

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 light solid lines.
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.

Secret	Dice	Share #1	Share #2	Share #3	Share #4
↓	↓	↓	↓	↓	↓
0	⚀	0	0	0	0
0	⚀	1	2	3	4
0	⚀	2	4	1	3
0	⚀	3	1	4	2
0	⚀	4	3	2	1
0	⚀	re-throw			
1	⚀	0	4	3	2
1	⚀	1	1	1	1
1	⚀	2	3	4	0
1	⚀	3	0	2	4
1	⚀	4	2	0	3
1	⚀	re-throw			
2	⚀	0	3	1	4
2	⚀	1	0	4	3
2	⚀	2	2	2	2
2	⚀	3	4	0	1
2	⚀	4	1	3	0
2	⚀	re-throw			
3	⚀	0	2	4	1
3	⚀	1	4	2	0
3	⚀	2	1	0	4
3	⚀	3	3	3	3
3	⚀	4	0	1	2
3	⚀	re-throw			
4	⚀	0	1	2	3
4	⚀	1	3	0	2
4	⚀	2	0	3	1
4	⚀	3	2	1	0
4	⚀	4	4	4	4
4	⚀	re-throw			

psst, this is a secret share

Description: _____

Date: _____

Signature: _____

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

psst: <https://github.com/Sjilver/psst/>

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

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=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	

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

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

Secret share #1:

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

psst, this is a secret share

Description: _____

Date: _____

Signature: _____

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

psst: <https://github.com/Sjilver/psst/>

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

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)

00=a	01=b	02=c
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	

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

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	_____

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

psst, this is a secret share

Description: _____

Date: _____

Signature: _____

Share # 3 of: 3 [] 4 []

psst: <https://github.com/Sjilver/psst/>

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

Secret (first column)
Share #3 (this share, second 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.

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

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	_____

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=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	

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

psst, this is a secret share

Description: _____

Date: _____

Signature: _____

Share # 4 of 4

psst: <https://github.com/Sjilver/psst/>

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

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.

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

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	_____

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=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

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