دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

به نام خدا

تمرین عملی اول درس امنیت کامپیوتر

آشنایی با امنیت گذرواژه و رمزنگاری

دکتر حمیدرضا شهریاری

پاییز ۱۴۰۲

نکات مهم:

کد: استفاده از کتاب خانه های مرسوم در محدوده رمزنگاری مجاز است.برای راحتی و درگیر نبودن با رابط کاربری گرافیکی، از کتاب خانه argparse و رابط کاربری کامند لاینی (CLI) استفاده کنید. برای مثال میتوانید مانند تصویر زیر عمل کنید:

```
PS C:\Users\erfan> python d:/python/password_cracker.py mode standard  l 3

what is search space  alphabet

 password is slm
PS C:\Users\erfan>
```

```
PS C:\Users\erfan> python d:/python/password_cracker.py mode firstletter  l 3

 what is 1st letter?s

what is search space  alphabet

 password is slm
PS C:\Users\erfan>
```

گزارش: بخش اصلی ارزشیابی شما گزارش است. لذا ارسال کدها بدون گزارش شامل نمره نخواهد بود. گزارش باید شامل اسکرین شات از کد و خروجی و نحوه کار ابزارها باشد. همچنین سعی کنید توضیحی کوتاه درباره نحوه پیاده سازی و کارکرد توابع و کدها اراعه دهید.

تذکر: هرنوع کپی برداری غیرقابل قبول بوده و باعث درج نمره منفی برای هر دو طرف خواهد بود.

ارسال: فایل گزارش به همراه فایل کدها را به صورت یک فایل فشرده درآورده و آن را با فرمت prj1_studentfamilyname_studentnumber.zip در سامانه بارگذاری نمایید.

تاخیر: درمجموع ۱۰ روز تاخیر قابل قبول خواهد بود که هر روز تاخیر منجر به کسر ۵ درصد از نمره تمرین خواهد بود.

** درصورت نیاز میتوانید سوالات خود را در خصوص انجام تمرین، از طریق راه های ارتباطی زیر از تدریس یار بپرسید.

ایمیل: erf.mohammadi@aut.ac.ir

تعریف تمرین:

فاز اول تمرین شامل دو بخش است.

بخش اول شامل مطالعه استاندار گذرواژه و پیاده سازی یک ارزیاب میزان قدرت(Password Strength Checker) گذرواژه می باشد.

بخش دوم شامل پیاده سازی یک ابزار کرک گذرواژه (brute force password crackr) می باشد.

فاز دوم:

در این فاز از شما خواسته شده است تا یک ابزار برای رمز کردن فایل ها پیاده سازی کنید.

هدف از این تمرین آشنایی شما با امنیت گذرواژه ها و همچنین رمزنگاری فایل ها در سیستم عامل است.

فاز اول- بخش ۱:

لطفا در ابتدا بخش مربوط به امنیت گذرواژه در سند استاندارد NIST.sp.800-63b را که در سامانه به همراه فایل تمرین بارگذاری شده است، مطالعه بفرمایید. سپس با توجه به توضیحات داده شده در این سند، ابزار ارزیابی امنیت گذرواژه با زبان پایتون پیاده سازی کنید.

دقت فرمایید که برنامه شما باید گذواژه را به عنوان ورودی دریافت کرده و پس از بررسی آن، میزان قدرت آن را به عنوان خروجی و با توجه به استاندارد به کاربر نمایش دهد.

** درصورت استفاده از دیکشنری های گذرواژه مورد استفاده در حملات دیکشنری و بررسی آن که آیا پسورد داده شده در دیکشنری موجود میباشد یا خیر شامل نمره مثبت خواهد بود.

فاز ۱-بخش ۲:

در این بخش از شما خواسته شده است تا با استفاده از زبان پایتون یک ابزار کرک پسورد را پیاده سازی کنید. دقت کنید ابزار باید بگونه ای باشد که یک رشته به عنوان پسوردی که باید کرک شود به عنوان ورودی گرفته و سپس اقدام به پیدا کردن آن پسورد بکند و حدس مدت زمان بررسی و همچنین تعداد حدس ها را به عنوان خروجی به کاربر نمایش دهد. برای سهولت میتوانید تعداد کارکترهای پسورد را نیز به عنوان ورودی به برنامه بدهید.

دقت کنید برنامه باید شامل مودهای کاری زیر باشد.

۱-مود استاندارد که تنها تعداد کارکتر پسورد را از کاربر میگیرد.

۲-مود جست وجو با دانستن حرف اول: در این مود حرف اول پسورد به عنوان ورودی به برنامه داده میشود.

۳- مود جست و جو با دانستن k کاراکتر از گذرواژه: در این مود مقدار k کاراکتر از n کاراکتر گذرواژه به عنوان ورودی به برنامه داده میشود.

دقت کنید در تمامی این ۳ حالت باید فضای کارکتری جست و جو از کاربر پرسیده شود و با توجه به آن جست و جو انجام شود. برای سهولت میتوانید تنها از این ۳ حالت استفاده کنید.

{تنها اعداد} {اعداد و حروف کوچک} {تنها حروف کوچک}

**استفاده از فضای کاراکتر {اعداد و حروف و کوچک و بزرگ و کاراکتر} شامل نمره مثبت خواهد بود

درنتیجه و به طور خلاصه برنامه باید شامل کامندها و آپشن های زیر باشد:

تعیین مود جست و جو، تعیین فضای جست وجو، تعیین طول پسورد مورنظر.

نکته: برای کوتاه ترکردن زمان اجرا می‌توانید از پسوردهایی با طول کوچک استفاده کنید.

فاز ۲

در این تمرین از شما خواسته شده است تا با استفاده از زبان پایتون یک ابزار رمزنگاری پیاده‌سازی کنید. دقت کنید برای عملیات رمز کردن و رمزگشایی می‌توانید از کتابخانه‌های موجود برای زبان پایتون استفاده کنید. همچنین محدودتی در استفاده از الگوریتم‌های رمزنگاری موجود وجود ندارد؛ اما دقت کنید که حتماً در گزارش خود کتابخانه و الگوریتم مورداستفاده را معرفی و توابع استفاده شده را توضیح دهید.

این ابزار باید در دو مود کاری زیر پیاده‌سازی شود.

مود رمزنگاری: در این مود برنامه یک فایل را به‌عنوان ورودی گرفته و پس از رمز کردن آن را به‌صورت رمز شده در سیستم ذخیره می‌کند.

مود رمزگشایی: در این مود برنامه یک فایل رمز شده را به‌عنوان ورودی گرفته و پس از رمزگشایی آن، فایل را در سیستم ذخیره می‌کند.

نکته مهم: در هر دو مود کاری، کلید رمزنگاری باید به‌عنوان یک‌رشته متنی گذرواژه از کاربر گرفته شود.

برای سهولت می‌توانید تنها از فایل‌هایی با فرمت txt برای رمز کردن و رمزگشایی استفاده کنید.

موفق باشید