Mnemonic code for generating *deterministic keys*

Marek Palatinus · Pavol Rusnak · Aaron Voisine · Sean Bowe

slush@satoshilabs.com · stick@satoshilabs.com · voisine@gmail.com · ewillbefull@gmail.com

39

Abstract

This BIP describes the implementation of a mnemonic code or mnemonic sentence -- a group of easy to remember words -- for the generation of deterministic wallets.

It consists of two parts: generating the mnemonic and converting it into a binary seed. This seed can be later used to generate deterministic wallets using BIP-0032 or similar methods.

Copyright

This BIP falls under the MIT License.

Motivation

A mnemonic code or sentence is superior for human interaction compared to the handling of raw binary or hexadecimal representations of a wallet seed. The sentence could be written on paper or spoken over the telephone.

This guide is meant to be a way to transport computer-generated randomness with a human-readable transcription. It's not a way to process user-created sentences (also known as brainwallets) into a wallet seed.

Generating the mnemonic

The mnemonic must encode entropy in a multiple of 32 bits. With more entropy security is improved but the sentence length increases. We refer to the initial entropy length as ENT. The allowed size of ENT is 128-256 bits.

First, an initial entropy of ENT bits is generated. A checksum is generated by taking the first `ENT / 32` bits of its SHA256 hash. This checksum is appended to the end of the initial entropy. Next, these concatenated bits are split into groups of 11 bits, each encoding a number from 0-2047, serving as an index into a wordlist. Finally, we convert these numbers into words and use the joined words as a mnemonic sentence.

The following table describes the relation between the initial entropy length (ENT), the checksum length (CS), and the length of the generated mnemonic sentence (MS) in words.

```
CS = ENT / 32
MS = (ENT + CS) / 11

|  ENT  | CS | ENT+CS |  MS  |
+-------+----+--------+------+
|  128  |  4 |   132  |  12  |
|  160  |  5 |   165  |  15  |
|  192  |  6 |   198  |  18  |
|  224  |  7 |   231  |  21  |
|  256  |  8 |   264  |  24  |
```

Wordlist

An ideal wordlist has the following characteristics:

a) smart selection of words

- the wordlist is created in such a way that it's enough to type the first four letters to unambiguously identify the word

b) similar words avoided

- word pairs like "build" and "built", "woman" and "women", or "quick" and "quickly" not only make remembering the sentence difficult but are also more error prone and more difficult to guess

c) sorted wordlists

- the wordlist is sorted which allows for more efficient lookup of the code words (i.e. implementations can use binary search instead of linear search)
- this also allows trie (a prefix tree) to be used, e.g. for better compression

The wordlist can contain native characters, but they must be encoded in UTF-8 using Normalization Form Compatibility Decomposition (NFKD).

From mnemonic to seed

A user may decide to protect their mnemonic with a passphrase. If a passphrase is not present, an empty string "" is used instead.

To create a binary seed from the mnemonic, we use the PBKDF2 function with a mnemonic sentence (in UTF-8 NFKD) used as the password and the string "mnemonic" + passphrase (again in UTF-8 NFKD) used as the salt. The iteration count is set to 2048 and HMAC-SHA512 is used as the pseudo-random function. The length of the derived key is 512 bits (= 64 bytes).

This seed can be later used to generate deterministic wallets using BIP-0032 or similar methods.

The conversion of the mnemonic sentence to a binary seed is completely independent from generating the sentence. This results in a rather simple code; there are no constraints on sentence structure and clients are free to implement their own wordlists or even whole sentence generators, allowing for flexibility in wordlists for typo detection or other purposes.

Although using a mnemonic not generated by the algorithm described in "Generating the mnemonic" section is possible, this is not advised and software must compute a checksum for the mnemonic sentence using a wordlist and issue a warning if it is invalid.

The described method also provides plausible deniability, because every passphrase generates a valid seed (and thus a deterministic wallet) but only the correct one will make the desired wallet available.

Wordlists

Since the vast majority of BIP39 wallets supports only the English wordlist, it is **strongly discouraged** to use non-English wordlists for generating the mnemonic sentences.

If you still feel your application really needs to use a localized wordlist, use one of the following instead of inventing your own.

- Wordlists

Test vectors

The test vectors include input entropy, mnemonic and seed. The passphrase "TREZOR" is used for all vectors.

`https://github.com/trezor/python-mnemonic/blob/master/vectors.json`

Also see `https://github.com/bip32JP/bip32JP.github.io/blob/master/test_JP_BIP39.json`

(Japanese wordlist test with heavily normalized symbols as passphrase)

Shortcomings

Some shortcomings have been identified with this proposal:

- Generated seed depends on the wordlist that was used for the mnemonic. Because the "mnemonic to seed" process uses the mnemonic sentence directly rather than the original entropy, translating the mnemonic to a different wordlist necessarily creates a completely different seed. This is not an issue if you only support the English wordlist, as recommended above.
- Because the seed is generated by hashing the mnemonic, it is not possible to represent an arbitrary BIP-0032 seed via a BIP-0039 sentence: the conversion is one-way only (from BIP-0039 sentence to BIP-0032 seed).
- The checksum is short. This means it only gives modest odds of catching random errors (1-in-256 errors will be missed). It is also not able to provide any assistance in correcting errors.
- No versioning scheme. When originally introduced, there was no way to distinguish the address format that should be used for a BIP-0039 key. This is now largely mitigated by use of descriptor wallets (BIP-0380) in addition to a seed however.

Related Work

The authors of BIP-0039 proposed the SLIP-0039 scheme as an intended successor to BIP-0039 improving on the above shortcomings.

Reference Implementation

Reference implementation including wordlists is available from

`http://github.com/trezor/python-mnemonic`

`bip-0039/english.txt`

```
abandon  antique  because  buffalo  chest  cousin  deputy  early  excuse  flight  glare  hole  isolate  lesson  medal  neither  own  pony  range  roof  sheriff  sorry  sun  tobacco  unfair  want
ability  anxiety  become  build  chicken  cover  derive  earn  execute  flip  glass  holiday  issue  letter  media  nephew  owner  pool  rapid  rookie  shield  sort  sunny  today  unfold  warfare
able  any  beef  bulb  chief  coyote  describe  earth  exercise  float  glide  hollow  item  level  melody  nerve  oxygen  popular  rare  room  shift  soul  sunset  toddler  unhappy  warm
about  apart  before  bulk  child  crack  desert  easily  exhaust  flock  glimpse  home  ivory  liar  melt  nest  oyster  portion  rate  rose  shine  sound  super  toe  uniform  warrior
above  apology  begin  bullet  chimney  cradle  design  east  exhibit  floor  globe  honey  jacket  liberty  member  net  ozone  position  rather  rotate  ship  soup  supply  together  unique  wash
absent  appear  behave  bundle  choice  craft  desk  easy  exile  flower  gloom  hood  jaguar  library  memory  network  pact  possible  raven  rough  shiver  source  supreme  toilet  unit  wasp
absorb  apple  behind  bunker  choose  cram  despair  echo  exist  fluid  glory  hope  jar  license  mention  neutral  paddle  post  raw  round  shock  south  sure  token  universe  waste
abstract  approve  believe  burden  chronic  crane  destroy  ecology  exit  flush  glove  horn  jazz  life  menu  never  page  potato  razor  route  shoe  space  surface  tomato  unknown  water
absurd  april  below  burger  chuckle  crash  detail  economy  exotic  fly  glow  horror  jealous  lift  mercy  news  pair  pottery  ready  royal  shoot  spare  surge  tomorrow  unlock  wave
abuse  arch  belt  burst  chunk  crater  detect  edge  expand  foam  glue  horse  jeans  light  merge  next  palace  poverty  real  rubber  shop  spatial  surprise  tone  until  way
access  arctic  bench  bus  churn  crawl  develop  edit  expect  focus  goat  hospital  jelly  like  merit  nice  palm  powder  reason  rude  short  spawn  surround  tongue  unusual  wealth
accident  area  benefit  business  cigar  crazy  device  educate  expire  fog  goddess  host  jewel  limb  merry  night  panda  power  rebel  rug  shoulder  speak  survey  tonight  unveil  weapon
account  arena  best  busy  cinnamon  cream  devote  effort  explain  foil  gold  hotel  job  limit  mesh  noble  panel  practice  rebuild  rule  shove  special  suspect  tool  update  wear
accuse  argue  betray  butter  circle  credit  diagram  egg  expose  fold  good  hour  join  link  message  noise  panic  praise  recall  run  shrimp  speed  sustain  tooth  upgrade  weasel
achieve  arm  better  buyer  citizen  creek  dial  eight  express  follow  goose  hover  joke  lion  metal  nominee  panther  predict  receive  runway  shrug  spell  swallow  top  uphold  weather
acid  armed  between  buzz  city  crew  diamond  either  extend  food  gorilla  hub  journey  liquid  method  noodle  paper  prefer  recipe  rural  shuffle  spend  swamp  topic  upon  web
acoustic  armor  beyond  cabbage  civil  cricket  diary  elbow  extra  foot  gospel  huge  joy  list  middle  normal  parade  prepare  record  sad  shy  sphere  swap  topple  upper  wedding
acquire  army  bicycle  cabin  claim  crime  dice  elder  eye  force  gossip  human  judge  little  midnight  north  parent  present  recycle  saddle  sibling  spice  swarm  torch  upset  weekend
across  around  bid  cable  clap  crisp  diesel  electric  eyebrow  forest  govern  humble  juice  live  milk  nose  park  pretty  reduce  sadness  sick  spider  swear  tornado  urban  weird
act  arrange  bike  cactus  clarify  critic  diet  elegant  fabric  forget  gown  humor  jump  lizard  million  notable  parrot  prevent  reflect  safe  side  spike  sweet  tortoise  urge  welcome
action  arrest  bind  cage  claw  crop  differ  element  face  fork  grab  hundred  jungle  load  mimic  note  party  price  reform  sail  siege  spin  swift  toss  usage  west
actor  arrive  biology  cake  clay  cross  digital  elephant  faculty  fortune  grace  hungry  junior  loan  mind  nothing  pass  pride  refuse  salad  sight  spirit  swim  total  use  wet
actress  arrow  bird  call  clean  crouch  dignity  elevator  fade  forum  grain  hunt  junk  lobster  minimum  notice  patch  primary  region  salmon  sign  split  swing  tourist  used  whale
actual  art  birth  calm  clerk  crowd  dilemma  elite  faint  forward  grant  hurdle  just  local  minor  novel  path  print  regret  salon  silent  spoil  switch  toward  useful  what
adapt  artefact  bitter  camera  clever  crucial  dinner  else  faith  fossil  grape  hurry  kangaroo  lock  minute  now  patient  priority  regular  salt  silk  sponsor  sword  tower  useless  wheat
add  artist  black  camp  click  cruel  dinosaur  embark  fall  foster  grass  hurt  keen  logic  miracle  nuclear  patrol  prison  reject  salute  silly  spoon  symbol  town  usual  wheel
addict  artwork  blade  can  client  cruise  direct  embody  false  found  gravity  husband  keep  lonely  mirror  number  pattern  private  relax  same  silver  sport  symptom  toy  utility  when
address  ask  blame  canal  cliff  crumble  dirt  embrace  fame  fox  great  hybrid  ketchup  long  misery  nurse  pause  prize  release  sample  similar  spot  syrup  track  vacant  where
adjust  aspect  blanket  cancel  climb  crunch  disagree  emerge  family  fragile  green  ice  key  loop  miss  nut  pave  problem  relief  sand  simple  spray  system  trade  vacuum  whip
admit  assault  blast  candy  clinic  crush  discover  emotion  famous  frame  grid  icon  kick  lottery  mistake  oak  payment  process  rely  satisfy  since  spread  table  traffic  vague  whisper
adult  asset  bleak  cannon  clip  cry  disease  employ  fan  frequent  grief  idea  kid  loud  mix  obey  peace  produce  remain  satoshi  sing  spring  tackle  tragic  valid  wide
advance  assist  bless  canoe  clock  crystal  dish  empower  fancy  fresh  grit  identify  kidney  lounge  mixed  object  peanut  profit  remember  sauce  siren  spy  tag  train  valley  width
advice  assume  blind  canvas  clog  cube  dismiss  empty  fantasy  friend  grocery  idle  kind  love  mixture  oblige  pear  program  remind  sausage  sister  square  tail  transfer  valve  wife
aerobic  asthma  blood  canyon  close  culture  disorder  enable  farm  fringe  group  ignore  kingdom  loyal  mobile  obscure  peasant  project  remove  save  situate  squeeze  talent  trap  van  wild
affair  athlete  blossom  capable  cloth  cup  display  enact  fashion  frog  grow  ill  kiss  lucky  model  observe  pelican  promote  render  say  six  squirrel  talk  trash  vanish  will
afford  atom  blouse  capital  cloud  cupboard  distance  end  fat  front  grunt  illegal  kit  luggage  modify  obtain  pen  proof  renew  scale  size  stable  tank  travel  vapor  win
afraid  attack  blue  captain  clown  curious  divert  endless  fatal  frost  guard  illness  kitchen  lumber  mom  obvious  penalty  property  rent  scan  skate  stadium  tape  tray  various  window
again  attend  blur  car  club  current  divide  endorse  father  frown  guess  image  kite  lunar  moment  occur  pencil  prosper  reopen  scare  sketch  staff  target  treat  vast  wine
age  attitude  blush  carbon  clump  curtain  divorce  enemy  fatigue  frozen  guide  imitate  kitten  lunch  monitor  ocean  people  protect  repair  scatter  ski  stage  task  tree  vault  wing
agent  attract  board  card  cluster  curve  dizzy  energy  fault  fruit  guilt  immense  kiwi  luxury  monkey  october  pepper  proud  repeat  scene  skill  stairs  taste  trend  vehicle  wink
agree  auction  boat  cargo  clutch  cushion  doctor  enforce  favorite  fuel  guitar  immune  knee  lyrics  monster  odor  perfect  provide  replace  scheme  skin  stamp  tattoo  trial  velvet  winner
ahead  audit  body  carpet  coach  custom  document  engage  feature  fun  gun  impact  knife  machine  month  off  permit  public  report  school  skirt  stand  taxi  tribe  vendor  winter
aim  august  boil  carry  coast  cute  dog  engine  february  funny  gym  impose  knock  mad  moon  offer  person  pudding  require  science  skull  start  teach  trick  venture  wire
air  aunt  bomb  cart  coconut  cycle  doll  enhance  federal  furnace  habit  improve  know  magic  moral  office  pet  pull  rescue  scissors  slab  state  team  trigger  venue  wisdom
airport  author  bone  case  code  dad  dolphin  enjoy  fee  fury  hair  impulse  lab  magnet  more  often  phone  pulp  resemble  scorpion  slam  stay  tell  trim  verb  wise
aisle  auto  bonus  cash  coffee  damage  domain  enlist  feed  future  half  inch  label  maid  morning  oil  photo  pulse  resist  scout  sleep  steak  ten  trip  verify  wish
alarm  autumn  book  casino  coil  damp  donate  enough  feel  gadget  hammer  include  labor  mail  mosquito  okay  phrase  pumpkin  resource  scrap  slender  steel  tenant  trophy  version  witness
album  average  boost  castle  coin  dance  donkey  enrich  female  gain  hamster  income  ladder  main  mother  old  physical  punch  response  screen  slice  stem  tennis  trouble  very  wolf
alcohol  avocado  border  casual  collect  danger  donor  enroll  fence  galaxy  hand  increase  lady  major  motion  olive  piano  pupil  result  script  slide  step  tent  truck  vessel  woman
alert  avoid  boring  cat  color  daring  door  ensure  festival  gallery  happy  index  lake  make  motor  olympic  picnic  puppy  retire  scrub  slight  stereo  term  true  veteran  wonder
alien  awake  borrow  catalog  column  dash  dose  enter  fetch  game  harbor  indicate  lamp  mammal  mountain  omit  picture  purchase  retreat  sea  slim  stick  test  truly  viable  wood
all  aware  boss  catch  combine  daughter  double  entire  fever  gap  hard  indoor  language  man  mouse  once  piece  purity  return  search  slogan  still  text  trumpet  vibrant  wool
alley  away  bottom  category  come  dawn  dove  entry  few  garage  harsh  industry  laptop  manage  move  one  pig  purpose  reunion  season  slot  sting  thank  trust  vicious  word
allow  awesome  bounce  cattle  comfort  day  draft  envelope  fiber  garbage  harvest  infant  large  mandate  movie  onion  pigeon  purse  reveal  seat  slow  stock  that  truth  victory  work
almost  awful  box  caught  comic  deal  dragon  episode  fiction  garden  hat  inflict  later  mango  much  online  pill  push  review  second  slush  stomach  theme  try  video  world
alone  awkward  boy  cause  common  debate  drama  equal  field  garlic  have  inform  latin  mansion  muffin  only  pilot  put  reward  secret  small  stone  then  tube  view  worry
alpha  axis  bracket  caution  company  debris  drastic  equip  figure  garment  hawk  inhale  laugh  manual  mule  open  pink  puzzle  rhythm  section  smart  stool  theory  tuition  village  worth
already  baby  brain  cave  concert  decade  draw  era  file  gas  hazard  inherit  laundry  maple  multiply  opera  pioneer  pyramid  rib  security  smile  story  there  tumble  vintage  wrap
also  bachelor  brand  ceiling  conduct  december  dream  erase  film  gasp  head  initial  lava  marble  muscle  opinion  pipe  quality  ribbon  seed  smoke  stove  they  tuna  violin  wreck
alter  bacon  brass  celery  confirm  decide  dress  erode  filter  gate  health  inject  law  march  museum  oppose  pistol  quantum  rice  seek  smooth  strategy  thing  tunnel  virtual  wrestle
always  badge  brave  cement  congress  decline  drift  erosion  final  gather  heart  injury  lawn  margin  mushroom  option  pitch  quarter  rich  segment  snack  street  this  turkey  virus  wrist
amateur  bag  bread  census  connect  decorate  drill  error  find  gauge  heavy  inmate  lawsuit  marine  music  orange  pizza  question  ride  select  snake  strike  thought  turn  visa  write
amazing  balance  breeze  century  consider  decrease  drink  erupt  fine  gaze  hedgehog  inner  layer  market  must  orbit  place  quick  ridge  sell  snap  strong  three  turtle  visit  wrong
among  balcony  brick  cereal  control  deer  drip  escape  finger  general  height  innocent  lazy  marriage  mutual  orchard  planet  quit  rifle  seminar  sniff  struggle  thrive  twelve  visual  yard
amount  ball  bridge  certain  convince  defense  drive  essay  finish  genius  hello  input  leader  mask  myself  order  plastic  quiz  right  senior  snow  student  throw  twenty  vital  year
amused  bamboo  brief  chair  cook  define  drop  essence  fire  genre  helmet  inquiry  leaf  mass  mystery  ordinary  plate  quote  rigid  sense  soap  stuff  thumb  twice  vivid  yellow
analyst  banana  bright  chalk  cool  defy  drum  estate  firm  gentle  help  insane  learn  master  myth  organ  play  rabbit  ring  sentence  soccer  stumble  thunder  twin  vocal  you
anchor  banner  bring  champion  copper  degree  dry  eternal  first  genuine  hen  insect  leave  match  naive  orient  please  raccoon  riot  series  social  style  ticket  twist  voice  young
ancient  bar  brisk  change  copy  delay  duck  ethics  fiscal  gesture  hero  inside  lecture  material  name  original  pledge  race  ripple  service  sock  subject  tide  two  void  youth
anger  barely  broccoli  chaos  coral  deliver  dumb  evidence  fish  ghost  hidden  inspire  left  math  napkin  orphan  pluck  rack  risk  session  soda  submit  tiger  type  volcano  zebra
angle  bargain  broken  chapter  core  demand  dune  evil  fit  giant  high  install  leg  matrix  narrow  ostrich  plug  radar  ritual  settle  soft  subway  tilt  typical  volume  zero
angry  barrel  bronze  charge  corn  demise  during  evoke  fitness  gift  hill  intact  legal  matter  nasty  other  plunge  radio  rival  setup  solar  success  timber  ugly  vote  zone
animal  base  broom  chase  correct  denial  dust  evolve  fix  giggle  hint  interest  legend  maximum  nation  outdoor  poem  rail  river  seven  soldier  such  time  umbrella  voyage  zoo
ankle  basic  brother  chat  cost  dentist  dutch  exact  flag  ginger  hip  into  leisure  maze  nature  outer  poet  rain  road  shadow  solid  sudden  tiny  unable  wage
announce  basket  brown  cheap  cotton  deny  duty  example  flame  giraffe  hire  invest  lemon  meadow  near  output  point  raise  roast  shaft  solution  suffer  tip  unaware  wagon
annual  battle  brush  check  couch  depart  dwarf  excess  flash  girl  history  invite  lend  mean  neck  outside  polar  rally  robot  shallow  solve  sugar  tired  uncle  wait
another  beach  bubble  cheese  country  depend  dynamic  exchange  flat  give  hobby  involve  length  measure  need  oval  pole  ramp  robust  share  someone  suggest  tissue  uncover  walk
answer  bean  buddy  chef  couple  deposit  eager  excite  flavor  glad  hockey  iron  lens  meat  negative  oven  police  ranch  rocket  shed  song  suit  title  under  wall
antenna  beauty  budget  cherry  course  depth  eagle  exclude  flee  glance  hold  island  leopard  mechanic  neglect  over  pond  random  romance  shell  soon  summer  toast  undo  walnut
```

MIT License. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.