به نام خدا

تمرین سری دوم درس امنیت

زهرا دهقانیان

۹۴۳۱۰۳۹

پاییز ۹۷

سوال ۱)

در قسمت اول این سوال از ما خواسته شده که به کمک کتابخانه hashlib دو تابع درهم ساز sha256 و md5 را اجرا کنیم که این کار به سادگی به کمک خطوط زیر قابل انجام است :

```
sha = hashlib.sha256()
md = hashlib.md5()
sha.update(b"If you want to keep a secret, you must also hide it from
yourself")
md.update(b"If you want to keep a secret, you must also hide it from
yourself")
print("<--- question 1 --->")
print("##plain text : If you want to keep a secret, you must also hide
it from yourself")
print("##cipher text with sha256 : " + sha.hexdigest())
print("##cipher text with md5 : " + md.hexdigest())
```

که خروجی حاصل از اجرای کد فوق خواهد بود :

```
<--- question 1 --->
##plain text : If you want to keep a secret, you must also hide it from yourself
##cipher text with sha256 : aca0ba757235a44b8addac6f6419ecdbd37dcdd01661864e47de2ccf1bdef3b9
##cipher text with md5 : f868791dabbbba52bf6e7d9ca445a44b
```

و با تغییر ۱ حرف در ورودی (حذف آخرین کاراکتر) خروجی به صورت زیر است :

```
<--- delete last character --->
##plain text : If you want to keep a secret, you must also hide it from yoursel
##cipher text with sha256 : fe7bdf530a9c6754dccc4fe5036f3f98d2a5b50268c45ac51644ac489c0322be
##cipher text with md5 : 953e0491d5151987c3a5d1b56815b3f1
```

سوال ۲)

در این بخش به کمک کتابخانه PYDes به حل این سوال میپردازیم و به کمک قطعه کد ساده زیر این سوال را حل میکنیم :

```
import pyDes
data = b"0123456789ABCDEF"
k = pyDes.des(bytes.fromhex("133457799BBCDFF1"))
d = k.encrypt(data)
print("<--- question 2 --->")
print("##plain text : "+str(data))
print("##cipher text with DES : %r" % d)
print("##Decrypted text : %r" % k.decrypt(d))
```

که خروجی کد بالا معادل زیر خواهد بود :

```
<--- question 2 --->
##plain text : b'0123456789ABCDEF'
##cipher text with DES : b'l\xbd"\x85\x8b\xce\xdby\xab\xa1\xa7\xbe"\x14\xc5B'
##Decrypted text : b'0123456789ABCDEF'
```

سوال ۳)

یکی از روش های مرسوم در مواجهه با متن رمز شده توسط الگوریتم سزار زمانی که تنها ciphertext را داشته باشیم frequency analysis است ، به این صورت که بررسی میکند که هر حرفی در متن رمز شده چند با تکرار میشود و به کمک اطلاعات آماری از پیش دانسته کلید را شناسایی میکند یعنی به طور مثال میدانیم حرف e بیشترین تکرار را داراست پس به احتمال زیاد حرفی که بیشترین تکرار را دارد شیفت یافته همین حرف خواهد بود.

اما یک راه راحت تر برای حل این مسیله این است که متن رمز شده را به عنوان متن ساده در ورودی **cryptool** قرار دهیم و با کلید های مختلف شیفت دهیم و هر گاه در خروجی به متن معناداری رسیدیم میفهمیم که کلید را بدست آوردیم.

در مثال فوق با اعمال رویکرد بالا با ۱۰ بار چرخش به متن با مفهوم میرسیم پس کلید الگوریتم سزار باید ۱۶= ۱۰ - ۲۶ باشد . متن حاصل از رمزگشایی عبارت صورت سوال به شکل زیر است:

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.