

28

Do you have a password?

[main](#) [Back](#)

암호를 풀어야 뭘 볼수 있지! 암호가 있거나 한건가!
이 문제를 낸 사람은 너무 쉬워서 사람들이 빨리 풀지
않을까 걱정하다가 시름시름 앓고 있다는 전설이 있다.

Does it have a real password?

I am afraid that this challenge is very esay.

You need not do brute-force

[down](#)

Thanks to : heizelnet

이름



Am_I_key.zip*



Am_I_key2.txt*



Am_I_key3.txt*

압축파일을 다운 받으면 안에 이 3가지 암호화된 파일이 들어있는 걸 확인 할 수 있다.

해당 파일의 flag 부분을 보면

HxD - [C:\Users\ReverseEngineering\Desktop\So_Simple.zip]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?

16 ANSI 16 진수

So_Simple.zip

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000120	00	00	00	A5	05	00	00	0D	00	00	00	41	6D	5F	49	5F	...₩.....Am_I
00000130	6B	65	79	33	2E	74	78	74	73	29	CD	CD	AD	74	19	25	key3.txts)íí.t.%
00000140	46	89	51	62	94	18	25	06	25	01	00	50	4B	01	02	14	F%Qb".%.%.PK...
00000150	00	14	00	09	08	08	00	FD	78	55	43	23	13	24	6C	92	...[.ýxUC#. \$l'
00000160	00	00	00	CD	00	00	00	0C	00	08	00	00	00	00	00	01	...í.....
00000170	00	20	00	00	00	00	00	00	00	00	41	6D	5F	49	5F	6BAm_I ke
00000180	79	2E	7A	69	70	7A	E5	04	00	B5	03	00	00	50	4B	01	y.zipzâ..µ...PK.
00000190	02	14	00	14	00	09	08	08	00	C4	79	55	43	AA	7C	88ÄyUC^ ^
000001A0	E7	1E	00	00	00	EF	10	00	00	0D	00	00	00	00	00	00	Ç....i.....
000001B0	00	01	00	20	00	00	00	C4	00	00	00	41	6D	5F	49	5FÄ...Am_I
000001C0	6B	65	79	32	2E	74	78	74	50	4B	01	02	14	00	14	00	key2.txtPK.....
000001D0	09	08	08	00	9C	79	55	43	83	EC	3E	A4	13	00	00	00	...øyUCfi>ø....
000001E0	A5	05	00	00	0D	00	00	00	00	00	00	01	00	20	00	00	₩.....
000001F0	00	00	0D	01	00	00	41	6D	5F	49	5F	6B	65	79	33	2EAm_I_key3.
00000200	74	78	74	50	4B	05	06	00	00	00	03	00	03	00	B8	00	txtPK.....,

오프셋: 153 블록 153-154 길이: 2 덮어쓰기

HxD - [C:\Users\ReverseEngineering\Desktop\So_Simple.zip]

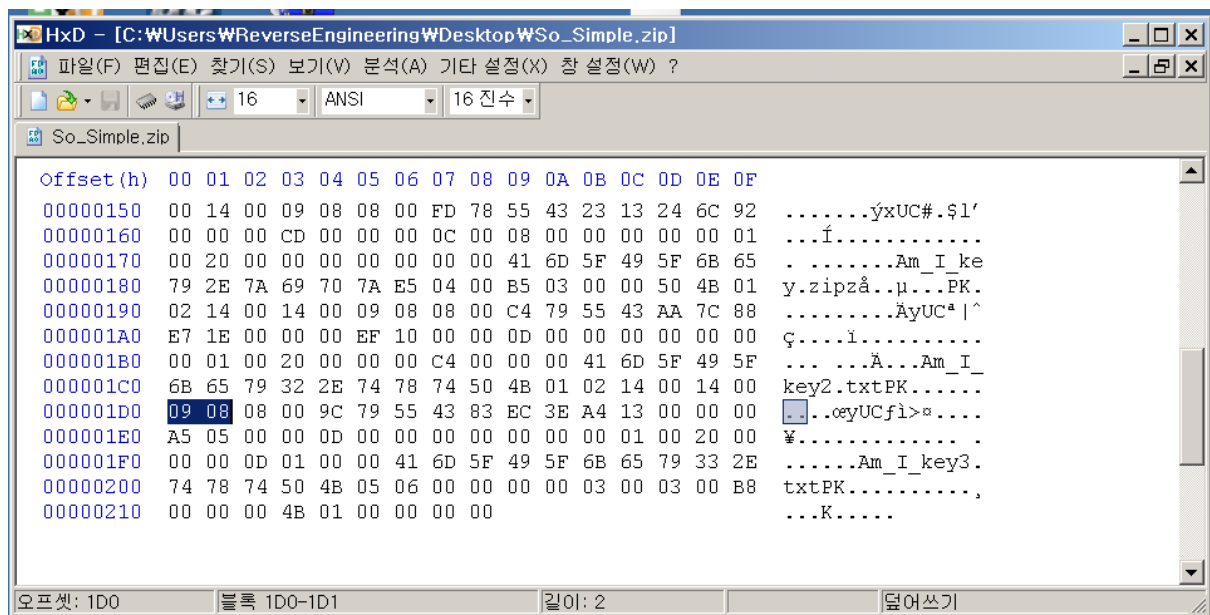
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?

16 ANSI 16 진수

So_Simple.zip

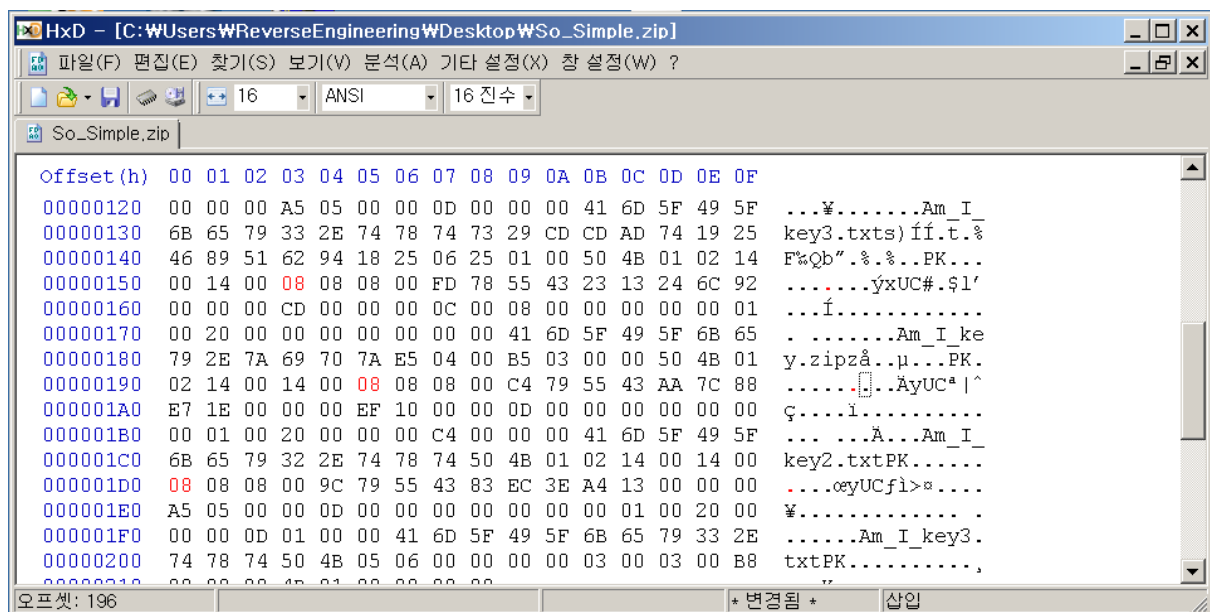
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000120	00	00	00	A5	05	00	00	0D	00	00	00	41	6D	5F	49	5F	...₩.....Am_I
00000130	6B	65	79	33	2E	74	78	74	73	29	CD	CD	AD	74	19	25	key3.txts)íí.t.%
00000140	46	89	51	62	94	18	25	06	25	01	00	50	4B	01	02	14	F%Qb".%.%.PK...
00000150	00	14	00	09	08	08	00	FD	78	55	43	23	13	24	6C	92	...[.ýxUC#. \$l'
00000160	00	00	00	CD	00	00	00	0C	00	08	00	00	00	00	00	01	...í.....
00000170	00	20	00	00	00	00	00	00	00	00	41	6D	5F	49	5F	6BAm_I ke
00000180	79	2E	7A	69	70	7A	E5	04	00	B5	03	00	00	50	4B	01	y.zipzâ..µ...PK.
00000190	02	14	00	14	00	09	08	08	00	C4	79	55	43	AA	7C	88ÄyUC^ ^
000001A0	E7	1E	00	00	00	EF	10	00	00	0D	00	00	00	00	00	00	Ç....i.....
000001B0	00	01	00	20	00	00	00	C4	00	00	00	41	6D	5F	49	5FÄ...Am_I
000001C0	6B	65	79	32	2E	74	78	74	50	4B	01	02	14	00	14	00	key2.txtPK.....
000001D0	09	08	08	00	9C	79	55	43	83	EC	3E	A4	13	00	00	00	...øyUCfi>ø....
000001E0	A5	05	00	00	0D	00	00	00	00	00	00	01	00	20	00	00	₩.....
000001F0	00	00	0D	01	00	00	41	6D	5F	49	5F	6B	65	79	33	2EAm_I_key3.
00000200	74	78	74	50	4B	05	06	00	00	00	03	00	03	00	B8	00	txtPK.....,

오프셋: 195 블록 195-196 길이: 2 덮어쓰기



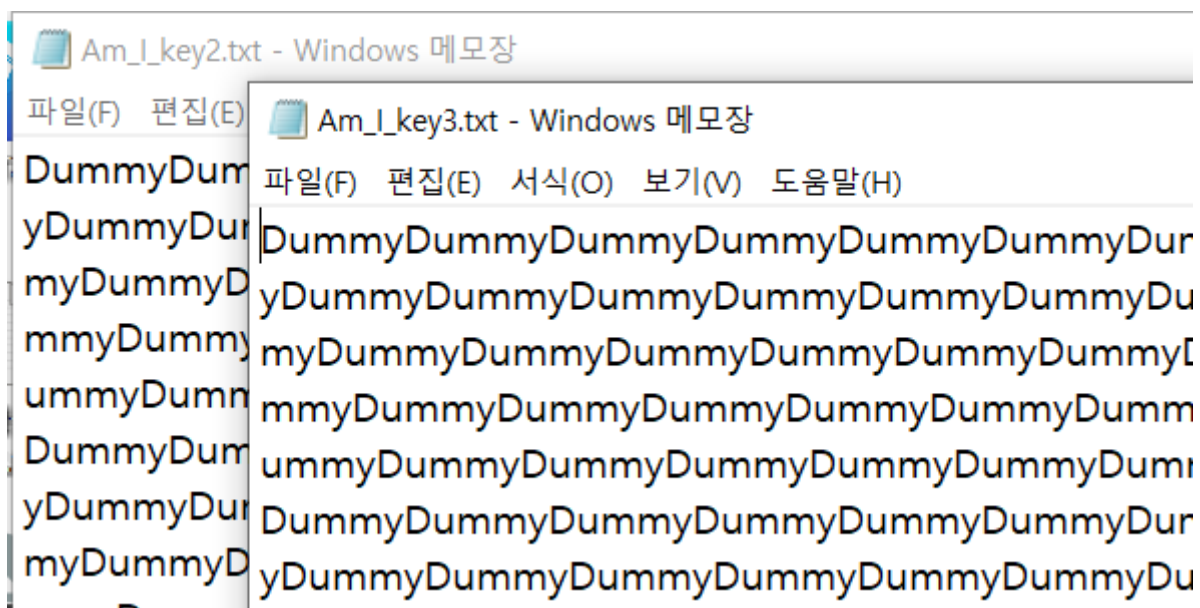
모두 09 08 으로 암호화와 관련된 bit 01부분이 1인 것을 알 수 있다.

따라서 암호화를 해제하기 위해 09 08을 08 08으로 바꿔주어 bit 01부분을 0으로 바꿔주었다.



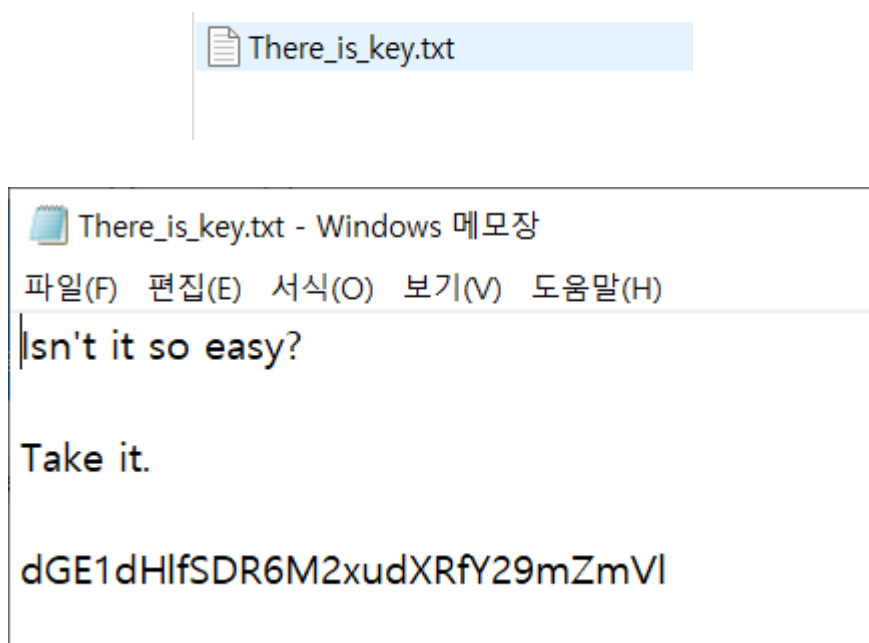
Am_I_key.zip
Am_I_key2.txt
Am_I_key3.txt

이처럼 암호가 풀리게 되었고



Am I key2,3 텍스트 파일은 그냥 dummy가 들어 있었다.

Am_I_key1을 열어보면



이렇게 값이 들어있고 해당 값을 base64 디코딩 해준 값을 넣어 문제를 풀 수 있다.

I N P U T A U T H K E Y

SUBMIT

suninatas.com 내용:

Congratulation, You have solved Challenge 28!

확인