psst: paper-based secret sharing technique

You can use psst to split a secret into up to four parts.

Each part in isolation reveals nothing about the secret (except its length).

Any two parts combined allow the secret to be restored.

- 1) Get a safe and calm space, an hour of free time, a pen, a six-sided dice, scissors, and transparent adhesive tape.
- 2) Write the secret down here:

01	 02	03	04
05	 06	07	08
09	 10	11	12
13	 14	15	16
17	 18	19	20
21	22	23	24

3) Convert the secret to digits using one of the the text conversion tables printed on the secret share sheets. For bip-39 seeds, use the first five or more letters of each word. Pad shorter words with "q" to not reveal word lengths.

01	 02	03	04
05	 06	07	08
09	 10	11	12
13	 14	15	16
17	 18	19	20
21	 22	23	24

- 4) Split each digit into four shares. For each digit:
 - Locate the corresponding block in the table to the right.
 - Throw a six-sided dice to select a random row therein.
 - Write each of the four shares onto its sheet.
- 5) Test! Verify that you can reconstruct the secret using two of the sheets. Now is the last chance to correct mistakes.
- 6) Cut the sheets along the horizontal solid lines.
- 7) Fold the sheets into their final form, along dotted lines:
 - Fold the sides so that they cover the secret share.
 - Fold horizontally twice. Fold the secret below the center, then below the title. The title page is now the top layer. The secret is the middle layer, with 2 layers above/below.
 - Wrap the top flaps around the package.
- 8) Add a description, date, and signature. In the description, write what the secret represents and how it was converted into digits.
- 9) Cut the signature in thin stripes, along <u>light</u> solid <u>lines</u>.

 This makes it fragile; stripes break when the share is opened.
- 10) Fix the top flaps with adhesive tape. Attach carefully, so that removing the tape will tear the signature.

 Optionally add other tamper detection, like a seal or bag.
- 11) Destroy (eg, burn) this sheet and other copies of the secret.

```
Dice
0
    •
    ٠.
             2
    ·.
         2
0
0
    ::1
         3
             1
0
         4
             3
         re-throw
1
    \Box
    1
1
    ٠.
             3
             2
    ::
1
        re-throw
2
   ⊡
        0
            3
                1
2
   ·.
        1
             0
                      3
   \overline{\cdot}
             2
2
   ::
2
   ::
             1
         re-throw
3
   \overline{\phantom{a}}
        0
3
3
   \dot{}
3
             3 3
3
            0 1
3
    ::
         re-throw
    \overline{\phantom{a}}
         0
                      3
    ٠.
        1
             3
4
4
    ٠.
         2
             0 3 1
    ::
4
    ::
```

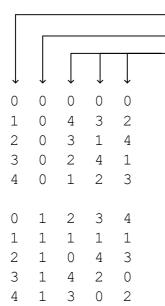
□ re-throw

Description:	

Share # 1 of: 2 [] 3 [] 4 []

psst: https://github.com/Sjlver/psst/

Date: ______



2 0 3

0 3 1 4 2

3 4 0

3 3 3

4 3 2

2 1

4 2 0 3

4 0 1 2

3

1

- Secret (first column)
- Share #1 (this share, second column)
- Shares #2, #3, #4 (remaining columns)

To recover the secret using two shares, process each digit individually.

Any two shares uniquely identify a row in the table to the left.

The secret is the concatenation of the digits labeled "Secret (first col)".

To recover the text form, combine two digits per letter and refer to one of the tables on the right.

Text (a-z) conversion:

(note x/j are
merged)

00=a	01 = b	02=c
03 = d	04 = e	
10=f	11=g	12=h
13=i	14=k	
20=1	21=m	22=n
23=0	24 = p	
30 = q	31=r	32=s
33=t	34 = u	
40=v	41=w	42=y
43 = z	44 = x/	j

0 2 4 1 3 1 2 3 4 0 **Secret share #1:** 2 2 2 2 2 2 01

23

01	02
03	04
05	06
07	08
09	10
11	12
13	14
15	16
17	18
19	20
21	22

24

Hex conversion:

00=0 01=1 02=2 03=3 10=4 11=5 12=6 13=7 20=8 21=9 22=a 23=b 30=c 31=d 32=e 33=f

ASCII conversion:

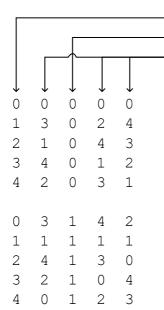
use 3 digits xyz res = 25x+5y+z+3

Description:		_
		_

Share # 2 of: 2 [] 3 [] 4 []

psst: https://github.com/Sjlver/psst/

Date:
Signature:



- Secret (first column)
- Share #2 (this share, third column)
- Shares #1, #3, #4 (remaining columns)

To recover the secret using two shares, process each digit individually. Any two shares uniquely identify a row in the table to the left.

The secret is the concatenation of the digits labeled "Secret (first col)".

To recover the text form, combine two digits per letter and refer to one of the tables on the right.

Text (a-z) conversion:

(note x/j are
merged)

03 = d	04=e	
10=f	11=g	12=h
13=i	14=k	
20=1	21=m	22 = n
23=0	24 = p	
30=q	31=r	32=s
33=t	34 = u	
40=v	41=w	42=y
43=7	44 = x /	i

00=a 01=b 02=c

1	4	2	0	3	
1 2 3 4	4 2 0 3	2 2 2 2	0 2	3 2 1	
3	0	2	4	1	
4	3	2	1	0	
0	4	3	2	1	
0 1 2 3 4	4 2 0 3	3 3 3 3	2 4		
2	0	3		0 4 3 2	
3	3	3	1 3	3	
4	1	3	0	2	
0	2	4	1	3	
1	0	4		2	
1 2 3	2 0 3 1	4 4 4	3 0 2	3 2 1 0	
3	1	4	2	0	

0 1 2 3 4

Secret share #2:

01	02	
03	04	
05	06	
07	08	
09	10	
11	12	
13	14	
15	16	
17	18	
19	20	
21	22	
23	24	

Hex conversion:

)2=2	03=3
L0 = 4	11=5
12=6	13=7
8=05	21=9
22=a	23=b
30=c	31 = d
32=e	33=f

00=0 01=1

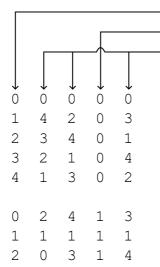
ASCII conversion:

use 3 digits xyz res = 25x+5y+z+3

Description:

Share # 3 of: 3 [] 4 []

psst: https://github.com/Sjlver/psst/



0 1

2.

- Secret (first column)
- Share #3 (this share, fourth column)
- Shares #1, #2, #4 (remaining columns)

To recover the secret using two shares, process each digit individually. Any two shares uniquely identify a row in the table to the left.

The secret is the concatenation of the digits labeled "Secret (first col)".

To recover the text form, combine two digits per letter and refer to one of the tables on the right.

Text (a-z) conversion:

(note x/j are
merged)

03=d 04=e 10=f 11=g 12=h 13=i 14=k 20=l 21=m 22=n 23=o 24=p 30=q 31=r 32=s 33=t 34=u 40=v 41=w 42=y 43=z 44=x/j

00=a 01=b 02=c

1 3 0 2 4 2 2 2 2 2 2 3 1 4 2 0 4 0 1 2 3

4

0	1	2	3	4
1	0	4	3	2
2	4	1	3	0
3	3	3	3	3
4	2	0	3	1

1	2	3	4	0
2	1	0	4	3
3	0	2	4	1

0 3 1 4 2

Secret share #3:

01	02	
03	04	
05	06	
07	08	
09	10	
11	12	
13	14	
15	16	
17	18	
19	20	
21	22	
23	24	

Hex conversion:

02=2 03=3 10=4 11=5 12=6 13=7 20=8 21=9 22=a 23=b 30=c 31=d 32=e 33=f

00=0 01=1

ASCII conversion:

use 3 digits xyz res = 25x+5y+z+3

Description:

Share # 4 of 4

psst: https://github.com/Sjlver/psst/

Text (a-z)

Date:

Signature:

(note x/j are
merged)

00=a 01=b 02=c 03=d 04=e 10=f 11=g 12=h 13=i 14=k 20=1 21=m 22=n 23=o 24=p 30=q 31=r 32=s

33=t 34=u 40=v 41=w 42=y

43=z $44=x/\dot{1}$

.....

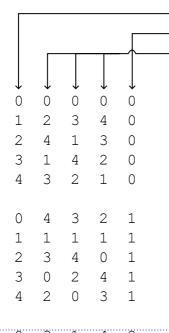
Hex conversion:

02=2 03=3 10=4 11=5 12=6 13=7 20=8 21=9 22=a 23=b 30=c 31=d 32=e 33=f

00=0 01=1

ASCII conversion:

use 3 digits xyz res = 25x+5y+z+3



4 3 2

2 2 2

4 1 3

3 3 3

2 3 4

3 1 4

1 0 4

4 0 1 2

3

1 4 2 0 3

1 3 0 2 4

1 0 4 3

1 2

1

2 2

3

1

3

0

1

2 0

3 2

0 2

- Secret (first column)
- Share #4 (this share, last column)
- Shares #1, #2, #3 (remaining columns)

To recover the secret using two shares, process each digit individually. Any two shares uniquely identify a row in the table to the left.

The secret is the concatenation of the digits labeled "Secret (first col)".

To recover the text form, combine two digits per letter and refer to one of the tables on the right.

Secret share #4:

01	02	
03	04	
05	06	
07	 08	
09	10	
11	 12	
13	 14	
15	 16	
17	18	
19	20	
21	22	
23	24	