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 رمزشده آن جایگزین می‌شود. یک واحد ممکن است یک حرف باشد (که معمولاً این طور است) یا دو حرف، سه حرف یا حتی ترکیبی از آنها و شکل‌های 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 می‌دهد ولی رمزنگاری جابجایی حروف را تغییر نمی‌دهد و فقط آنها را با هم جابجا می‌کند.

یکی از ساده‌ترین مثال‌های این روش رمز سزار می‌باشد.

رمزنگاری جانشینی انواع مختلفی دارد. اگر رمزنگاری بر روی یک حرف انجام شود به آن رمزنگاری جانشینی ساده گویند. به این نوع رمزنگاری روی گروه‌های بزرگتری از حروف، پلی‌گرافیک گویند. یک رمزنگاری تک حرفی از جانشینی ثابت بر روی کل پیام استفاده می‌کند. درحالیکه رمزنگاری چند حرفی از چندین جانشینی در موقعیت‌های مختلف در یک پیام استفاده می‌کند، به طوریکه یک واحد از متن اصلی به یکی از چندین احتمال در متن رمزشده نگاشته می‌شود و برعکس.

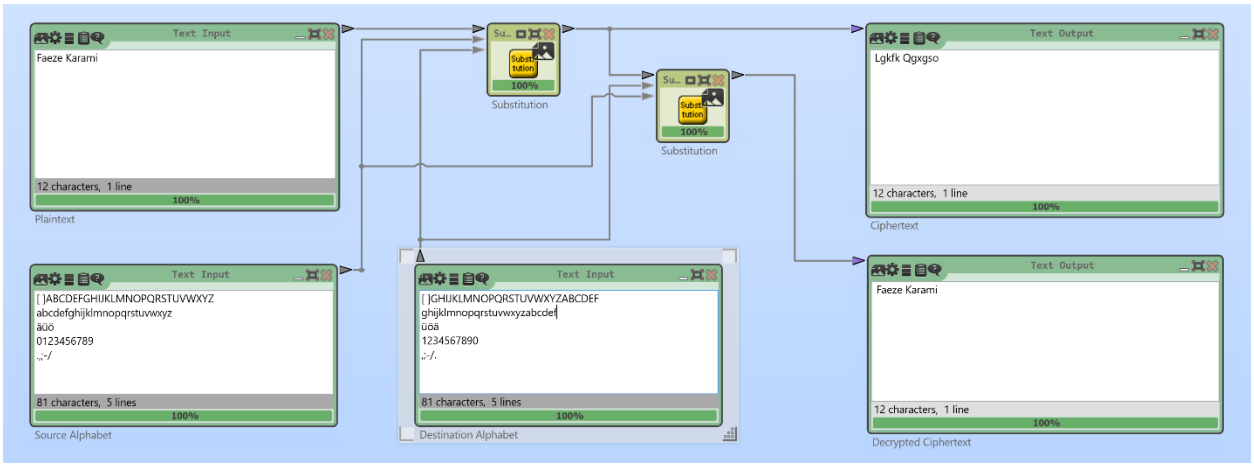
جانشینی ساده

جانشینی یک حرف (جانشینی ساده) را با نوشتن حروف الفبا با یک ترتیب خاص به منظور نشان دادن جانشینی، می‌توان 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 می‌کنند) یا در یک مدل پیچیده‌تر پیش روند که در این صورت به آن الفبای ترکیبی(mixed alphabet) یا الفبای بی‌ترتیب(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 templates>>Cryptography>>Classical>>Substitutin Cipher را باز میکنیم.

در قسمت Plaintext متن اصلی Faeze Karamiرا وارد می کنیم. در قسمت Source Alphabet کلید را حروف و کاراکتر های زبان انگلیسی و نگاشت کاراکتر ها را به 6 کاراکتر بعد در نظر میگیریم به عنوان مثال a->g یا Z->F. و با زدن کلید start متن رمز شده Lgkfk Qgxgsoخواهد بود.


Text Input
Faeze Karami
12 characters, 1 line
100%
Plaintext
Su...
Substitution
100%
Substitution
Su...
Substitution
100%
Substitution
Text Output
Lgkfk Qgxgso
12 characters, 1 line
100%
Ciphertext
Text Input
[ ]ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
äüö
0123456789
.,:-/
81 characters, 5 lines
100%
Source Alphabet
Text Input
[ ]GHIJKLMNOPQRSTUVWXYZABCDEF
ghijklmnopqrstuvwxyzabcdef
üöä
1234567890
,:-/.
81 characters, 5 lines
100%
Destination Alphabet
Text Output
Faeze Karami
12 characters, 1 line
100%
Decrypted Ciphertext