بعد در نظر میگیریم به عنوان مثال a->b یا A->Z. و با زدن کلید start متن رمز شده Tfjqef Pnjewbs خواهد بود.

