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

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.