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

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.