تکلیف اول

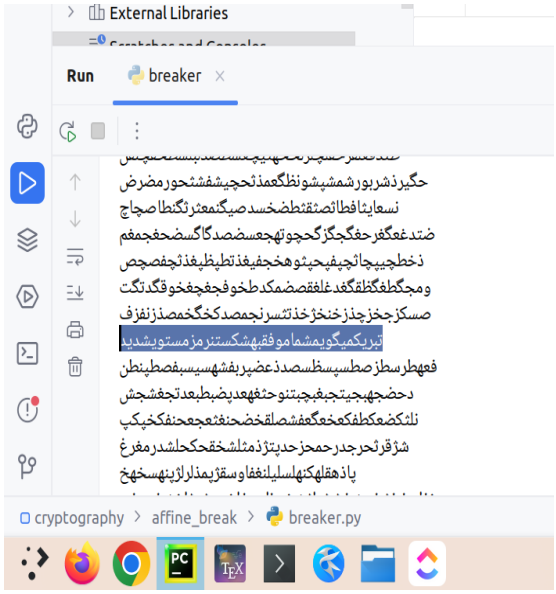
مهدی حق‌وردی

۱۴ اسفند ۱۴۰۲

فهرست مطالب

۱ سوال اول - شکستن متن شنود شده

متن شنود شده را توسط کدی که در اینجا[1] وجود دارد را با تمامی کلیدهای ممکن امتحان کردم و هر کدام از خروجی‌ها را بررسی کردم که به این رسیدم:



[1] https://github.com/mahdihaghverdi/cryptography/tree/main/affine_break

۱.۱ توضیحات کد

- `pre_needed.py`

مقادیری که این ماژول وجود دارند مقادیری مانند الفبای فارسی، تمام کلیدها و یک سری ثابت هستند که در برنامه برای رمزنگاری و رمزگشایی به آنها نیاز است.

- `functions.py`

توابعی که در این ماژول هستند دو تابع `encode` و `decode` هستند که طبق فرمول‌های رمز مستوی نوشته شده‌اند.

- `breaker.py`

در این ماژول در حلقه‌ی `for` اول، متن رمزشده را با تمامی کلیدهای ممکن رمزگشایی کرده و نتیجه را پرینت می‌کنیم و سپس در خروجی به دنبال یک متن معنی دار می‌گردیم.

حالا برای پیدا کردن کلید هم می‌توانیم بین کلیدها بگردیم و آن کلیدی که متن با آن رمز شده را پیدا کنیم که آن کلید: `Key(a=5, b=3)` است.

۲ شکستن رمز ویجینر با دانستن طول کلید

۱. با انجام ندادن عملیات آنالیزی

اگر نخواهیم عملیات آنالیزی روی متن رمز شده انجام دهیم، order شکستن متن رمز شده باید $O(26^k)$ که در آن k طول کلید است را انجام داد. که در سوال $k = 5 \Rightarrow 26^5$ می‌شود. [2]

۲. با انجام دادن عملیات آنالیزی

[2] from https://stackoverflow.com/a/29553484/19510840