MONEROMASTER.COM

Table of Contents

Page 1. Instructions

Page 2. Encrypt Mnemonic Seed (Steps 1-3)

Page 3. Decrypt Mnemonic Seed (Step 4)

You Will Need:

Printer, pencil, scissors, eraser (optional), ruler (optional)

Instructions

Step 1. Locate Your Mnemonic Seed

Your Monero Mnemonic Seed is a phrase with 13, 14, or 25 random words generated when you first created your non-custodial wallet.

Locate this (or create a new wallet) and write out the words on a sheet of paper.

TIP: Write out a new copy of your Mnemonic Seed with a pencil and then destroy this temporary copy once this encryption process is complete.

Step 2. Choose A Keyword

Your keyword is a password that will be used to encrypt and decipher your Mnemonic Seed using the Vigenère Polyalphabetic Cipher.

To create a strong, yet memorable keyword, abbreviate a famous quote using an acronym. For example, a quote from the Shakespearean play, Macbeth:

"O, full of scorpions is my mind, dear wife! Thou know'st that Banquo and his Fleance lives."

This could be rendered:

OFOSIMMDWTKTBAHFL

TIP: For an added layer of security, you could reposition the order of your Mnemonic Seed. This way even if your plaintext was deciphered, the order of the random words will still need to be known to access your Monero.

Step 3. Encrypt Your Mnemonic Seed

Using the Vigenère table, align the first letter of your keyword to the top x-axis and the first letter of your Mnemonic seed to the left-most y-axis. The intersection is your encrypted letter.

TIP: For added security, you could run a second pass of encryption over your encrypted text with a new keyword. This means you would need to decipher your cyphertext twice to reveal your seed plaintext.

On the bottom left is room to list your restore height which would speed up the synchronization time should you restore your wallet on a new device.

Finally, cut out your cipher text and store it securely. Destroy the leftover "Encrypt Mnemonic Seed" sheet.

TIP: Before destroying your leftover "Encrypt Mnemonic Seed" sheet, first decipher your encrypted text to ensure you made no errors in your encryption.

Step 4. Decrypt Your Mnemonic Seed

To decrypt your seed, simply write out your keyword repeatedly above your cyphertext and use the Vigenère table to once again uncover its meaning.

Find your cyphertext in the y-axis of your keyword, then move along the x-axis to reveal the seed letter.



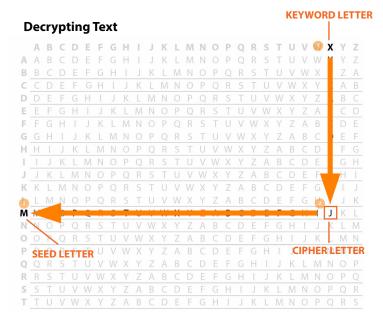
MONERO MASTER

Example

Keyword: XMRXMRXMRXMR ... Mnemonic Seed: Monero ... Ciphertext: JAEBDF ...

		Keyword XMR			
X M R X M R			nonic Seed		
1. MONERO	2	_ 3	_ 4	_ 5	6
7	8	9	10	_ 11	12
13	14	15	16	17	18
19	20	21	22	23	24
		25			
		Cip	hertext		
1. JAEBDF	2	3	4	_ 5	6

Encrypting Text A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A





Encrypt Mnemonic Seed

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A A B C D E F G H I J K L M N O P Q R S T U V W X Y Z $\textbf{B} \;\; \textbf{B} \;\; \textbf{C} \;\; \textbf{D} \;\; \textbf{E} \;\; \textbf{F} \;\; \textbf{G} \;\; \textbf{H} \;\; \textbf{I} \;\; \textbf{J} \;\; \textbf{K} \;\; \textbf{L} \;\; \textbf{M} \;\; \textbf{N} \;\; \textbf{O} \;\; \textbf{P} \;\; \textbf{Q} \;\; \textbf{R} \;\; \textbf{S} \;\; \textbf{T} \;\; \textbf{U} \;\; \textbf{V} \;\; \textbf{W} \;\; \textbf{X} \;\; \textbf{Y} \;\; \textbf{Z} \;\; \textbf{A}$ $\textbf{C} \ \ \mathsf{C} \ \ \mathsf{D} \ \ \mathsf{E} \ \ \mathsf{F} \ \ \mathsf{G} \ \ \mathsf{H} \ \ \mathsf{I} \ \ \mathsf{J} \ \ \mathsf{K} \ \ \mathsf{L} \ \ \mathsf{M} \ \ \mathsf{N} \ \ \mathsf{O} \ \ \mathsf{P} \ \ \mathsf{Q} \ \ \mathsf{R} \ \ \mathsf{S} \ \ \mathsf{T} \ \ \mathsf{U} \ \ \mathsf{V} \ \ \mathsf{W} \ \ \mathsf{X} \ \ \mathsf{Y} \ \ \mathsf{Z} \ \ \mathsf{A} \ \ \mathsf{B}$ D D E F G H I J K L M N O P Q R S T U V W X Y Z A B C E E F G H I J K L M N O P Q R S T U V W X Y Z A B C D F F G H I J K L M N O P Q R S T U V W X Y Z A B C D E GGHIJKLMNOPQRSTUVWXYZABCDEF HHIJKLMNOPQRSTUVWXYZABCDEFG I I J K L M N O P Q R S T U V W X Y Z A B C D E F G H J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I KKLMNOPQRSTUVWXYZABCDEFGHIJ L L M N O P Q R S T U V W X Y Z A B C D E F G H I J K M M N O P Q R S T U V W X Y Z A B C D E F G H I J K L N N O P Q R S T U V W X Y Z A B C D E F G H I J K L M O O P Q R S T U V W X Y Z A B C D E F G H I J K L M N $\textbf{P} \hspace{0.1cm} \textbf{P} \hspace{0.1cm} \textbf{Q} \hspace{0.1cm} \textbf{R} \hspace{0.1cm} \textbf{S} \hspace{0.1cm} \textbf{T} \hspace{0.1cm} \textbf{U} \hspace{0.1cm} \textbf{V} \hspace{0.1cm} \textbf{W} \hspace{0.1cm} \textbf{X} \hspace{0.1cm} \textbf{Y} \hspace{0.1cm} \textbf{Z} \hspace{0.1cm} \textbf{A} \hspace{0.1cm} \textbf{B} \hspace{0.1cm} \textbf{C} \hspace{0.1cm} \textbf{D} \hspace{0.1cm} \textbf{E} \hspace{0.1cm} \textbf{F} \hspace{0.1cm} \textbf{G} \hspace{0.1cm} \textbf{H} \hspace{0.1cm} \textbf{I} \hspace{0.1cm} \textbf{J} \hspace{0.1cm} \textbf{K} \hspace{0.1cm} \textbf{L} \hspace{0.1cm} \textbf{M} \hspace{0.1cm} \textbf{N} \hspace{0.1cm} \textbf{O} \hspace{0.1cm}$ Q Q R S T U V W X Y Z A B C D E F G H I J K L M N O P R S T U V W X Y Z A B C D E F G H I J K L M N O P Q S T U V W X Y Z A B C D E F G H I J K L M N O P Q R T T U V W X Y Z A B C D E F G H I J K L M N O P Q R U U V W X Y Z A B C D E F G H I J K L M N O P Q R S T V V W X Y Z A B C D E F G H I J K L M N O P Q R S T U WWXYZABCDEFGHIJKLMNOPQRSTUV X X Y Z A B C D E F G H I J K L M N O P Q R S T U V W Z A B C D E F G H I J K L M N O P Q R S T U V W X Z Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Keyword

Mnemonic Seed

1	2	3	4	5	6	
7	8	9	10	11	12	
13	14	15	16	17	18	
19	20	21	22	23	24	
		2	5			
			Ciphertext			
	_			_		
1	2	3	4,	5	6	
7	8	9	10	11	12	
13	14	15	16	17	18	
19	20	21	22	23	24	
		2	5.			

Restore Height: ____



Decrypt Mnemonic Seed

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A A B C D E F G H I J K L M N O P Q R S T U V W X Y Z BBCDEFGHIJKLMNOPQRSTUVWXYZA $\textbf{C} \ \ \mathsf{C} \ \ \mathsf{D} \ \ \mathsf{E} \ \ \mathsf{F} \ \ \mathsf{G} \ \ \mathsf{H} \ \ \mathsf{I} \ \ \mathsf{J} \ \ \mathsf{K} \ \ \mathsf{L} \ \ \mathsf{M} \ \ \mathsf{N} \ \ \mathsf{O} \ \ \mathsf{P} \ \ \mathsf{Q} \ \ \mathsf{R} \ \ \mathsf{S} \ \ \mathsf{T} \ \ \mathsf{U} \ \ \mathsf{V} \ \ \mathsf{W} \ \ \mathsf{X} \ \ \mathsf{Y} \ \ \mathsf{Z} \ \ \mathsf{A} \ \ \mathsf{B}$ D D E F G H I J K L M N O P Q R S T U V W X Y Z A B C E E F G H I J K L M N O P Q R S T U V W X Y Z A B C D F F G H I J K L M N O P Q R S T U V W X Y Z A B C D E GGHIJKLMNOPQRSTUVWXYZABCDEF H H I J K L M N O P Q R S T U V W X Y Z A B C D E F G I I J K L M N O P Q R S T U V W X Y Z A B C D E F G H J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I K K L M N O P Q R S T U V W X Y Z A B C D E F G H I J L L M N O P Q R S T U V W X Y Z A B C D E F G H I J K M M N O P Q R S T U V W X Y Z A B C D E F G H I J K L $oldsymbol{\mathsf{N}}$ $oldsymbol{\mathsf{N}}$ $oldsymbol{\mathsf{O}}$ $oldsymbol{\mathsf{P}}$ $oldsymbol{\mathsf{Q}}$ $oldsymbol{\mathsf{R}}$ $oldsymbol{\mathsf{S}}$ $oldsymbol{\mathsf{T}}$ $oldsymbol{\mathsf{U}}$ $oldsymbol{\mathsf{V}}$ $oldsymbol{\mathsf{W}}$ $oldsymbol{\mathsf{X}}$ $oldsymbol{\mathsf{Y}}$ $oldsymbol{\mathsf{Z}}$ $oldsymbol{\mathsf{A}}$ $oldsymbol{\mathsf{B}}$ $oldsymbol{\mathsf{C}}$ $oldsymbol{\mathsf{D}}$ $oldsymbol{\mathsf{E}}$ $oldsymbol{\mathsf{F}}$ $oldsymbol{\mathsf{G}}$ $oldsymbol{\mathsf{H}}$ $oldsymbol{\mathsf{I}}$ $oldsymbol{\mathsf{N}}$ $oldsymbol{\mathsf{Q}}$ $oldsymbol{\mathsf{N}}$ $oldsymbol{\mathsf{N}}$ $oldsymbol{\mathsf{Q}}$ $oldsymbol{\mathsf{N}}$ $oldsymbol{\mathsf{N}}$ oldsymbolO O P Q R S T U V W X Y Z A B C D E F G H I J K L M N $\textbf{P} \hspace{0.1cm} \textbf{P} \hspace{0.1cm} \textbf{Q} \hspace{0.1cm} \textbf{R} \hspace{0.1cm} \textbf{S} \hspace{0.1cm} \textbf{T} \hspace{0.1cm} \textbf{U} \hspace{0.1cm} \textbf{V} \hspace{0.1cm} \textbf{W} \hspace{0.1cm} \textbf{X} \hspace{0.1cm} \textbf{Y} \hspace{0.1cm} \textbf{Z} \hspace{0.1cm} \textbf{A} \hspace{0.1cm} \textbf{B} \hspace{0.1cm} \textbf{C} \hspace{0.1cm} \textbf{D} \hspace{0.1cm} \textbf{E} \hspace{0.1cm} \textbf{F} \hspace{0.1cm} \textbf{G} \hspace{0.1cm} \textbf{H} \hspace{0.1cm} \textbf{I} \hspace{0.1cm} \textbf{J} \hspace{0.1cm} \textbf{K} \hspace{0.1cm} \textbf{L} \hspace{0.1cm} \textbf{M} \hspace{0.1cm} \textbf{N} \hspace{0.1cm} \textbf{O} \hspace{0.1cm}$ Q Q R S T U V W X Y Z A B C D E F G H I J K L M N O P STUVWXYZABCDEFGHIJKLMNOPQ S T U V W X Y Z A B C D E F G H I J K L M N O P Q R T T U V W X Y Z A B C D E F G H I J K L M N O P Q R U U V W X Y Z A B C D E F G H I J K L M N O P Q R S T $oldsymbol{V}$ $oldsymbol{V}$ $oldsymbol{W}$ $oldsymbol{X}$ $oldsymbol{Y}$ $oldsymbol{Z}$ $oldsymbol{A}$ $oldsymbol{B}$ $oldsymbol{C}$ $oldsymbol{D}$ $oldsymbol{E}$ $oldsymbol{F}$ $oldsymbol{G}$ $oldsymbol{H}$ $oldsymbol{I}$ $oldsymbol{A}$ $oldsymbol{G}$ $oldsymbol{W}$ $oldsymbol{X}$ $oldsymbol{Y}$ $oldsymbol{Z}$ $oldsymbol{A}$ $oldsymbol{B}$ $oldsymbol{G}$ $oldsymbol{G}$ $oldsymbol{W}$ $oldsymbol{X}$ $oldsymbol{Y}$ $oldsymbol{Z}$ $oldsymbol{A}$ $oldsymbol{G}$ $oldsymbol{G$ WWXYZABCDEFGHIJKLMNOPQRSTUV YZABCDEFGHIJKLMNOPQRS Z A B C D E F G H I J K L M N O P Q R S T U V W X Z Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Keyword

Ciphertext

Place Cutout Ciphertext Here

`							
Mnemonic Seed							
1	2	3	4,	5	6		
7	8	9	10	11	12		
13	14	15	16	17	18		
19	20	21	22	23	24		