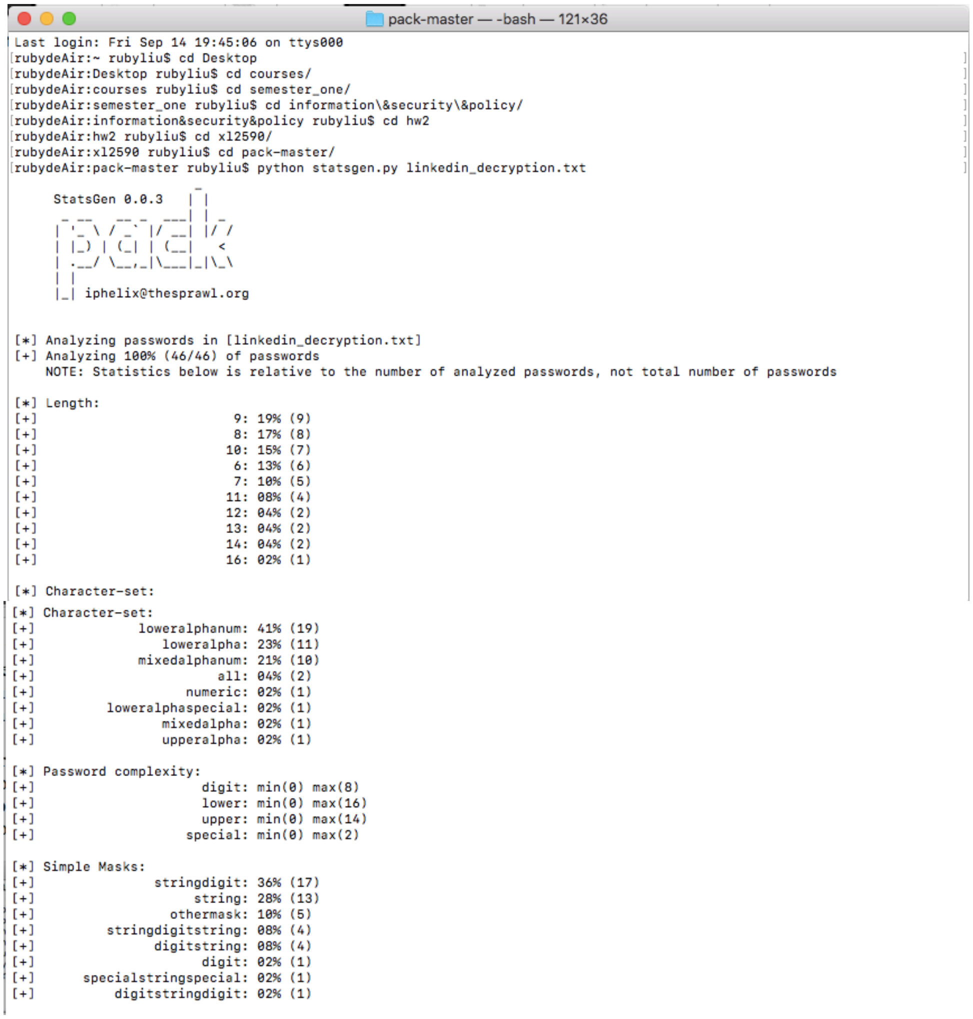
1.The technique you used to obtain the passwords

First consider whether the encryption algorithm is reversible. If it is reversible, the code of the decryption algorithm can be implemented for the encryption algorithm. Considering that the encryption algorithms used in this time are irreversible algorithms, they can only be solved by exhaustive methods.

First of all, I look for some websites on the Internet and can brute force ciphertext information. Through a small amount of plaintext information provided by the website, it is possible to infer the general rules of plain text editing. By putting these plaintexts' information into the PACK tool, which is used to analyze the password. And I can analyze the normal rule of the existence of the plaintext. Through this result, I can find the corresponding password library, and then save the password library to the corresponding file. The analysis results are as follows,



```
Last login: Fri Sep 14 19:45:06 on ttys000
rubydeAir:~ rubyliu$ cd Desktop
rubydeAir:Desktop rubyliu$ cd courses/
rubydeAir:courses rubyliu$ cd semester_one/
rubydeAir:semester_one rubyliu$ cd information\&security\&policy/
rubydeAir:information&security&policy rubyliu$ cd hw2
rubydeAir:hw2 rubyliu$ cd x12590/
rubydeAir:x12590 rubyliu$ cd pack-master/
rubydeAir:pack-master rubyliu$ python statsgen.py linkedin_decryption.txt
                       _
     StatsGen 0.0.3   | |
      _ __   __ _  ___| | _
     | '_ \ / _` |/ __| |/ /
     | |_) | (_| | (__|   <
     | .__/ \__,_|\___|_|\_\
     | |
     |_| iphelix@thesprawl.org


[*] Analyzing passwords in [linkedin_decryption.txt]
[+] Analyzing 100% (46/46) of passwords
    NOTE: Statistics below is relative to the number of analyzed passwords, not total number of passwords

[*] Length:
[+]                         9: 19% (9)
[+]                         8: 17% (8)
[+]                        10: 15% (7)
[+]                         6: 13% (6)
[+]                         7: 10% (5)
[+]                        11: 08% (4)
[+]                        12: 04% (2)
[+]                        13: 04% (2)
[+]                        14: 04% (2)
[+]                        16: 02% (1)

[*] Character-set:
[*] Character-set:
[+]             loweralphanum: 41% (19)
[+]                loweralpha: 23% (11)
[+]             mixedalphanum: 21% (10)
[+]                       all: 04% (2)
[+]                   numeric: 02% (1)
[+]         loweralphaspecial: 02% (1)
[+]                mixedalpha: 02% (1)
[+]                upperalpha: 02% (1)

[*] Password complexity:
[+]                     digit: min(0) max(8)
[+]                     lower: min(0) max(16)
[+]                     upper: min(0) max(14)
[+]                   special: min(0) max(2)

[*] Simple Masks:
[+]               stringdigit: 36% (17)
[+]                    string: 28% (13)
[+]                 othermask: 10% (5)
[+]         stringdigitstring: 08% (4)
[+]               digitstring: 08% (4)
[+]                     digit: 02% (1)
[+]      specialstringspecial: 02% (1)
[+]          digitstringdigit: 02% (1)
```

2.Other techniques you considered.

In fact, the first way I think of is to directly exhaustive, for example, a six-digit password, which can be one to six letters or five letters and one number, and so on, to give a different possible passwords Choice.

And, the easiest way is to directly input ciphertext information from some tool websites, and directly obtain the plaintext information through the powerful computing power of the server serve.

3.How were the passwords stored? Compare the difficulty in cracking passwords protected with each type of storage

Most of the passwords I have cracked are the first half of the letter form, followed by the number, which is also the ordinary password composition mode. Passwords that are more difficult to decipher are first composed of multiple symbols, including letters, numbers, and special symbols. Passwords that are the most difficult to decipher should be a mixture of the above three forms. When letters, numbers and special symbols are mixed, the possibility of password deciphering is the lowest.