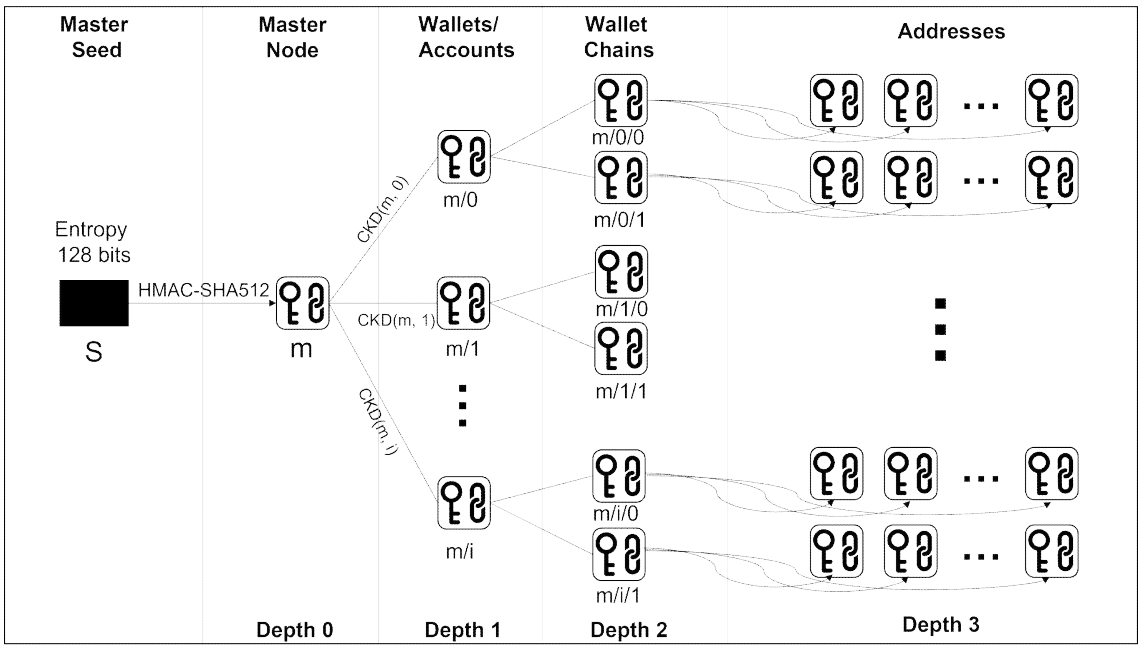
2022 암호분석경진대회

4번 문제

암호지갑은 암호화폐에서 사용되는 개인키/공개키쌍을 생성 및 저장하여, 사용자로 하여금 암호화폐 거래를 편리하게 해주는 수단이다. 암호지갑의 개인키/공개키쌍은 키 유도 기법들 중 하나인 Hierarchical Deterministic Key Derivation을 통해 생성된다. 이는 아래 그림과 같이 특정 Seed로부터 다수의 키쌍을 생성하는 방식으로 동작한다(Hierarchical Deterministic Wallet의 개념 및 개인키/공개키쌍 과정은 BIP-0032 문서 참고).

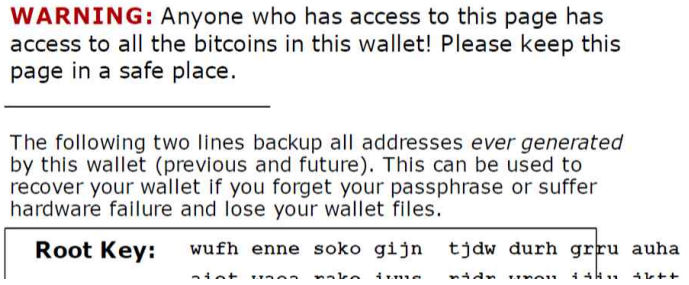


<Hierarchical Deterministic Key Derivation 기법>

Seed(위 그림상의 S)는 BIP-0039에 따라 단어사전(Wordlist) 중 무작위로 선택한 Mnemonic Code와 Salt, 사용자 패스워드를 입력받아 PBKDF2를 통해 생성한다. 여기서 Mnemonic Code를 결정하기 위한 초기 엔트로피(Initial entropy)는 난수성이 충분한 난수이다(Seed 생성 방법은 BIP-0039 문서 참고). 이후 HMAC-SHA512를 이용해 마스터 개인키/공개키쌍, 하위 공개키/개인키쌍을 생성한다.

1	abandon	2038	wrong
2	ability	2039	yard
3	able	2040	year
4	about	2041	yellow
5	above	2042	you
6	absent	2043	young
7	absorb	2044	youth
8	abstract	2045	zebra
9	absurd	2046	zero
10	abuse	2047	zone
11	access	2048	zoo

<Mnemonic 코드 사전 예시>



<니모닉 코드 예시(Armory 암호지갑 Mnemonic 코드 백업 문서)>

위에서 설명한 Hierarchical Deterministic Key Derivation은 Seed가 알려지면 모든 키가 알려지므로 사용자는 Mnemonic 코드가 유출되지 않도록 주의해야 한다. 또한 Mnemonic Code가 선택되는 단어사전에 포함된 단어의 개수가 충분히 크지 않다면 안전하지 않다.

[문제]

암호지갑에 포함된 정보가 <wallet>과 같이 주어지고 Mnemonic Code 단어사전이 <wordlist>와 같이 주어졌을 때, 이를 활용하여 <wallet>에 포함된 공개키에 상응하는 개인키 값을 구하여 (개인키 값, 풀이과정 및 구현 소스코드)를 제출하시오. (단, Seed 생성 과정에서 사용되는 초기 엔트로피는 128 bits이며, wordlist 중 선택된 Mnemonic Code는 중복되어 사용되지 않았다고 가정함)


```
{
“xPubKey”:\xpub661MyMwAqRbcFwkbijMsskkrPEja9rZQAvGavNLGpthpwzbPyBDjCFUiLHVQXED2YM9pUAC7zz62ShWRPRdwbyyWEQ5CK1yP5vPWrmGCg7D“\”
"xPrivKey":null,“
”xPrivKeyEncrypted":"{
    \"IV\":\"TGOpwxj3UiffLawxlO8P0Q==\",
    \"V\":1,
    \"Key Derivation Iteration\":1000,
    \"Key Length\":128,
    \"Tag Size\":64,
    \"Adata\":\"\",
    \"Cipher\":\"AES-CCM\",
    \"Salt\":\"2B2CnAzrhrU=\",
    \"Cipher Text\":\"kN197TSnBiyqHv+Ul1ioNdvmNZV3zDSkane+qTrLKLoJaeTh2mUooYKYY+EgztWp6ichJfqUWCM0D9Yd72j4Ytj4wVLVRP+5VcUBqpnHli2gVIYlETocig92bNCzlZdb42jheXbRd+EvH5ZSanq3Sr3uQJN/eN0=\"}",
"mnemonic":null,
"mnemonicEncrypted":
    "{\"IV\":\"2k+eN8VqCnilue22ENpdfQ==\",
    \"V\":1,
    \"Key Derivation Iteration\":1000,
    \"Key Length\":128,
    \"Tag Size\":64,
    \"Adata\":\"\",
    \"Cipher\":\"AES-CCM\",
    \"Salt\":\"2B2CnAzrhrU=\",
    \"ct\":\"NjuugzjFTbX7Tj05w4FVpPnyP9lru7uFtPRPwkn1nQGprvFirzHSjLVCipWEJqUayFb/Ksm46yIWtbPCTF0viJUD4+lcBcSlpMpBuwxBc92yUaQ5aE8lX21s\"}",
"mnemonicHasPassphrase":false
}
```


<wallet>

0	abandon
224	bright
248	business
365	color
958	jelly
964	joy
1033	license
1114	mercy
1156	mountain
1798	this
1293	payment
1358	prefer
1401	quality
1354	power
2047	zoo

<wordlist>

[참고]

- BIP-0039 참고자료 : https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- BIP-0032 참고자료 : https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#Specification_Wallet_structure