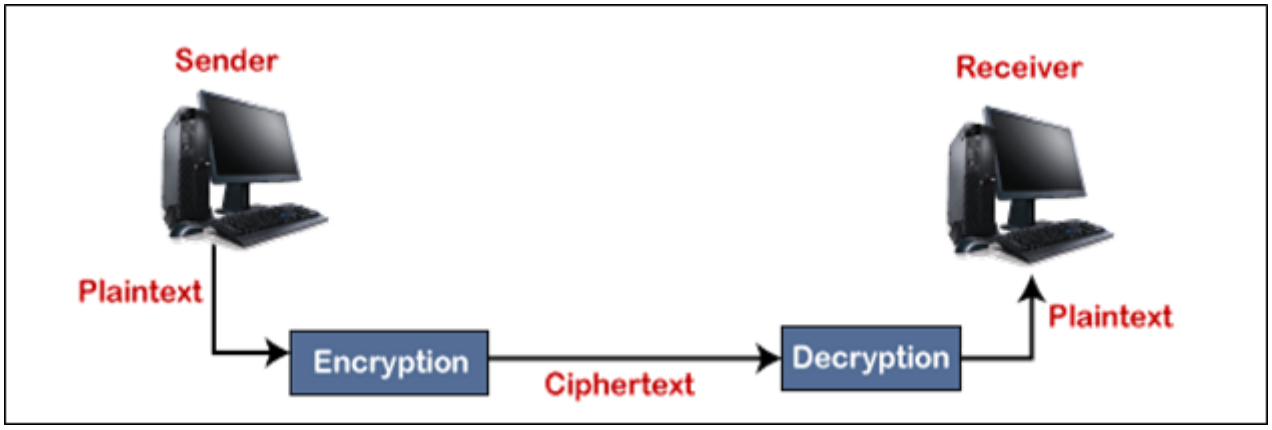
بسمه تعالی

دانشگاه شهیدبهشتی
دانشکده مهندسی و علوم کامپیوتر
امنیت شبکه‌های کامپیوتری پیشرفته
تمرین اول

رمزنگاری به فناوری‌ای اشاره دارد که اطلاعات در حال انتقال را از یک نقطه به نقطه دیگر ایمن می‌کند. در پایین‌ترین سطح، این امر با استفاده از الگوریتم‌ها و محاسبات ریاضی به دست می‌آید. با رمزگذاری داده‌ها، حریم خصوصی فرستنده و گیرنده محافظت می‌شود. رمزنگاری در واقع الگوی (الگوریتمی) که به صورت ریاضی و منطقی می‌باشد و جهت تبدیل اطلاعات آشکار(plain text) به اطلاعاتی نا مفهوم و بی معنی (cipher text) ولی بازگشت پذیر به کار می‌رود.در تصویر زیر عملکرد رمزنگاری در سیستم‌های کامپیوتری قابل درک است.



در این تمرین هدف پیاده سازی الگوریتم‌های رمزنگاری با استفاده از پایتون نسخه ۳ می باشد.در پیاده سازی انجام شده باید موارد زیر مشخص باشد:

-الگوریتم تولید کلید
-الگوریتم رمزنگاری
-الگوریتم رمزگشائی

توجه: دانشجویان تنها مجاز به استفاده از کتابخانه Mathematical functions می‌باشند.

https://docs.python.org/3/library/math.html

مطلوب است دانشجویان با توجه به الگوریتم رمزنگاری که در سامانه درس افزار برای آنها مشخص شده است پیاده سازی مورد نظر را انجام دهند. کد شبیه سازی #StudentNumber.py و گزارش پروژه #StudentNumber.pdf را در قالب یک فایل Zip با نام #StudentNumber.zip در مهلت مقرر بارگذاری کنید.

موفق باشید.