What is Secret Sharing?

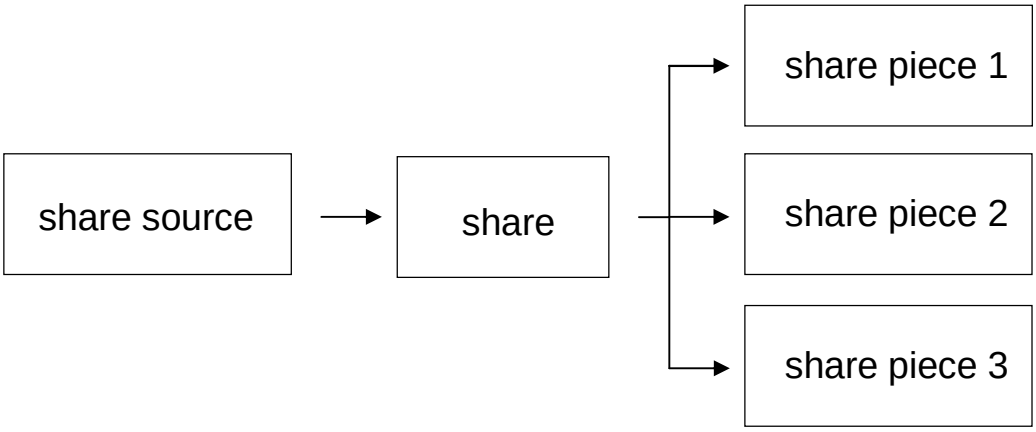
Secret sharing is like that:

Divide one file into several files.

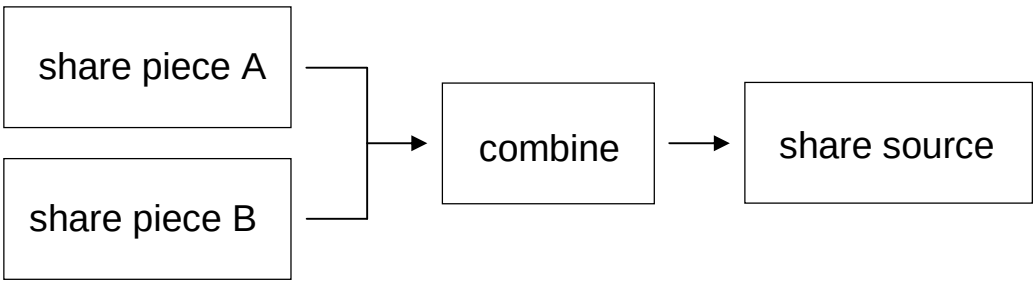
If you divide the divided file by the specified number, you can restore it to the original file.

For example, with (2, 3) 3 share 2 combine, it is as following:

share



combine



This will be something like that:

Divide one file into three files.

Arrange any two of the three files and apply "combine" to return to the original file.

For example, it might be something like

“Transfer the treasure map to a transparent sheet."

And

By overlaying transparent sheets for a specified number,
you can see the treasure map.

The mechanism is something like this.

In the case of the (2, 3) 3 share 2 combine above:

Transfer the treasure map onto three transparent sheets.

By overlaying any two of the three transparent sheets,
you can see the treasure map.

it is like this.

In this example, the share piece used for combining may be either 1, 2 or 3.

However, it is no good that "the same thing is two".

In that case, you can not combine.

It can not be joined unless it is a separate dispersion piece.

There is no such thing as the order, so in this case, it is to return in these three ways:

1, 2

1, 3

2, 3

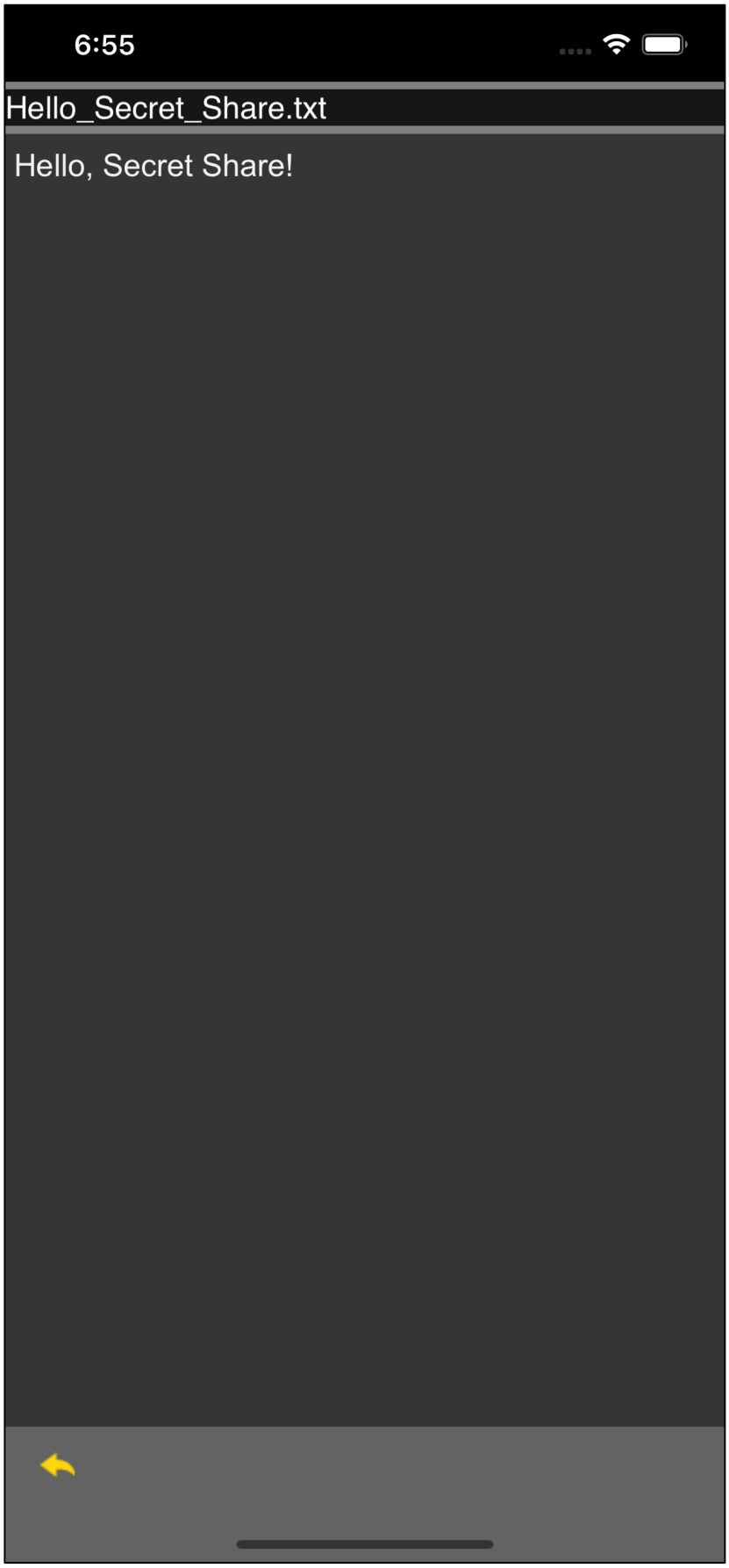
In general, cipher uses an encryption key (decryption key), but secret sharing does not use a key.

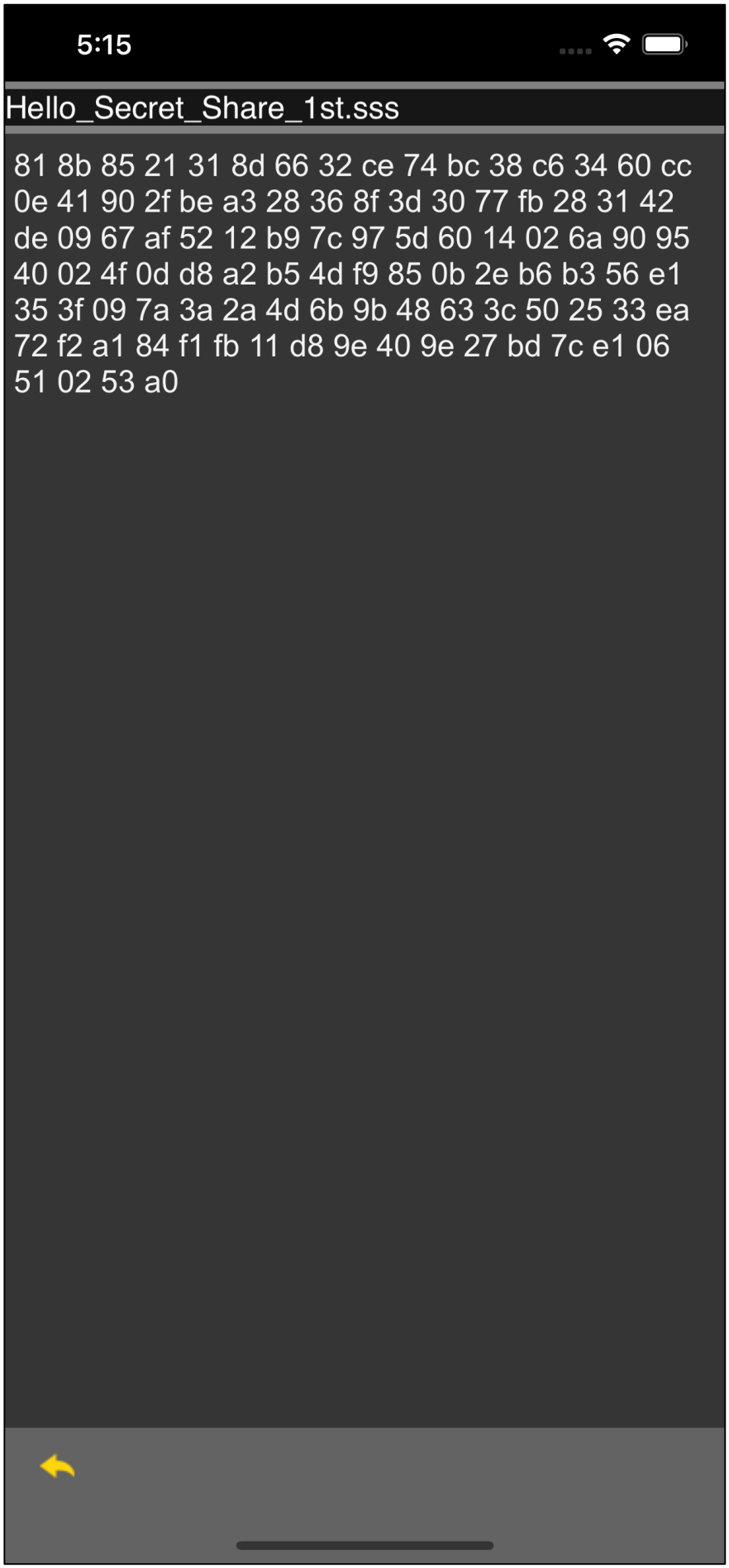
However, if you use secret sharing (software) which use secret sharing and cipher using a key together, in this case, a cipher key is used.

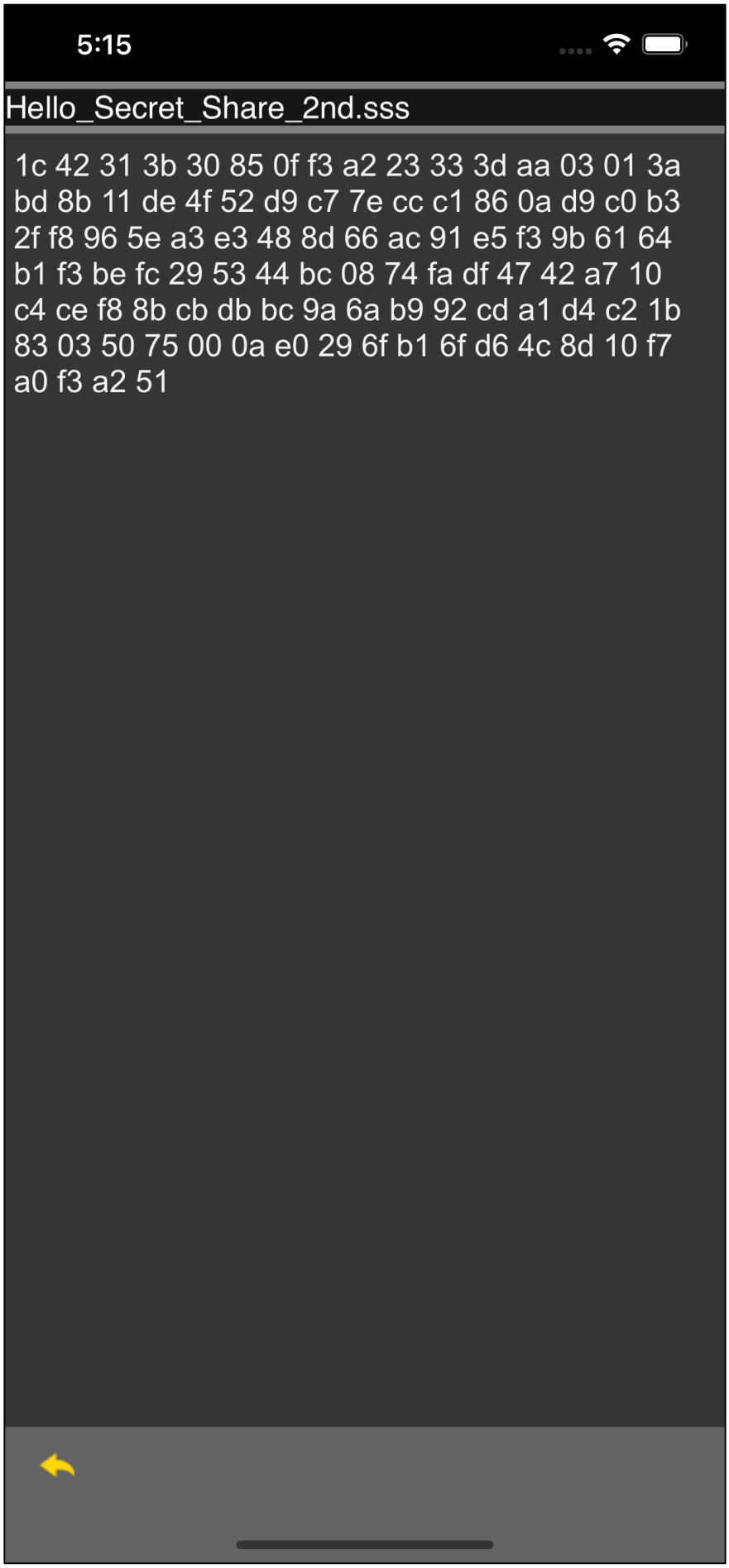
But, secret sharing itself does not use encryption keys (decryption keys) at all.

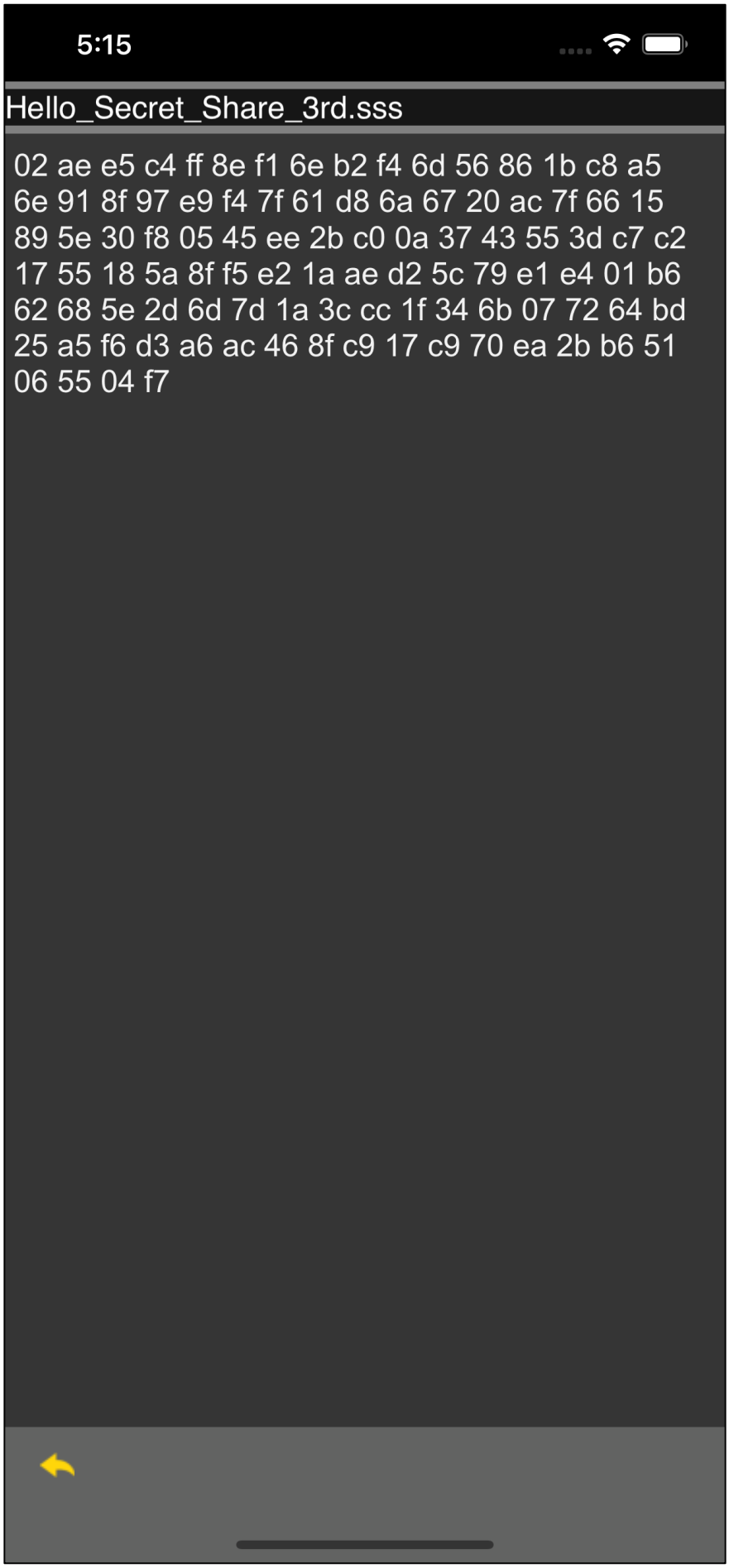
So to speak, the individual share pieces generated by sharing become like cipher text and decryption key.

The share by (2, 3) 3 share 2 combine is, for example, as follows.




5:15
Hello_Secret_Share_1st.sss
81 8b 85 21 31 8d 66 32 ce 74 bc 38 c6 34 60 cc
0e 41 90 2f be a3 28 36 8f 3d 30 77 fb 28 31 42
de 09 67 af 52 12 b9 7c 97 5d 60 14 02 6a 90 95
40 02 4f 0d d8 a2 b5 4d f9 85 0b 2e b6 b3 56 e1
35 3f 09 7a 3a 2a 4d 6b 9b 48 63 3c 50 25 33 ea
72 f2 a1 84 f1 fb 11 d8 9e 40 9e 27 bd 7c e1 06
51 02 53 a0


5:15
Hello_Secret_Share_2nd.sss
1c 42 31 3b 30 85 0f f3 a2 23 33 3d aa 03 01 3a
bd 8b 11 de 4f 52 d9 c7 7e cc c1 86 0a d9 c0 b3
2f f8 96 5e a3 e3 48 8d 66 ac 91 e5 f3 9b 61 64
b1 f3 be fc 29 53 44 bc 08 74 fa df 47 42 a7 10
c4 ce f8 8b cb db bc 9a 6a b9 92 cd a1 d4 c2 1b
83 03 50 75 00 0a e0 29 6f b1 6f d6 4c 8d 10 f7
a0 f3 a2 51


5:15
Hello_Secret_Share_3rd.sss
02 ae e5 c4 ff 8e f1 6e b2 f4 6d 56 86 1b c8 a5
6e 91 8f 97 e9 f4 7f 61 d8 6a 67 20 ac 7f 66 15
89 5e 30 f8 05 45 ee 2b c0 0a 37 43 55 3d c7 c2
17 55 18 5a 8f f5 e2 1a ae d2 5c 79 e1 e4 01 b6
62 68 5e 2d 6d 7d 1a 3c cc 1f 34 6b 07 72 64 bd
25 a5 f6 d3 a6 ac 46 8f c9 17 c9 70 ea 2b b6 51
06 55 04 f7

Hello_Secret_Share_1st.sss

Hello_Secret_Share_2nd.sss

Hello_Secret_Share_3rd.sss

it can not be restored unless one can arrange two of the three share pieces.

Each of the three share pieces only has some data of the source data.

The source data information can not be obtained by performing any operation on each share piece.

Shamia's secret sharing scheme is something like such things;

share … Make (Convert) data into simultaneous equations.

combine … Solve simultaneous equations and return to data.

Each share piece is like a series of coefficients of simultaneous equations.

combine

Arrange the number of simultaneous equations (share pieces) necessary to solve the simultaneous equations, and solve the simultaneous equations back to the original data.

Unless this is done, any information about the source data will not get .

Only you can arrange as many pieces of share as you need for combine.

Secret sharing conceals an information by this.

In ordinary cipher, it needs "You must remember the encryption key (password)."

On the other hand, on secret sharing, it needs remembering that

> “Which piece of share and which piece of share can be combined?”

And you have to manage each share piece not to lose it, not to break it.

This is, in a sense, more cumbersome than ordinary cipher.

However, if only you can arrange the necessary number of share pieces for combine, then no matter what operation is applied to the individual share pieces, the contents of the share source is never known.

This "robustness to analysis" is the main gain of using secret sharing.

> The number of share pieces required for combining can not be arranged by others.

As long as this is true, secret sharing is secure.