


Infini45T

박준혁 (한국디지털미디어고등학교 1학년)

2011.07.10

## 1번 문제

다음과 같은 .prx 형식의 파일이 주어진다.

 securityNO.prx

우선 prx 파일이 맞는지 파일 시그니처를 이용해 알아보자.

파일 시그니처들의 모음이 있는 사이트는 [http://www.garykessler.net/library/file\\_sigs.html](http://www.garykessler.net/library/file_sigs.html) 이다.


파일 시그니처를 보기 위해 hexs 에디터로 열어보았다.

1F 8B 08 대충 이렇게 앞의 것들을 검색해서 실제 확장자를 찾는다.


```
1F 8B 08 08 B6 99 FC 4D 00 03 73 65 63 75 72 69 .<...Qum..securi
74 79 4E 4F 2E 6C 69 62 00 9D 7C 43 AC 28 0A B0 tyNO.lib..|C- (.°
74 79 4E 4F 2E 6C 69 62 00 9D 7C 43 AC 28 0A B0 tyNO.lib..|C- (.°
```

위의 파일 시그니처 사이트에 찾아보니 gz 확장자인 것을 알았다.

확장자를 gz 으로 바꾸고 압축을 풀어보았다.

 securityNO.gz


다음과 같이 securityNO.lib 파일이 나왔다.

 securityNO.lib


또 다시 hexs 로 파일 시그니처를 보았다.

```
50 4B 03 04 14 00 00 00 08 00 37 5E C9 3E 39 D0 PK.....7^É>9Đ
1D B7 97 53 00 00 1B AF 00 00 0E 00 08 00 73 65 .-S...-.....se
68 75 73 68 74 70 4E 4F 2E 6C 73 70 73 73 75 04 00 securityNO.lib.¿
```

파일 시그니처를 검색후 PK, zip파일인것을 알았고 확장자를 변경했다.

 securityNO.zip


또 압축을 푸니 hwp파일이 나왔다.

 securityNO.hwp

헥스로 보니 FWS, swf 파일인 것을 알았다.

```
46 57 53 04 1B AF 00 00 78 00 06 D6 00 00 1B 58 FWS...x..Ö...X
00 00 01 02 00 35 08 01 00 7B 2C 86 5B 8C E4 19 .....5...{,+[æ.
D2 00 01 12 8D DB B3 D8 68 33 9A 02 00 21 5F 21 ò  ñ²ñ³³  1 1
```

swf로 확장자를 변경후 실행해보았다.

 securityNO.swf

NAHS9229 라는 키 값이 나왔고 인증에 성공했다.

**NAHS9229**

## 2번 문제

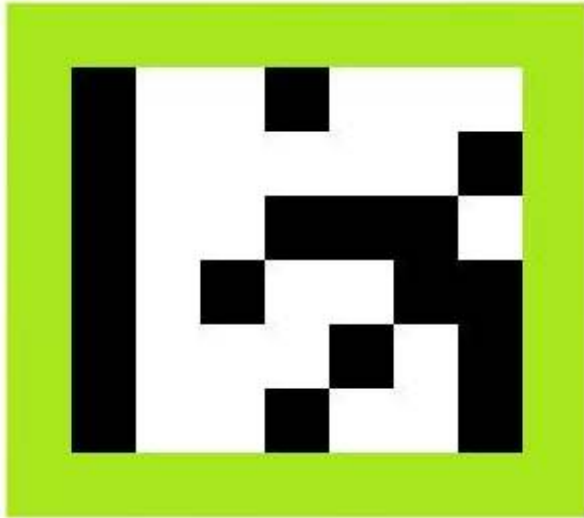
다음과 같은 qr코드가 주어졌다.



나는 XRen QRCode Tool 을 이용해서 qr코드를 디코드했다.  
디코드 결과 <http://m.site.naver.com/00UHw> 사이트가 나왔다.



위의 사이트에 들어가 다음과 같은 사진을 다운받았다.



처음에는 뭔가 했는데 작년 hust 대회와 비슷하다는 생각이 들고 흑을 1로, 백을 0으로 하여 6줄짜리 아스키 코드를 작성해 보았다.

```
1001000
1000001
1001110
1010011
1000101
1001001
```

다음과 같은 2진수 아스키코드를 만들었고, 계산기를 이용해 10진수로 변환해보았다.

```
72
65
78
83
69
73
```

다음과 같은 10진수가 나왔고, 아스키표를 이용해 문자로 변환해보았다.

HANSEI 라는 키 값이 나왔고 인증에 성공했다.

### 3번 문제

3번 문제는 대회 도중 운영진들의 협의 결과 취소되었고 4번으로 넘어갔다.

Stage 3

1	2	1	1	2		2	2	2	2	2
2	2	1	2		1					

우연히 책상정리를 하다가 예전 초등학교 때 친구들과 장난삼아 주고받았던 비밀 편지를 발견하였다. 추억에 잠겨 잠시 예전에 썼던 글을 읽어보다 마지막 글귀를 보고 웃고 말았다.

정답 :

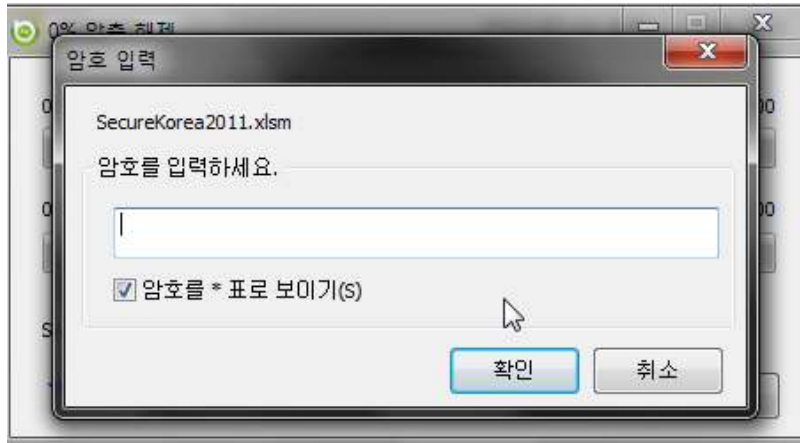
제출하기

#### 4번 문제

다음과 같은 zip 파일이 주어진다.

 reversing.zip

압축 풀기를 시도했으나 암호가 있는것을 확인 할 수 있다.



나는 AZPR 프로그램으로 비밀번호를 구하기로 하였다.



대회는 시간제한이 있으므로, 복잡한 비밀번호는 아닐것이라 생각하고 Length를 5로 잡고 브루트포싱을 시작했고, sK2! 라는 비밀번호를 얻었다.



압축을 해제하니 다음과 같은 xlsx 파일이 나왔다.

SecureKorea2011.xlsx

hex로 열어보니 PK, zip파일인 것을 알 수 있었다.

```
50 4B 03 04 14 00 00 00 08 00 00 00 21 00 B5 55 PK.....!.pU
30 23 EB 00 00 00 4C 02 00 00 0B 00 08 00 5F 72 0#ë...L....._r
65 6C 73 2F 2F 72 65 6C 73 7A F5 04 00 B5 03 00 a1e/ r1972 "

```

zip으로 확장자를 바꾸어 압축을 풀니 다음과 같은 파일들이 나왔다.

2011 Codegate 대회와 비슷하게 엑셀을 이용한 문제가 나와서 어려울까봐 겁을 먹었다.

\_rels  
 doc  
 docProps  
 xl  
 [Content\_Types].xml

다행히 doc 폴더에 exe가 숨김형태로 들어있는 것을 발견했다.

SecureKorea2011.exe

실행시켜보니 다음과 같이 숫자로만 Password를 입력받고, 리버싱 문제라고 친절하게 설명까지 되어있다.

```
Secure Korea 2011!
=====

Created by Korea!
-----

This is reversing quiz.

password is ONLY numbers!

Password: _
```

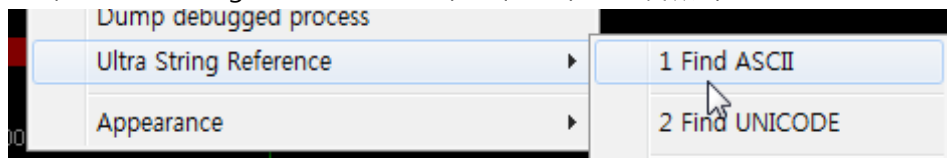
Password에 아무 숫자나 입력했더니 Wrong! 이라는 글씨가 떴다.

```
Password: 1234

Wrong! _
```

리버싱을 하기위해 올리디버거로 우선 열었다.

그리고 Ultra String Reference 를 이용해 문자열을 찾았다.



다음과 같이 문자열들이 보인다.

```
004014AA MOV DWORD PTR SS:[ESP+4],SecureKo,004401
004014E2 MOV DWORD PTR SS:[ESP+4],SecureKo,004401 password is ONLY numbers!
0040152E MOV DWORD PTR SS:[ESP+4],SecureKo,004401 Password:
00401572 MOV DWORD PTR SS:[ESP+4],SecureKo,004401 Congratulations! ^^
004015A8 MOV DWORD PTR SS:[ESP+4],SecureKo,004401 Wrong!
0040251E MOV DWORD PTR DS:[EAX],SecureKo,004425D0 020
```

Wrong! 를 더블클릭하여 해당 주소로 이동하였다.

```
00401566 . C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C0
0040156D . E8 2E8C0200 CALL SecureKo,0042A1A0
00401572 . C74424 04 B8 MOV DWORD PTR SS:[ESP+4],SecureKo,004401 Congratulations! ^^
0040157A . C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C0
00401581 . E8 C2AC0300 CALL SecureKo,0043C248
00401586 . C70424 60344 MOV DWORD PTR SS:[ESP],SecureKo,00443460
0040158D . E8 AE460200 CALL SecureKo,00425C40
00401592 . EB 34 JMP SHORT SecureKo,004015C8
00401594 > C74424 04 B8 MOV DWORD PTR SS:[ESP+4],SecureKo,0043B8
0040159C . C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C0
004015A3 . E8 F88B0200 CALL SecureKo,0042A1A0
004015A8 . C74424 04 CE MOV DWORD PTR SS:[ESP+4],SecureKo,004401 Wrong!
004015B0 . C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C0
```



위로 올려 Congratulations! ^~^ 로 점프하는구간 위에 CMP로 비교하는 구간이 있다.  
스택의 값을 77DE5E8C와 비교한다.

```
00401555 817D FC 8C5E CMP DWORD PTR SS:[EBP-4],77DE5E8C
0040155C 75 36 JNZ SHORT SecureKo,00401594
0040155E C74424 04 18 MOV DWORD PTR SS:[ESP+4],SecureKo,0043B
00401566 C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C
0040156D E8 2E8C0200 CALL SecureKo,0042A1A0
00401572 C74424 04 B8 MOV DWORD PTR SS:[ESP+4],SecureKo,00440 Congratulations! ^~^
```

Password가 오직 숫자라고 했으니 16진수인 77DE5E8C 를 10진수로 바꾸면 2011061900이 나온다.

다음과 같이 프로그램에서 정상적으로 작동되는 것을 볼 수 있고, 인증 결과 인증에 성공하였다.

```
password is ONLY numbers?

Password: 2011061900

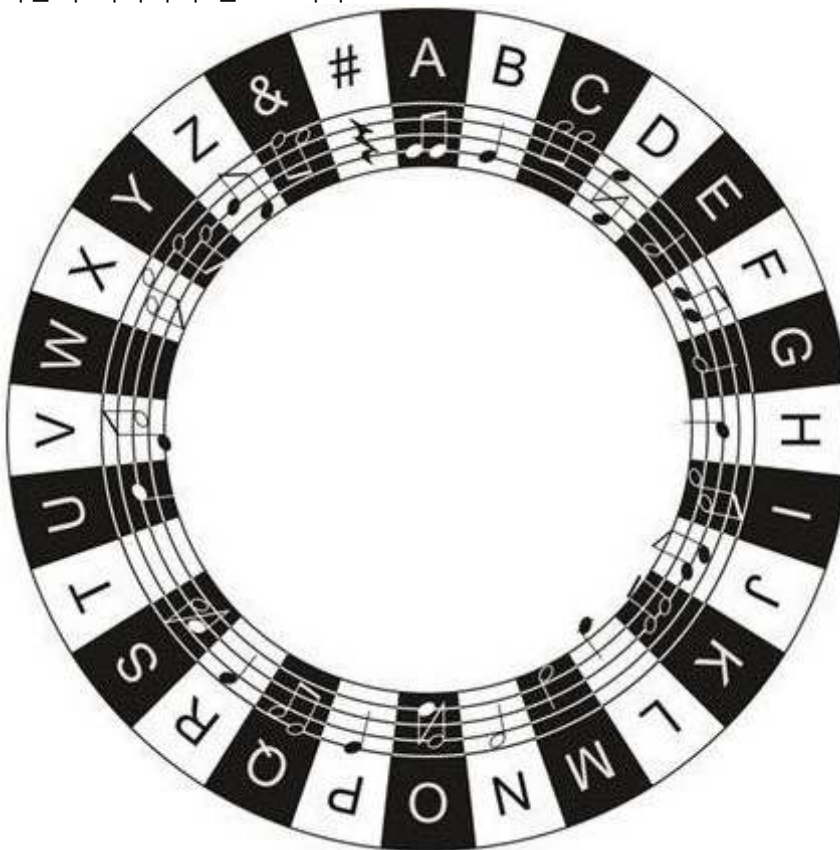
Congratulations! ^~^
```

### 5번 문제

다음과 같은 악보가 주어진다.




암호라는 생각이 들었고 음표암호를 검색, 마타하리 암호라는것을 알아냈다.  
다음이 마타하리 암호표이다.




위의 암호표대로 디코드하니 SECURITY가 나왔고 인증에 성공했다.

## 6번 문제

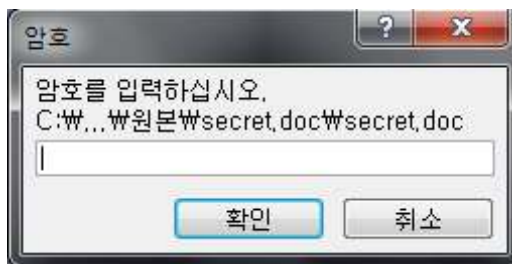
다음과 같이 gz 파일을 준다.

 secret.doc.gz

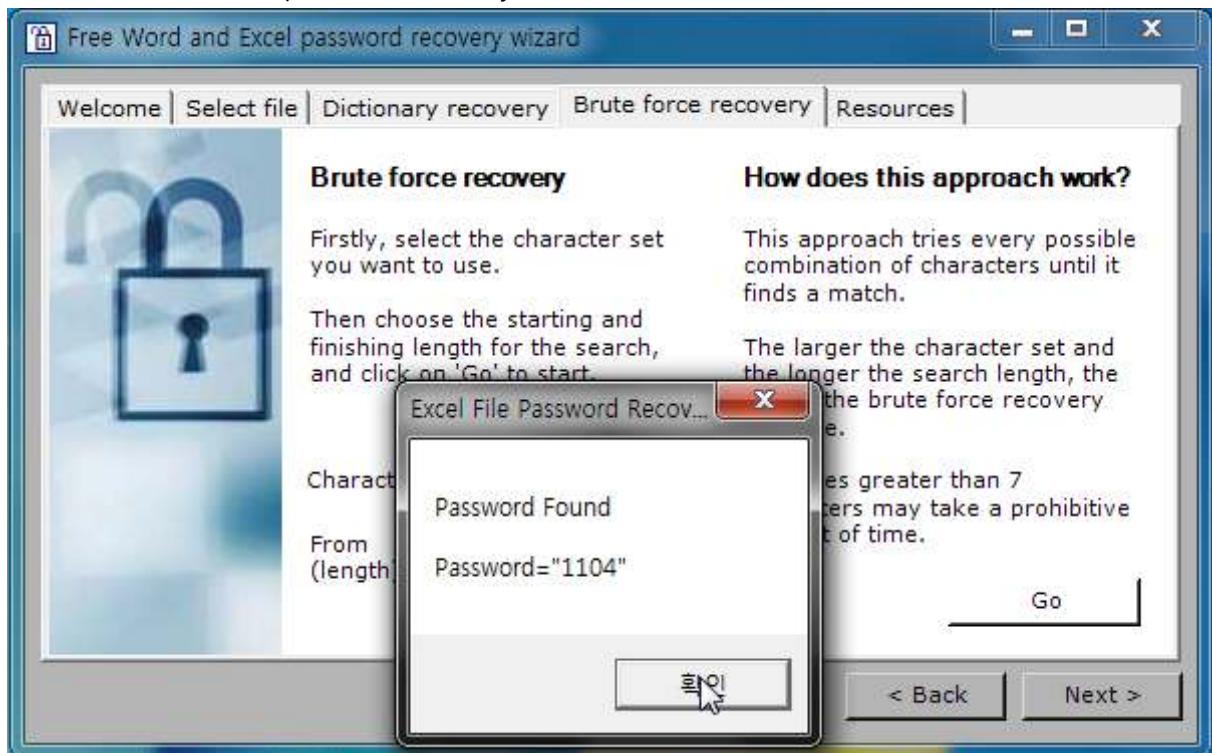
압축을 풀어보니 doc 파일을 준다.

 secret.doc

실행시켜보니 암호를 입력하라고 한다.



Free Word and Excel password recovery wizard 프로그램을 이용해서 비밀번호를 찾았다.



실행시켜보니 1104에서 100을 뺀 값을 인증시키라고한다.

패스워드를 찾으셨군요.

↵

패스워드에서 100을 뺀 값을 답안에 기입해주세요.

1004를 인증시켰고 인증에 성공했다.

## 7번 문제

7번 문제는 웹 해킹 문제였다.

로그인 폼이 있었고, securekorea 계정으로 로그인하라고 했다.

우선 내 아이디로 로그인 해보았다.

그러자, 쿠키에 user='아이디를 base64로 2번 인코드 한 값' 이 들어갔다.

securekorea를 base64로 2번 인코드 한 값을 쿠키에 넣어주니 다음과 같은 글이 떴다.

축하합니다. securekorea 계정으로 로그인 되었습니다.

아래의 코드값을 분석하여 전달하고자 하는 기밀 정보를 알아내시면 정답입니다.


코드값 : 115,101,99,117,114,101,35,107,111,114,101,97,35,95,49,95,67,111,110

코드값이 아스키코드라고 생각하여 디코드해보았다.

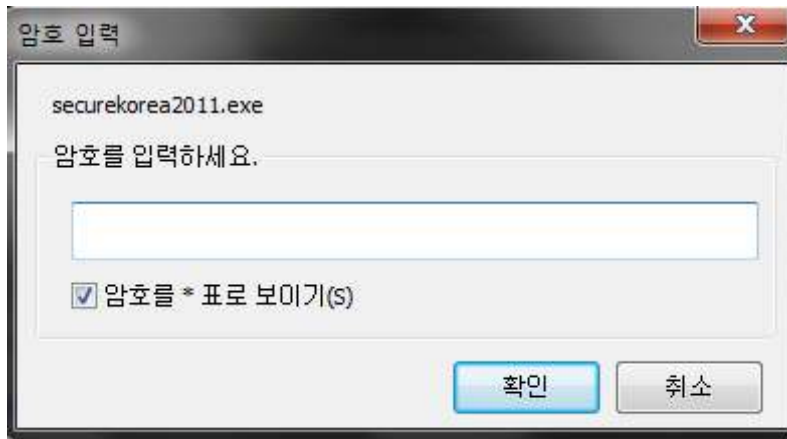
secure#korea#\_1\_Con 다음과 같은 키 값이 나왔고 인증에 성공했다.

## 8번 문제

8번 문제는 아무도 풀지 못하였고, 푸는 도중 대회가 끝났었다.  
다음과 같은 zip 파일을 준다.

 SecureKorea2011-Reversing.zip

다음과 같이 암호가 걸려있다.




AZPR로 브루트포싱을 하니 Sk@0! 라는 비밀번호를 얻었다.



압축을 풀면 다음과 같이 exe 파일이 나온다.

 securekorea2011.exe

압축을 푸니 securekorea2011-1.exe가 나왔다.

 securekorea2011-1.exe

다음과 같이 콘솔에서 작동하고 1234를 입력했더니 Fail! 라는 문자열이 출력되었다.

```
=====
Secure Korea 2011 해킹방어대회
=====

KEY를 입력하세요 : 1234
Fail!

KEY를 입력하세요 :
```

올리디버거로 열어보니 다음과 같이 어셈블된 코드들이 보인다.

패킹된것을 알 수 있다.

Address	Hex dump	Disassembly	Comment
00409720	\$ 60	PUSHAD	
00409721	, BE 00804000	MOV ESI,secureko,00408000	
00409726	, 80BE 0090FFF	LEA EDI,DWORD PTR DS:[ESI+FFFF9000]	
0040972C	, 57	PUSH EDI	
0040972D	, EB 0B	JMP SHORT secureko,0040973A	
0040972F	90	NOP	
00409730	> 8A06	MOV AL,BYTE PTR DS:[ESI]	
00409732	, 46	INC ESI	
00409733	, 8807	MOV BYTE PTR DS:[EDI],AL	
00409735	, 47	INC EDI	
00409736	> 010B	ADD EBX,EBX	

밑으로 내려보니 JMP로 점프를 하는 구간이 보인다.

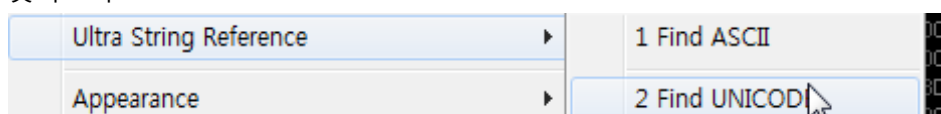
브레이크포인트를 걸고 실행시켜보자.

Address	Hex dump	Disassembly	Comment
00409891	, 57	PUSH EDI	
00409892	, FFD5	CALL EBP	
00409894	, 58	POP EAX	
00409895	, 61	POPAD	
00409896	, 8D4424 80	LEA EAX,DWORD PTR SS:[ESP-80]	
0040989A	> 6A 00	PUSH 0	
0040989C	, 39C4	CMP ESP,EAX	
0040989E	, 75 FA	JNZ SHORT secureko,0040989A	
004098A0	, 83EC 80	SUB ESP,-80	
004098A3	, E9 F07EFFFF	JMP secureko,00401798	
004098A8	, 48	DB 48	CHAR 'H'

그리고 F8을 누르면 점프되어 언패킹된 후의 스타트포인트로 간다.

Address	Hex dump	Disassembly	Comment
00401798	E8 7B040000	CALL secureko,00401C18	<Initial CPU
0040179D	E9 9FFDFFFF	JMP secureko,00401541	
004017A2	8BFF	MOV EDI,EDI	
004017A4	55	PUSH EBP	
004017A5	8BEC	MOV EBP,ESP	
004017A7	81EC 28030000	SUB ESP,328	
004017AD	A3 48614000	MOV DWORD PTR DS:[406148],EAX	
004017B2	890D 44614000	MOV DWORD PTR DS:[406144],ECX	
004017B8	8915 40614000	MOV DWORD PTR DS:[406140],EDX	

실제 코드가 존재하는 부분이므로 Ultra String Reference 플러그인을 이용해 UNICODE를 찾아보자.



다음과 같이 문자열이 뜬다.

2735f2c54e255f10ba7f03b6e318b843 이라는 md5값이 보인다.

Address	Disassembly	Text String
00402DC6	PUSH secureko,004042B8	2735f2c54e255f10ba7f03b6e318b843
00402E7B	MOV ESI,secureko,00404244	TTqP0/SoJReLPD0eRg?WJSSSWDqh0juVvheLQTGSKQGW_BR2RCB6MN: :
00402EC9	PUSH secureko,00404290	C:WindowsSystem32
00402FF8	PUSH secureko,004042DC	%02x
004030B4	PUSH secureko,004041A4	cls=====wn
004030C2	PUSH secureko,004041A8	=====wn
004030D5	PUSH secureko,004041CC	Secure Korea 2011 해킹방어대회 wn
004030E9	PUSH secureko,004041F0	=====wnwn
0040310A	PUSH secureko,00404214	KEY를 입력하세요 : Success!
004031C9	PUSH secureko,00404228	Success!
004031E4	PUSH secureko,00404234	pause
00403236	PUSH secureko,0040423C	Fail!



<http://www.md5decrypter.com/> 사이트에서 md5 디코드를 해보자.

다음과 같이 디코드된 결과가 뜬다.

저 주소가 답이거나 저 메일주소로 메일을 보내면 뭔가 더 있을 것 같지만 대회가 종료되어 아쉽게 풀지는 못하였다.

Results
Md5 Hash: 2735f2c54e255f10ba7f03b6e318b843
Normal Text: nanum.info@gmail.com