میترا عمرانی
شماره دانشجویی: 993613047

کد ارائه شده اجرای رمز Affine و حمله به آن با استفاده از تجزیه و تحلیل فراوانی کلمات در زبان انگلیسی را پیادهسازی میکند.

کلاس AffineCipher:

1. تابع cal_inv_mod:

- این تابع معکوس برای هر عدد در پایهی مشخص شده (mode) را محاسبه میکند.
- از تمام جفتهای ممکن اعداد در بازه [0، mode) عبور میکند و اگر حاصلضرب یک جفت در مد موردنظر برابر با 1 باشد، جفت به عنوان معکوس در نظر گرفته میشود.
- نتیجه در یک دیکشنری (InversesInMode) ذخیره میشود که کلید آن عدد است و مقدار آن معکوس آن عدد.
- این تابع این دیکشنری را برمیگرداند.

این تابع به منظور بهینه سازی کد، به علت عدم نیاز به محاسبهی معکوس برای هر عدد هنگامی که در حال امتحان درستی جواب هستیم، نوشته شده است. در صورتی که این دیکشنری نباشه، در قسمت decyription باید هربار معکوس محاسبه کنیم که وقتگیر خواهد شد.

2. تابع decryption:

- این تابع با استفاده از رمز Affine، رمزگشایی انجام میدهد.
- ورودیهای این تابع شامل متن رمز (cipher_txt)، (a_inve) و b هستند.

- این تابه بر هر کاراکتر در متن رمز، تبدیل معکوس تبدیل آفین را اعمال می‌کند و نتیجه را به یک کاراکتر تبدیل می‌کند.
- متن رمزگشایی شده کاراکتر به کاراکتر ساخته شده و برگردانده می‌شود.

3. تابع encryption:
- این متد با استفاده از رمز Affine، رمزگذاری انجام می‌دهد.
- ورودی‌های این متد شامل متن ساده (plain_txt)، کلید a و شیفت b هستند.
- متن رمزگذاری شده کاراکتر به کاراکتر ساخته شده و برگردانده می‌شود.

کلاس attack:

1. تابع cal_sorted_freq:
- این تابع فراوانی هر کاراکتر در متن رمز را محاسبه کرده و یک لیست از تاپل‌ها که فراوانی‌ها را مرتب شده نمایان می‌کنند را برمی‌گرداند.

2. تابع freq_attack:
- این تابع تلاش می‌کند حمله‌ای با تجزیه و تحلیل فراوانی به رمز Affine انجام دهد.
- ورودی‌های این تابع شامل متن رمز (cipher_txt)، متن ساده موجود (plain_txt) و معکوس‌ها (Inverses) هستند.
- از فراوانی کاراکترها در متن رمز استفاده کرده و سعی می‌کند آنها را با فراوانی‌های مورد انتظار (freq_alpha) مطابقت دهد.

- برای هر ترکیب از کاراکترها و فراوانی‌هایشان، سعی می‌کند مقادیر پتانسیلی برای کلید رمز Affine (a و b) پیدا کند.

- اگر یک کلید پتانسیلی پیدا شود، از تابع decryption برای بررسی اینکه آیا با استفاده از آن کلید رمزگشایی متن رمز به متن ساده موجود منجر به نتیجه مورد انتظار می‌شود یا خیر، استفاده می‌کند.
- اگر یک کلید معتبر پیدا شود، آن را به صورت یک تاپل (a، b) برمی‌گرداند.

اجرای اصلی:

1. رمزگذاری:
- کد متن ساده داده شده (plaintext) را با استفاده از رمز Affine با یک کلید مشخص (a، b) رمزگذاری می‌کند.
- سپس متن رمزگذاری شده را با استفاده از همان کلید رمزگشایی کرده و درستی عملیات رمزگذاری و رمزگشایی را تأیید می‌کند.

2. حمله:
- کد سعی می‌کند حمله‌ای با تجزیه و تحلیل فراوانی به رمز Affine با استفاده از متد freq_attack انجام دهد.
- در صورت موفقیت، کلیدهای کشف شده برای رمزگشایی را چاپ می‌کند.