BIP 0032 TestVectors

From Bitcoin

Test vector 1

```
Master (hex): 000102030405060708090a0b0c0d0e0f
* [Chain m]
  * Identifier
    * (hex):       3442193e1bb70916e914552172cd4e2dbc9df811
    * (fpr):       0x3442193e
    * (main addr): 15mKKb2eos1hWa6tisdPwwDC1a5J1y9nma
  * Secret key
    * (hex):       e8f32e723decf4051aefac8e2c93c9c5b214313817cdb01a1494b917c8436b35
    * (wif):       L52XzL2cMkHxqxBXRyEpnPQZGUs3uKiL3R11XbAdHigRzDozKZeW
  * Public key
    * (hex):       0339a36013301597daef41fbe593a02cc513d0b55527ec2df1050e2e8ff49c85c2
  * Chain code
    * (hex):       873dff81c02f525623fd1fe5167eac3a55a049de3d314bb42ee227ffed37d508
  * Serialized
    * (pub hex):   0488b21e000000000000000000873dff81c02f525623fd1fe5167eac3a55a049de3d314bb42ee22
    * (prv hex):   0488ade400000000000000000873dff81c02f525623fd1fe5167eac3a55a049de3d314bb42ee22
    * (pub b58):   xpub661MyMwAqRbcFtXgS5sYJABqqG9YLmC4Q1Rdap9gSE8NqtwybGhePY2gZ29ESFjqJoCu1Rupje8
    * (prv b58):   xprv9s21ZrQH143K3QTDL4LXw2F7HEK3wJUD2nW2nRk4stbPy6cq3jPPqjiChkVvvNKmPGJxWUtg6Lr
* [Chain m/0']
  * Identifier
    * (hex):       5c1bd648ed23aa5fd50ba52b2457c11e9e80a6a7
    * (fpr):       0x5c1bd648
    * (main addr): 19Q2WoS5hSS6T8GjhK8KZLMgmWaq4neXrh
  * Secret key
    * (hex):       edb2e14f9ee77d26dd93b4ecede8d16ed408ce149b6cd80b0715a2d911a0afea
    * (wif):       L5BmPijJjrKbiUfG4zbiFKNqkvuJ8usooJmzuD7Z8dkRoTThYnAT
  * Public key
    * (hex):       035a784662a4a20a65bf6aab9ae98a6c068a81c52e4b032c0fb5400c706cfccc56
  * Chain code
    * (hex):       47fdacbd0f1097043b78c63c20c34ef4ed9a111d980047ad16282c7ae6236141
  * Serialized
    * (pub hex):   0488b21e013442193e8000000047fdacbd0f1097043b78c63c20c34ef4ed9a111d980047ad16282
    * (prv hex):   0488ade4013442193e8000000047fdacbd0f1097043b78c63c20c34ef4ed9a111d980047ad16282
    * (pub b58):   xpub68Gmy5EdvgibQVfPdqkBBCHxA5htiqg55crXYuXoQRKfDBFA1WEjWgP6LHhwBZeNK1VTsfTFUHC
    * (prv b58):   xprv9uHRZZhk6KAJC1avXpDAp4MDc3sQKNxDiPvvkX8Br5ngLNv1TxvUxt4cV1rGL5hj6KCesnDYUhd
* [Chain m/0'/1]
  * Identifier
    * (hex):       bef5a2f9a56a94aab12459f72ad9cf8cf19c7bbe
    * (fpr):       0xbef5a2f9
    * (main addr): 1JQheacLPdM5ySCkrZkV66G2ApAXe1mqLj
  * Secret key
    * (hex):       3c6cb8d0f6a264c91ea8b5030fadaa8e538b020f0a387421a12de9319dc93368
    * (wif):       KyFAjQ5rgrKvhXvNMtFB5PCSKUYD1yyPEe3xr3T34TZSUHycXtMM
  * Public key
    * (hex):       03501e454bf00751f24b1b489aa925215d66af2234e3891c3b21a52bedb3cd711c
  * Chain code
    * (hex):       2a7857631386ba23dacac34180dd1983734e444fdbf774041578e9b6adb37c19
  * Serialized
    * (pub hex):   0488b21e025c1bd648000000012a7857631386ba23dacac34180dd1983734e444fdbf774041578e
    * (prv hex):   0488ade4025c1bd648000000012a7857631386ba23dacac34180dd1983734e444fdbf774041578e
    * (pub b58):   xpub6ASuArnXKPbfEwhqN6e3mwBcDTgzisQN1wXN9BJcM47sSikHjJf3UFHKkNAWbWMiGj7Wf5uMash
    * (prv b58):   xprv9wTYmMFdV23N2TdNG573QoEsfRrWKQgWeibmLntzniatZvR9BmLnvSxqu53Kw1UmYPxLgboyZQa
* [Chain m/0'/1/2']
  * Identifier
    * (hex):       ee7ab90cde56a8c0e2bb086ac49748b8db9dce72
    * (fpr):       0xee7ab90c
    * (main addr): 1NjxqbA9aZWnh17q1UW3rB4EPu79wDXj7x
  * Secret key
```

```
    * (hex):       cbce0d719ecf7431d88e6a89fa1483e02e35092af60c042b1df2ff59fa424dca
    * (wif):       L43t3od1Gh7Lj55Bzjj1xDAgJDcL7YFo2nEcNaMGiyRZS1CidBVU
  * Public key
    * (hex):       0357bfe1e341d01c69fe5654309956cbea516822fba8a601743a012a7896ee8dc2
  * Chain code
    * (hex):       04466b9cc8e161e966409ca52986c584f07e9dc81f735db683c3ff6ec7b1503f
  * Serialized
    * (pub hex):   0488b21e03bef5a2f98000000204466b9cc8e161e966409ca52986c584f07e9dc81f735db683c3f
    * (prv hex):   0488ade403bef5a2f98000000204466b9cc8e161e966409ca52986c584f07e9dc81f735db683c3f
    * (pub b58):   xpub6D4BDPcP2GT577Vvch3R8wDkScZWzQzMMUm3PWbmWvVJrZwQY4VUNgqFJPMM3No2dFDFGTsxpG
    * (prv b58):   xprv9z4pot5VBttmtdRTWfWQmoH1taj2axGVzFqSb8C9xaxKymcFzXBDptWmT7FwuEzG3ryjH4ktypQ
* [Chain m/0'/1/2'/2]
  * Identifier
    * (hex):       d880d7d893848509a62d8fb74e32148dac68412f
    * (fpr):       0xd880d7d8
    * (main addr): 1LjmJcdPnDHhNTUgrWyhLGnRDKxQjoxAgt
  * Secret key
    * (hex):       0f479245fb19a38a1954c5c7c0ebab2f9bdfd96a17563ef28a6a4b1a2a764ef4
    * (wif):       KwjQsVuMjbCP2Zmr3VaFaStav7NvevwjvvkqrWd5Qmh1XVnCteBR
  * Public key
    * (hex):       02e8445082a72f29b75ca48748a914df60622a609cacfce8ed0e35804560741d29
  * Chain code
    * (hex):       cfb71883f01676f587d023cc53a35bc7f88f724b1f8c2892ac1275ac822a3edd
  * Serialized
    * (pub hex):   0488b21e04ee7ab90c00000002cfb71883f01676f587d023cc53a35bc7f88f724b1f8c2892ac127
    * (prv hex):   0488ade404ee7ab90c00000002cfb71883f01676f587d023cc53a35bc7f88f724b1f8c2892ac127
    * (pub b58):   xpub6FHa3pjLCk84BayeJxFW2SP4XRrFd1JYnxeLeU8EqN3vDfZmbqBqaGJAyiLjTAwm6ZLRQUMv1ZA
    * (prv b58):   xprvA2JDeKCSNNZky6uBCviVfJSKyQ1mDYahRjijr5idH2WwLsEd4Hsb2Tyh8RfQMuPh7f7RtyzTtdr
* [Chain m/0'/1/2'/2/1000000000]
  * Identifier
    * (hex):       d69aa102255fed74378278c7812701ea641fdf32
    * (fpr):       0xd69aa102
    * (main addr): 1LZiqrop2HGR4qrH1ULZPyBpU6AUP49Uam
  * Secret key
    * (hex):       471b76e389e528d6de6d816857e012c5455051cad6660850e58372a6c3e6e7c8
    * (wif):       Kybw8izYevo5xMh1TK7aUr7jHFCxXS1zv8p3oqFz3o2zFbhRXHYs
  * Public key
    * (hex):       022a471424da5e657499d1ff51cb43c47481a03b1e77f951fe64cec9f5a48f7011
  * Chain code
    * (hex):       c783e67b921d2beb8f6b389cc646d7263b4145701dadd2161548a8b078e65e9e
  * Serialized
    * (pub hex):   0488b21e05d880d7d83b9aca00c783e67b921d2beb8f6b389cc646d7263b4145701dadd2161548a
    * (prv hex):   0488ade405d880d7d83b9aca00c783e67b921d2beb8f6b389cc646d7263b4145701dadd2161548a
    * (pub b58):   xpub6H1LXWLaKsWFhvm6RVpEL9P4KfRZSW7abD2ttkWP3SSQvnyA8FSVqNTEcYFgJS2UaFcxupHiYkr
    * (prv b58):   xprvA41z7zogVVwxVSgdKUHDy1SKmdb533PjDz7J6N6mV6uS3ze1ai8FHa8kmHScGpWmj4WggLyQjgF
```

Test vector 2

```
Master (hex): fffcf9f6f3f0edeae7e4e1dedbd8d5d2cfccc9c6c3c0bdbab7b4b1aeaba8a5a29f9c999693908d8a8784
* [Chain m]
  * Identifier
    * (hex):       bd16bee53961a47d6ad888e29545434a89bdfe95
    * (fpr):       0xbd16bee5
    * (main addr): 1JEoxevbLLG8cVqeoGKQiAwoWbNYSUyYjg
  * Secret key
    * (hex):       4b03d6fc340455b363f51020ad3ecca4f0850280cf436c70c727923f6db46c3e
    * (wif):       KyjXhyHF9wTphBkfpxjL8hkDXDUSbE3tKANT94kXSyh6vn6nKaoy
  * Public key
    * (hex):       03cbcaa9c98c877a26977d00825c956a238e8dddfbd322cce4f74b0b5bd6ace4a7
  * Chain code
    * (hex):       60499f801b896d83179a4374aeb7822aaeaceaa0db1f85ee3e904c4defbd9689
  * Serialized
    * (pub hex):   0488b21e000000000000000000060499f801b896d83179a4374aeb7822aaeaceaa0db1f85ee3e904
    * (prv hex):   0488ade400000000000000000060499f801b896d83179a4374aeb7822aaeaceaa0db1f85ee3e904
    * (pub b58):   xpub661MyMwAqRbcFW31YEwpkMuc5THy2PSt5bDMsktWQcFF8syAmRUapSCGu8ED9W6oDMSgv6Zz8id
    * (prv b58):   xprv9s21ZrQH143K31xYSDQpPDxsXRTUcvj2iNHm5NUtrGiGG5e2DtALGdso3pGz6ssrdK4PFmM8NSp
```

```
* [Chain m/0]
  * Identifier
    * (hex):       5a61ff8eb7aaca3010db97ebda76121610b78096
    * (fpr):       0x5a61ff8e
    * (main addr): 19EuDJdgfRkwCmRzbzVBHZWQG9QNWhftbZ
  * Secret key
    * (hex):       abe74a98f6c7eabee0428f53798f0ab8aa1bd37873999041703c742f15ac7e1e
    * (wif):       L2ysLrR6KMSAtx7uPqmYpoTeiRzydXBattRXjXz5GDFPrdfPzKbj
  * Public key
    * (hex):       02fc9e5af0ac8d9b3cecfe2a888e2117ba3d089d8585886c9c826b6b22a98d12ea
  * Chain code
    * (hex):       f0909affaa7ee7abe5dd4e100598d4dc53cd709d5a5c2cac40e7412f232f7c9c
  * Serialized
    * (pub hex):   0488b21e01bd16bee500000000f0909affaa7ee7abe5dd4e100598d4dc53cd709d5a5c2cac40e74
    * (prv hex):   0488ade401bd16bee500000000f0909affaa7ee7abe5dd4e100598d4dc53cd709d5a5c2cac40e74
    * (pub b58):   xpub69H7F5d8KSRgmmdJg2KhpAK8SR3DjMwAdkxj3ZuxV27CprR9LgpeyGmXUbC6wb7ERfvrnKZjXoU
    * (prv b58):   xprv9vHkqa6EV4sPZHYqZznhT2NPtPCjKuDKGY38FBWLvgaDx45zo9WQRUT3dKYnjwih2yJD9mkrocE
* [Chain m/0/2147483647']
  * Identifier
    * (hex):       d8ab493736da02f11ed682f88339e720fb0379d1
    * (fpr):       0xd8ab4937
    * (main addr): 1Lke9bXGhn5VPrBuXgN12uGUphrttUErmk
  * Secret key
    * (hex):       877c779ad9687164e9c2f4f0f4ff0340814392330693ce95a58fe18fd52e6e93
    * (wif):       L1m5VpbXmMp57P3knskwhoMTLdhAAaXiHvnGLMribbfwzVRpz2Sr
  * Public key
    * (hex):       03c01e7425647bdefa82b12d9bad5e3e6865bee0502694b94ca58b666abc0a5c3b
  * Chain code
    * (hex):       be17a268474a6bb9c61e1d720cf6215e2a88c5406c4aee7b38547f585c9a37d9
  * Serialized
    * (pub hex):   0488b21e025a61ff8effffffffbe17a268474a6bb9c61e1d720cf6215e2a88c5406c4aee7b38547
    * (prv hex):   0488ade4025a61ff8effffffffbe17a268474a6bb9c61e1d720cf6215e2a88c5406c4aee7b38547
    * (pub b58):   xpub6ASAVgeehLbnwdqV6UKMHVzgqAG8Gr6riv3Fxxpj8ksbH9ebxaEyBLZ85ySDhKiLDBrQSARLq1uN
    * (prv b58):   xprv9wSp6B7kry3Vj9m1zSnLvN3xH8RdsPP1Mh7fAaR7aRLcQMKTR2vidYEeEg2mUCTAwCd6vnxVrcj
* [Chain m/0/2147483647'/1]
  * Identifier
    * (hex):       78412e3a2296a40de124307b6485bd19833e2e34
    * (fpr):       0x78412e3a
    * (main addr): 1BxrAr2pHpeBheusmd6fHDP2tSLAUa3qsW
  * Secret key
    * (hex):       704addf544a06e5ee4bea37098463c23613da32020d604506da8c0518e1da4b7
    * (wif):       KzyzXnznxSv249b4KuNkBwowaN3akiNeEHy5FWoPCJpStZbEKXN2
  * Public key
    * (hex):       03a7d1d856deb74c508e05031f9895dab54626251b3806e16b4bd12e781a7df5b9
  * Chain code
    * (hex):       f366f48f1ea9f2d1d3fe958c95ca84ea18e4c4ddb9366c336c927eb246fb38cb
  * Serialized
    * (pub hex):   0488b21e03d8ab493700000001f366f48f1ea9f2d1d3fe958c95ca84ea18e4c4ddb9366c336c927
    * (prv hex):   0488ade403d8ab493700000001f366f48f1ea9f2d1d3fe958c95ca84ea18e4c4ddb9366c336c927
    * (pub b58):   xpub6DF8uhdarytz3FWdA8TvFSvvAh8dP3283MY7p2V4SeE2wyWmG5mg5EwVvmdMVCQcoNJxGoWaU9D
    * (prv b58):   xprv9zFnWC6h2cLgpmSA46vutJzBcfJ8yaJGg8cX1e5StJh45BBciYTRXSd25UEPVuesF9yog62tGAQ
* [Chain m/0/2147483647'/1/2147483646']
  * Identifier
    * (hex):       31a507b815593dfc51ffc7245ae7e5aee304246e
    * (fpr):       0x31a507b8
    * (main addr): 15XVotxCAV7sRx1PSCkQNsGw3W9jT9A94R
  * Secret key
    * (hex):       f1c7c871a54a804afe328b4c83a1c33b8e5ff48f5087273f04efa83b247d6a2d
    * (wif):       L5KhaMvPYRW1ZoFmRjUtxxPypQ94m6BcDrPhqArhggdaTbbAFJEF
  * Public key
    * (hex):       02d2b36900396c9282fa14628566582f206a5dd0bcc8d5e892611806cafb0301f0
  * Chain code
    * (hex):       637807030d55d01f9a0cb3a7839515d796bd07706386a6eddf06cc29a65a0e29
  * Serialized
    * (pub hex):   0488b21e0478412e3affffffe637807030d55d01f9a0cb3a7839515d796bd07706386a6eddf06c
    * (prv hex):   0488ade40478412e3affffffe637807030d55d01f9a0cb3a7839515d796bd07706386a6eddf06c
    * (pub b58):   xpub6ERApfZwUNrhLCkDtcHTcxd75RbzS1ed54G1LkBUHQVHQKqhMkhgbmJbZRkrgZw4koxb5JaHWkY
    * (prv b58):   xprvA1RpRA33e1JQ7ifknakTFpgNXPmW2YvmhqLQYMmrj4xJXXWYpDPS3xz7iAxn8L39njGVyuoseXz
* [Chain m/0/2147483647'/1/2147483646'/2]
  * Identifier
```

```
    * (hex):       26132fdbe7bf89cbc64cf8dafa3f9f88b8666220
    * (fpr):       0x26132fdb
    * (main addr): 14UKfRV9ZPUp6ZC9PLhqbRtxdihW9em3xt
  * Secret key
    * (hex):       bb7d39bdb83ecf58f2fd82b6d918341cbef428661ef01ab97c28a4842125ac23
    * (wif):       L3WAYNAZPxx1fr7KCz7GN9nD5qMBnNiqEJNJMU1z9MMaannAt4aK
  * Public key
    * (hex):       024d902e1a2fc7a8755ab5b694c575fce742c48d9ff192e63df5193e4c7afe1f9c
  * Chain code
    * (hex):       9452b549be8cea3ecb7a84bec10dcfd94afe4d129ebfd3b3cb58eedf394ed271
  * Serialized
    * (pub hex):   0488b21e0531a507b8000000029452b549be8cea3ecb7a84bec10dcfd94afe4d129ebfd3b3cb58e
    * (prv hex):   0488ade40531a507b8000000029452b549be8cea3ecb7a84bec10dcfd94afe4d129ebfd3b3cb58e
    * (pub b58):   xpub6FnCn6nSzZAw5Tw7cgR9bi15UV96gLZhjDstkXXxvCLsUXBGXPdSnLFbdpq8p9HmGsApME5hQTZ
    * (prv b58):   xprvA2nrNbFZABcdryreWet9Ea4LvTJcGsqrMzxHx98MMrotbir7yrKCEXw7nadnHM8Dq38EGfSh6dc
```

Retrieved from "https://en.bitcoin.it/w/index.php?title=BIP_0032_TestVectors&oldid=38095"
