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

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.