**Password Cracking**

**2017313135 소프트웨어학과 권동민**

**Q1. Password cracking md5.txt using John the Ripper**

John the ripper version : john-1.9.0-jumbo-1

Check the first state



I first using just default password.lst file to crack the file md5.txt.

(I just set the mask ‘\w’ It means that I used password.lst only – not repeat)

텍스트이(가) 표시된 사진

자동 생성된 설명

There are just 6 password that is cracked.

In general, if it is hybrid mode, it means to crack by mask and password list to specify the string’s form. But I don’t have any idea about strings of sample md5.txt, so I just used standard mode to crack(not using mask and wordlist).

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

But I can’t crack 41 words. (I think that last 41 has special char)

**Q2. Password cracking md5.txt using Hashcat**

Straight mode:



텍스트이(가) 표시된 사진

자동 생성된 설명

Wordlist mode:



Using mask:



Hybrid mode:





**Q3. Which is faster(JDR, Hashcat)**

After I used both crack tools(john the ripper and Hashcat). I can see that there is huge difference between Hashcat and John the Ripper. In Hashcat, sometimes it showed some messages during execution because mask is change.

Hashcat:







John the Ripper:

텍스트이(가) 표시된 사진

자동 생성된 설명

We can know that Hashcat cracks ordered by string’s length, but john the ripper’s cracking order is not huge related to length of the string.

These are the result of cracking by using each crack tool after 10 minutes from starting.



텍스트이(가) 표시된 사진

자동 생성된 설명

John the ripper cracked 120 words but Hashcat crack just 77 words. So it seems that John the Ripper is more faster than Hashcat.

**Q4. Create own password cracking dictionary(wordlist)**

**-attach separate file(.txt)**

**Q5. Create own 4098 bit RSA private, public key using openssl**

Order of commands:

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

**Q6. Create own X.509 digital certificate using openssl**

텍스트이(가) 표시된 사진

자동 생성된 설명