秘密分散とは、どういったものか？

秘密分散というのは、

1つのファイルを、いくつかのファイルに分割する。
その分割したファイルを規定数分、揃えると、元のファイルに戻せる。

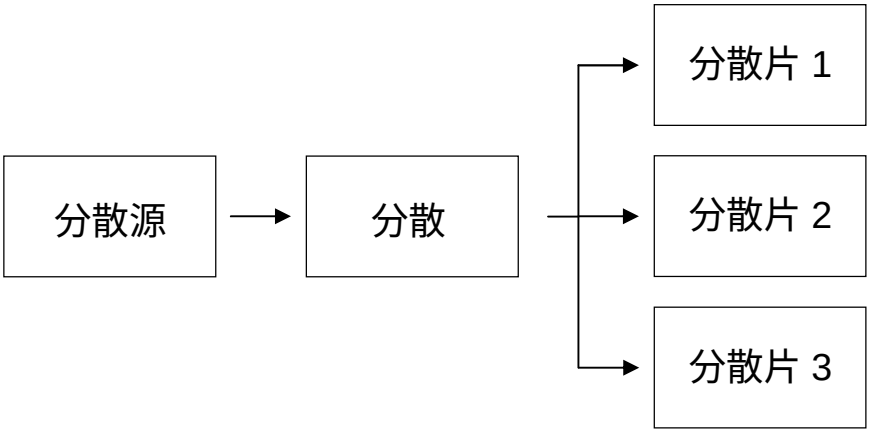
というものです。

たとえば、

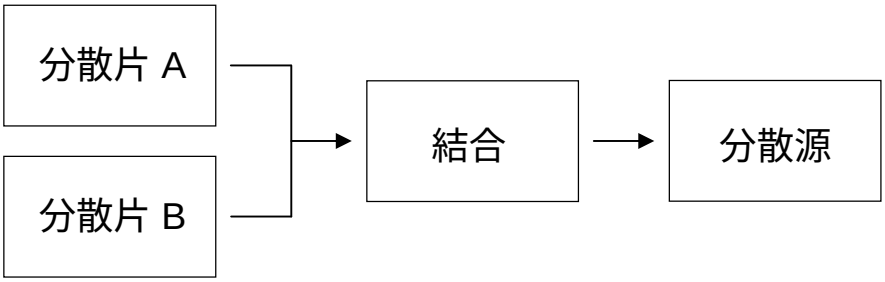
(2, 3) 3分割 2結合

では、

分散



結合



こういうことになります。

これは、

1つのファイルを、3つのファイルに分割する。
3つのファイルのうちの、任意の2つを揃えて、「結合」をかけると、元のファイルに戻る。

というものになります。

たとえて言うと、

宝の地図を、透明のシートに転写する。

というようなものかもしれません。
そして、

規定数分の、透明のシートを重ね合わせると、宝の地図を見ることできる。

というような仕掛けのものです。

上の、

(2, 3) 3分割 2結合

の場合では、

宝の地図を、3枚の透明のシートに転写する。

3枚の透明のシートのうちの、任意の2枚を重ね合わせると、
宝の地図を見ることができる。

というようなことです。

この例の場合、結合に使う分散片は、1、2、3 のうちのどれでも構いません。

ただ、「同じものが2つ」というのはだめです。その場合は、結合できません。
別々の分散片でないと、結合できません。

順序というようなものはありませんので、この場合

1, 2

1, 3

2, 3

の3通りで、戻るということになります。

一般に、暗号というものでは、暗号鍵(復号鍵)を使いますが、
秘密分散では、鍵は使いません。

ただ、

　　秘密分散 と 鍵を使うタイプの暗号 を併用している。

という、秘密分散(ソフトウェア)なら、使うことになります。

しかし、秘密分散自体は、暗号鍵(復号鍵)というものは、まったく使いません。

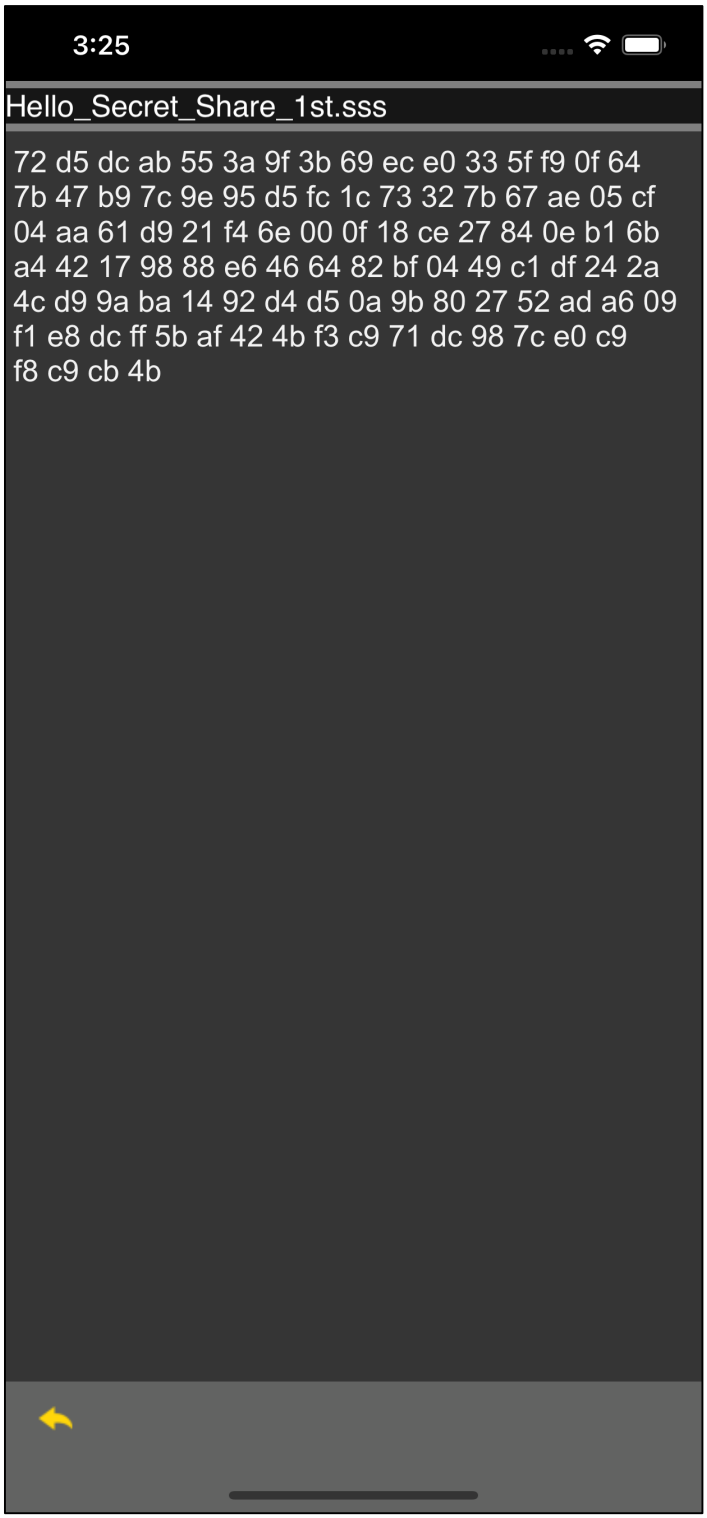
いわば、分散によって生成された、個々の分散片が

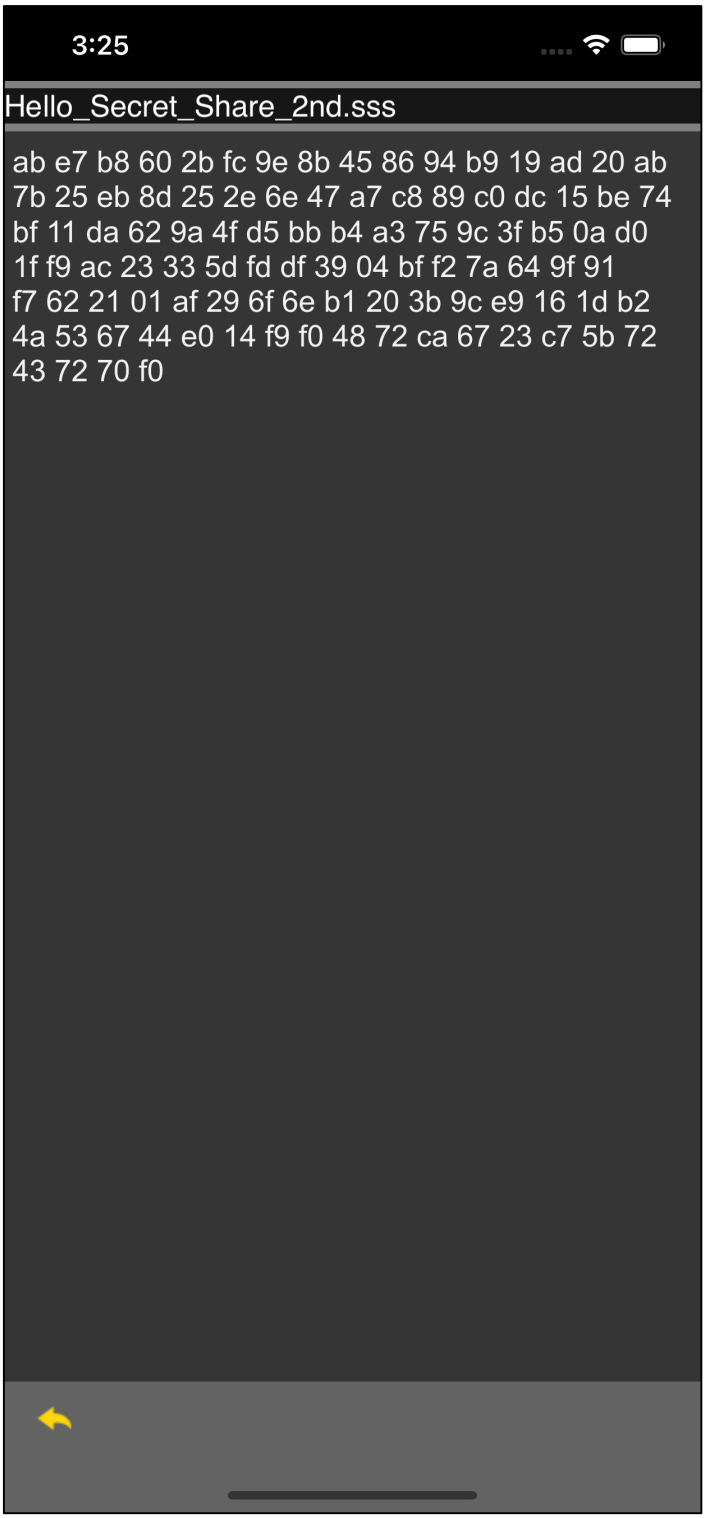
　　暗号文 かつ 復号鍵

というようなものになります。

(2, 3) 3分割 2結合

による分散というのは、たとえば、次のようなものになります。


3:25
Hello_Secret_Share_1st.sss
72 d5 dc ab 55 3a 9f 3b 69 ec e0 33 5f f9 0f 64
7b 47 b9 7c 9e 95 d5 fc 1c 73 32 7b 67 ae 05 cf
04 aa 61 d9 21 f4 6e 00 0f 18 ce 27 84 0e b1 6b
a4 42 17 98 88 e6 46 64 82 bf 04 49 c1 df 24 2a
4c d9 9a ba 14 92 d4 d5 0a 9b 80 27 52 ad a6 09
f1 e8 dc ff 5b af 42 4b f3 c9 71 dc 98 7c e0 c9
f8 c9 cb 4b


3:25
Hello_Secret_Share_2nd.sss
ab e7 b8 60 2b fc 9e 8b 45 86 94 b9 19 ad 20 ab
7b 25 eb 8d 25 2e 6e 47 a7 c8 89 c0 dc 15 be 74
bf 11 da 62 9a 4f d5 bb b4 a3 75 9c 3f b5 0a d0
1f f9 ac 23 33 5d fd df 39 04 bf f2 7a 64 9f 91
f7 62 21 01 af 29 6f 6e b1 20 3b 9c e9 16 1d b2
4a 53 67 44 e0 14 f9 f0 48 72 ca 67 23 c7 5b 72
43 72 70 f0


3:25
Hello_Secret_Share_3rd.sss
5f 5b a8 9f 7c c0 7e 06 7f e7 09 ee 6a 7e 71 dc
be f0 ed ea ca c1 81 a8 48 27 66 2f 33 fa 51 9b
50 fe 35 8d 75 a0 3a 54 5b 4c 9a 73 d0 5a e5 3f
f0 16 43 cc dc b2 12 30 d6 eb 50 1d 95 8b 70 7e
18 8d ce ee 40 c6 80 81 5e cf d4 73 06 f9 f2 5d
a5 bc 88 ab 0f fb 16 1f a7 9d 25 88 cc 28 b4 9d
ac 9d 9f 1f

Hello_Secret_Share_1st.sss

Hello_Secret_Share_2nd.sss

Hello_Secret_Share_3rd.sss

この3つの分散片のうちの、2つを揃えることができる人でないと、元には戻せません。

この3つの分散片は、それぞれ、源データの一部のデータを有しているだけです。

それぞれの分散片に、どのような操作をかけたところで、源データの情報は
得られません。

シャミアの秘密分散法というのは、

分散 … データを、連立方程式にする(変える)。

結合 … 連立方程式を解いて、データに戻す。

というものです。

各分散片は、連立方程式の係数の羅列というようなものになっています。

結合 … 連立方程式解くのに必要な数の連立方程式(分割片)を揃えて、
そして、連立方程式を解いて、元のデータに戻す。

これを行わない限りは、源データについての情報は、一切、得ることができません。

秘密分散というのは、

　　結合に必要な数の分散片を揃えることができるのは、自分だけ。

ということで、

　　情報の秘匿を行おう。

というものです。

ふつうの暗号では、

　　暗号鍵(パスワード)を覚えておかないといけない。

ということになります

これが、秘密分散では、

　　どの分散片 と どの分散片 とを結合させると、元に戻せるのか？

ということを覚えておかないといけない、ということになります。

そして、各分散片を、なくさないように、壊さないように、管理しなければなりません。

これは、ある意味、ふつうの暗号よりも、面倒で厄介です。

しかし、秘密分散というのは、

　　結合に必要な数の分散片を揃えることができるのは、自分だけ。

というのであれば、個々の分散片にどんな操作がかけられても、
分散源の内容が知られることはありません。

この「対解析性の強固さ」が、秘密分散を使うことによる、一番の利得になります。

　　結合に必要な数の分散片は、他人には、揃えることはできない。

こうなっている限り、秘密分散は、安全です。