تمرین عملی اول درس امنیت

ملیکا عبداللهی
۹۴۳۱۸۰۴

پاییز ۹۷

توضیح سوال اول:

برای استفاده از کتابخانه‌ی hashlib در python لازم به اجرای دستور زیر می‌باشد:

```
import hashlib
```

سپس دو جمله مورد نظر در سوال تعریف می‌شوند. در جمله دوم نسبت به جمله‌ی اول حرف k از کلمه‌ی keep حذف شده است.

```
sen_1 = b'If you want to keep a secret, you must also hide it from yourself'

sen_2 = b'If you want to eep a secret, you must also hide it from yourself'
```

ابتدا با استفاده از تابع md5 در کتابخانه hashlib جملات با استفاده از 128 بیت کدگذاری می شوند. (کد زیر مربوط به انجام این مرحله روی جمله اول می‌باشد)

```
hash_object_1 = hashlib.md5(sen_1)
```

برای ظاهر ساختن این 128 بیت با فرمت hex از hexdigest() استفاده می‌شود. سپس خروجی hex با استفاده از تابع int به عدد صحیح تبدیل شده و با استفاده از تابع format به شکل باینری در می آید. (کد زیر مربوط به انجام این مرحله روی جمله اول می‌باشد)

```
sen_1_md5 = format(int(hash_object_1.hexdigest(), 16), '0128b')
```

ظاهر جملات به شکل hex به صورت زیر می‌باشد:

```
hashed sentence (original sentence): f868791dabbbba52bf6e7d9ca445a44b

hashed sentence (without k in keep): 7ad3558dc499707cbb212d6e3bc9f898
```

در مرحله بعد لیستی ساخته می‌شود که شامل اندیس‌هایی در جملات باینری است که با هم متفاوت می‌باشند. طول این لیست تعداد بیت هایی را نشان می‌دهد که با حذف یک حرف تغییر می‌کنند.

```
diff = [i for i in range(len(sen_1_md5)) if sen_1_md5[i] != sen_2_md5[i]]
```

اختلاف بیت‌های این دو جمله‌ی باینری 60 محاسبه شده است.

در مرحله‌ی بعد همین اعمال با استفاده از تابع SHA256 در کتابخانه‌ی hashlib انجام می‌شود. این تابع جملات را با 256 بیت کد می‌کند. ظاهر جمله ها به شکل hex به صورت زیر می‌باشد:

```
hashed sentence (original sentence):
aca0ba757235a44b8addac6f6419ecdbd37dcdd01661864e47de2ccf1bdef3b9

hashed sentence (without k in keep):
e8d988cf0918524680b712c95b4cae3d84a2c3112305e79295f8de1988cae503
```

اختلاف این دو جمله نیز 131 بیت محاسبه شده است.

توضیح سوال دوم:

در این سوال برای پیاده سازی الگوریتم رمزگذاری DES از کتابخانه‌ی pydes در پایتون استفاده می‌شود. برای نصب این کتابخانه در ترمینال سیستم عامل از دستور pip install pydes استفاده می‌شود.

ابتدا کلید و پیام مورد نظر با استفاده از خطوط زیر از فرمت hex به بایت تبدیل می‌شوند:

```
key = '133457799BBCDFF1'
message = '0123456789ABCDEF'
key = bytes.fromhex(key)
message = bytes.fromhex(message)
```

با استفاده از تابع des در کتابخانه‌ی pydes یک شی از الگوریتم des با کلید مورد نظر ساخته می‌شود.

```
des_obj = pd.des(key)
```

در مرحله‌ی بعد پیام مورد نظر با استفاده از شی des_obj به صورت زیر کدگذاری می‌شود.

```
m = des_obj.encrypt(message)
```

خروجی یا همان m به فرمت بایت می‌باشد که با تبدیل آن به فرمت hex شکل زیر را پیدا کرده است:

```
85e813540f0ab405
```

توضیح سوال سوم:

مقدار شیفت مربوط به الگوریتم کدگذاری سزار در این متن برابر با ۱۶ می‌باشد. (برای الگوریتم سزار یک مقدار شیفت تعریف می‌شود و حروف الفبا طبق این مقدار شیفت جابه‌جا می‌شوند.)

متن کد شده به صورت زیر است:

Jxu Squiqh Syfxuh jusxdygku yi edu ev jxu uqhbyuij qdt iycfbuij cujxet ev udshofjyed jusxdygku. Yj'i iycfbo q jofu ev ikrijyjkjyed syfxuh, y.u., uqsx bujjuh ev q wylud junj yi hufbqsut ro q bujjuh iecu vynut dkcruh ev feiyjyedi temd jxu qbfxqruj. Veh unqcfbu myjx q ixyvj ev 1, Q mekbt ru hufbqsut ro R, R mekbt rusecu S, qdt ie ed. Jxu cujxet yi qffqhudjbo dqcut qvjuh Zkbyki Squiqh, mxe qffqhudjbo kiut yj je secckdysqju myjx xyi evvysyqbi.

Jxki je syfxuh q wylud junj mu duut qd ydjuwuh lqbku, ademd qi ixyvj mxysx ydtysqjui jxu dkcruh ev feiyjyed uqsx bujjuh ev jxu junj xqi ruud celut temd.

متن اصلی و کد نشده نیز به صورت زیر می‌باشد:

The Caesar cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.