رامتین احسانی – ۹۷۵۲۱۰۱۸

پروژه اول درس امنیت سیستم های کامپیوتری

شکستن رمز های Affine:

برای شکستن این رمز ها از روش brute-force استفاده کردم. در Affine برای رمز گذاری داشتیم:

(ax + b) modulo 26

پس با تست کردن عدد های مختلف a و b با brute-force در نهایت این رمز شکسته خواهد شد.

در کدی که نوشتم این ciphertext به این صورت شکسته خواهد شد:

```
if __name__ == '__main__':
    myMessage = "Pjo mvvqzo aqnjob qi m pyno gv sqzqmlnjmtopqa iwtipqpwpqqz aqnjob kjobo omaj loppob qz mz " \
                "mlnjmtop qi smnnoh pg qpi zwsobqa ouwqdmlozp ozabynpoh wiqzc m iqsnlo smpjosmpqaml vwzapqqz mzh " \
                "aqzdobpoh tmae pg m loppob.".upper()
    main(myMessage)
```

```
Hacking Affine...

Key: 194

THE AFFINE CIPHER IS A TYPE OF MONOALPHABETIC SUBSTITUTION CIPHER WHERE EACH LETTER IN AN ALPHABET IS MAPPED TO ITS NUMERIC EQUIVALENT
```

بعد از تست هر کلید، باید راهی برای تشخیص انگلیسی بودن یا نبودن متن داشته باشیم. برای اینکار فایل EnglishDetect.py را ساختم. برای تشخیص انگلیسی بودن، متن را به تابع isEnglish میدهیم. این تابع متن را واژه به واژه جدا میکند و character های non-letter را با regular expressions حذف میکند. علت حذف این character ها بخاطر این است که اگر حذف نشوند باعث گمراهی الگوریتم میشوند. برای مثال، "Great!" کلمه ای انگلیسی است ولی علامت "!" باعث میشود که در بانک کلمات ما پیدا نشود.

بعد از حذف character های اضافی، در بانک کلماتی words.txt جستجو میکند و با هر کلمه ای که در بانک پیدا میکند، تعداد match ها را افزایش میدهد.

در نهایت برای هر متن درصدی را باز میگرداند و در صورتی که این درصد از مقدار از پیش تعیین شده ای مانند ۲۰ درصد بیشتر باشد، آن را به عنوان متن انگلیسی قبول میکند.

برای تشخیص انگلیسی بودن، برای محکم کاری، از پکیجی در پایتون به نام textbolb هم استفاده کردم که در ادامه آن را توضیح میدهم.

پس در affine، با تست هر کلید و تشخیص انگلیسی بودن یا نبودن، اگر الگوریتم رمز گذاری affine بوده باشد، در نهایت به جواب میرسیم.

الفبای تعریف شده هم برابر با ABCDEFGHIJKLMNOPQRSTUVWXYZ است و ورودی هرچه باشد، با استفاده از ()upper به capital تبدیل میشود و خروجی هم به صورت capital است. اینکار برای سادگی الگوریتم انجام شد.

در صورت پیدا نکردن جوابی با affine، با پیغام زیر روبرو میشویم:

```
Hacking Affine...
Affine Failed to hack encryption.
```

در مرحله ی آخر، صرفا جهت محکم کاری، از textblob برای تشخیص انگلیسی بودن یا نبودن استفاده کردم که در صورتی که این مرحله با شکست مواجه شود، پیغام Possible Warning: blob not detected را میدهد. برای استفاده از این پکیج **باید متصل به اینترنت** باشید.

شکستن رمز های Vigenere:

برای شکستن این رمز ها کار ما سخت تر است چون کلید میتواند حالت های بسیار زیادی داشته باشد.

برای Vigenere از روش Kasiski examination برای پیدا کردن حالت های محتمل اندازه کلید انتخاب شده و از روش تحلیل فرکانسی برای تحلیل متن های بدست آمده با کلید های محتمل برای بدست آوردن کلید اصلی استفاده کردم.

فایل freqAnalysis.py برای تحلیل فرکانسی است.

روش Kasiski examination اینگونه عمل میکند که رشته از حرف هایی که در متن تکرار میشوند را پیدا میکند. فاصله بین این رشته ها به احتمال زیاد باید ضریبی از طول این رشته ها باشد. برای مثال:

```
abcdeabcdeabcdeabcdeabcdeabcdeabc
crypto is short for cryptography.
```

با رمزی مثل abcde با طول 5 کلمه crypto با abcdea همسان میشود.

پس از پیدا کردن طول رمز های ممکن با این روش، کلید های مختلف را امتحان میکنیم و با تحلیل فرکانسی که انجام میدهیم، در نهایت برای هر رمز یک امتیازی بدست میاید.

بر اساس این امتیاز ها کلید های محتمل خود را میسازیم و متن را decrypt میکنیم.

بعد از بدست آمدن plaintext باید تشخیص دهیم که متن انگلیسی است یا نه که روش استفاده شده در قسمت قبلی توضیح داده شد.

```
if __name__ == '__main__':
    ciphertext = "Lqrserpr Bmlthqq DuFftrur bes nrwr Navjqbqu 11, 1974 nr Lav Frqqojw, Cmonjodqne, tth trlk fmmlp rk " \
                 "Mryhqmn PlHepdlt enp itvmqu hsmuf qsow dwxiew Liodjj HiOduvia. Knw fmwmir uv tj Ifdqmaz dsh Gquren " \
                 "phxqezw, frd tlx qofkjv, wtr nw Gquren-nrwr, ie rk Kedpfr azg Wyselfr azfjwtdb. Mms ylihlq qfqe, " \
                 "Ilqlexp, bes tlx qafhwrax jwenpifxhqu'x jidvy rayh. Qiozdwho'e ifxhqu med mfmmehhi qizrw wtmwzw ae " \
                 "ds erflxx azg imsfunfufrw sf oxqx capnq barp xifojw, azg bes qyjr dqsngtqq nr sqyjvax lxwuqv tj " \
                 "Ayhwmcmq Xtlqqisr, fkj guxw ximu-dzxonltkrmsmmcmo hsmuf qsow vjviqv gc tth qetq 'Kfvvqb Uikmu', " \
                 "f jruhsh or Jjsrsh'x. Peaqfvda'v uirrrwqazfj wkuoqw bqffqe aeamoqv ys huv uerqqyw emuqc oz, " \
                 "dsh arwjv sujsmns knq ub znxh m wfpezw fkezw blo idsxep Ojsnmuis ta sjvfaur ynphw xhq vyeqq qfqe " \
                 "Xhsry Ilqpimpx, HiOduvia ejkaz dutemunrq aq f ruyejv or wjpehlxmoz ftqmquhmaxv frd qqzqafltrax " \
                 "swsqddrw. "
    main(ciphertext)
```

```
Hacking Vigenere...
Possible hack with key AMDFE:
Leonardo Wilhelm DiCaprio was born November 11, 1974 in Los Angeles, California, the only child of Irmelin DiCaprio and former
```

رمزگشایی:

بعد از پیاده سازی هر دو روش، هر دو را در فایلی به نام main.py فرا خواندم. با دادن متن به هر دو تابع با خروجی مانند زیر مواجه میشوید:

```
Hacking Affine...
Affine Failed to hack encryption.

Hacking Vigenere...
Possible hack with key AMDFE:
Leonardo Wilhelm DiCaprio was born November 11, 1974 in Los Angeles, California, the only child of Irmelin DiCaprio and

Process finished with exit code 0
```

در این تست، متن داده شده با کلید AMDFE با Vigenere رمز گذاری شده است. با Affine شکسته نشد ولی با Vigenere با موفقیت شکسته شده است.