

تکلیف اول

مهدی حقوردی

۱۵ اسفند ۱۴۰۲

فهرست مطالب

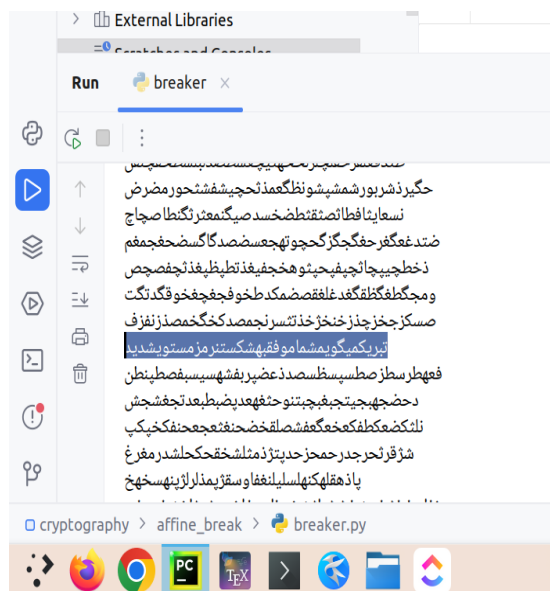
۲	۱ سوال اول - شکستن متن شنود شده
۲	۱.۱ توضیحات کد
۳	۲ شکستن رمز ویجینر با دانستن طول کلید
۴	۳ سوال سوم
۴	۱.۳ کلید از شماره دانشجویی
۴	۲.۳ رمزگشایی یک متن رمز شده با دو حرف آشکار
۵	۴ معکوس ماتریس در \mathbb{Z}_{26}
۵	۱.۴ 2×2
۵	۲.۴ 3×3

چکیده

پاسخ‌های تمرین اول به ترتیب سوالات در قالب قسمت‌های نام برده در فهرست نوشته شده‌اند. تمامی کدها و فایل‌های پاسخ‌دهی بعد از تمام شدن مهلت تمرین روی گیت‌هاب push شده‌اند تا کسی از روی آنها ننویسد. اگر در پاسخی از منبعی استفاده شده است، لینکی از آن منبع در پانویس گذاشته شده است.

۱ سوال اول - شکستن متن شنود شده

متن شنود شده را توسط کدی که در اینجا¹ وجود دارد را با تمامی کلیدهای ممکن امتحان کردم و هر کدام از خروجی‌ها را بررسی کردم که به این رسیدم:



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 رمز شده 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.

¹https://github.com/mahdiaghverdi/cryptography/tree/main/affine_break

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

اما اگر بخواهیم باهوش باشیم و با انجام دادن عملیات آنالیزی روی متن رمز شده، آن را بشکنیم می‌توانیم با همین روش brute-force ولی با تعداد تلاش بسیار کمتری رمز را بشکنیم. حالا که رمز ما ۵ حرف دارد، باید برای هر $\forall i \in \{0, 1, 2, 3, 4\}$ چنین کنیم:

$$p_i, p_{i+k}, p_{i+2k}, p_{i+3k}, \dots \quad (1)$$

انجام دهیم و متونی را از cipher text استخراج کنیم. برای مثال چنین متن رمز شده‌ای داریم:

PPQCAXQVEKGYBNKMAZUYBNGBALJONITSZMJYIMVRAGVOHTVRAUCTKSGDDWUOXITLAZUVAVVRAZCVKBQPIWPOU

و $k = 4$ داده شده است (یا از طریق روش کاسیسکی پیدا شده است). حالا طبق رابطه‌ی ۱ برای هر یک از حروف کلید به ترتیب، متنش را استخراج می‌کنیم:

$$i = 0 \bullet$$

PPQCAXQVEKGYBNKMAZUYBNGBALJONITSZMJYIMVRAGVOHTVRAUCTKSGDDWUOXITLAZUVAVVRAZCVKBQPIWPOU

و به همین ترتیب برای $i = 1, i = 2$ و $i = 3$.

حالا برای هر یک از متون بدست آمده یک تحلیل آنالیزی انجام می‌دهیم و حروفی که ممکن است بجای آن حرف باشند را پیدا می‌کنیم. برای مثال در مورد بالا چنین حروفی پیدا می‌شوند:

A, I, N, W, and X : $i = 0 \bullet$

I and Z : $i = 1 \bullet$

C : $i = 2 \bullet$

K, N, R, V, and Y : $i = 3 \bullet$

که حالا فضای کلیدهای ما می‌شود: $50 = 5 \times 1 \times 2 \times 5$ که بسیار بسیار کمتر از 26^4 است و می‌توانیم روی جایگشت‌های کلید با این حروف brute-force را اجرا کنیم.³

²from <https://stackoverflow.com/a/29553484/19510840>

³from <https://inventwithpython.com/hacking/chapter21.html>

۳ سوال سوم

۱.۳ کلید از شماره دانشجویی

شماره دانشجویی: ۴۰۰۳۶۱۳۰۲۳ مقدار a در کلید رمز مستوی باید معکوس ضربی داشته باشد، که هم در فارسی و هم در انگلیسی عدد ۲ معکوس ضربی ندارد (چون زوج است و نسبت به ۲۶ یا ۳۲ اول نیست). پس دو رقم آخر شماره دانشجویی من نمی‌توانند یک کلید برای رمز مستوی باشند.

۲.۳ رمزگشایی یک متن رمز شده با دو حرف آشکار

طبق صورت سوال: $P \rightarrow M$ و $J \rightarrow A$ و

$$C_i = E_k(P_i) = aP_i + b \bmod 26 \quad (۲)$$

پس:

$$12a + b \equiv 15 \pmod{26}$$

$$b \equiv 9 \pmod{26} \Rightarrow b = 9, a = 7$$

برای محاسبه‌ی معکوس ضربی عدد ۷ چنین می‌کنیم:

$$a^{\Phi(26)-1} \bmod 26 \Rightarrow 7^{11} \equiv 15 \pmod{26}$$

و حالا طبق فرمول

$$P_i = D_k(C_i) = (C_i - b) \times a^{-1} \bmod 26 \quad (۳)$$

متن رمز شده را رمزگشایی می‌کنیم:

- $Y = 24 \rightarrow (24 - 9) \times 15 \equiv 17 \rightarrow R$
- $Z = 25 \rightarrow (25 - 9) \times 15 \equiv 6 \rightarrow G$
- $Q = 16 \rightarrow (16 - 9) \times 15 \equiv 1 \rightarrow B$
- $L = 11 \rightarrow (11 - 9) \times 15 \equiv 4 \rightarrow E$
- $S = 18 \rightarrow (18 - 9) \times 15 \equiv 5 \rightarrow F$
- $A = 0 \rightarrow (0 - 9) \times 15 \equiv 21 \rightarrow V$
- $P = 15 \rightarrow (15 - 9) \times 15 \equiv 12 \rightarrow M$
- $J = 9 \rightarrow (9 - 9) \times 15 \equiv 0 \rightarrow A$

پس متن اصلی: RGBEFVMA بوده است.

۴ معکوس ماتریس در \mathbb{Z}_{26}

۱.۴ 2x2

ماتریس معکوس $A = \begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}$ را در پیمانه‌ی ۲۶ بدست آورید.

$$A = \begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix} \Rightarrow C = \begin{pmatrix} 5 & -9 \\ -5 & 2 \end{pmatrix} \Rightarrow \text{adj}(A) = \begin{pmatrix} 5 & -5 \\ -9 & 2 \end{pmatrix}$$

$$\det(A) = (2 \times 5) - (9 \times 5) = -31 \stackrel{26}{\equiv} 17 \rightarrow 17^{-1} = 23$$

$$\det(A)^{-1} \cdot \text{adj}(A) = \begin{pmatrix} 23 \times 5 & 23 \times (-5) \\ 23 \times (-9) & 23 \times 2 \end{pmatrix} \Rightarrow A^{-1} = \begin{pmatrix} 11 & 15 \\ 1 & 20 \end{pmatrix}$$

۲.۴ 3x3

ماتریس معکوس $A = \begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$ را در پیمانه‌ی ۲۶ بدست آورید.

$$A = \begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix} \Rightarrow C = \begin{pmatrix} + \begin{vmatrix} 23 & 2 \\ 15 & 9 \end{vmatrix} & - \begin{vmatrix} 4 & 2 \\ 17 & 9 \end{vmatrix} & + \begin{vmatrix} 4 & 23 \\ 17 & 15 \end{vmatrix} \\ - \begin{vmatrix} 11 & 12 \\ 15 & 9 \end{vmatrix} & + \begin{vmatrix} 1 & 12 \\ 17 & 9 \end{vmatrix} & - \begin{vmatrix} 1 & 11 \\ 17 & 15 \end{vmatrix} \\ + \begin{vmatrix} 11 & 12 \\ 23 & 2 \end{vmatrix} & - \begin{vmatrix} 1 & 12 \\ 4 & 2 \end{vmatrix} & + \begin{vmatrix} 1 & 11 \\ 4 & 23 \end{vmatrix} \end{pmatrix}$$

$$\Rightarrow C = \begin{pmatrix} 21 & 24 & 7 \\ 3 & 3 & 16 \\ 6 & 20 & 5 \end{pmatrix}$$

$$\Rightarrow \text{adj}(A) = \begin{pmatrix} 21 & 3 & 6 \\ 24 & 3 & 20 \\ 7 & 16 & 5 \end{pmatrix}$$

$$\begin{aligned} \det(A) &= (1 \times \begin{vmatrix} 23 & 2 \\ 15 & 9 \end{vmatrix}) + (-11 \times \begin{vmatrix} 4 & 2 \\ 17 & 9 \end{vmatrix}) + (12 \times \begin{vmatrix} 4 & 23 \\ 17 & 15 \end{vmatrix}) \\ &= (1 \times 21) + (-11 \times 2) + (12 \times 7) = 83 \stackrel{26}{\equiv} 5 \rightarrow 5^{-1} = 21 \end{aligned}$$

$$\det(A)^{-1} \cdot \text{adj}(A) = \begin{pmatrix} 21 \times 21 & 21 \times 3 & 21 \times 6 \\ 21 \times 24 & 21 \times 3 & 21 \times 20 \\ 21 \times 7 & 21 \times 16 & 21 \times 5 \end{pmatrix} \Rightarrow A^{-1} = \begin{pmatrix} 25 & 11 & 22 \\ 10 & 11 & 4 \\ 17 & 24 & 1 \end{pmatrix}$$