www.ciphermachinesandcryptology.com

Secret Splitting
A Practical and Secure Way to Delegate Keys

DIRK RIJMENANTS

Abstract Every day, we use codes and passwords for computer access, encrypted files, on-line e-mail accounts, PIN codes, credit cards, safe deposit boxes and digital locks. To memorize all these passwords would be impossible. You could write them down but that's not very secure. You don't want to disclose your passwords to someone else, let alone to share them with multiple persons. However, when something happens to you, or in case of emergency, others might need to have access to things you protected with a password or code. The solution is called Secret Splitting. It's very easy to use and requires nothing more than a pencil and paper.

Keywords Secret Splitting, One-time Pad, Shares, Random Numbers, Secret Sharing

What is Secret Splitting

Secret Splitting enables you to leave your password or code in the custody of multiple persons without disclosing the secret. In Secret Splitting, also called Secret Sharing in cryptography, your secret information is split into several different shares. All shares are required to retrieve the original information and it is mathematically impossible to obtain the original information if one of the shares is not available. The information obtained from separate shares does not reveal any information or partial information about the original and does not assist in any way in retrieving the original information. Of course, we cannot simply cut the secret information in half, as this would reveal at least half of the original information and possibly lead to complete disclosure.

Where to Use Secret Splitting

Suppose someone has stored his money, documents, or other valuables in a safe. He splits the number combination to the safe. Each of his children receives one share, and in case of emergency, an illness or death of the parent, the children can only access the safe when all of them agree upon opening the safe.

This example shows clearly, what Secret Splitting is about: sharing responsibility instead of sharing secrets. Secret Splitting has two unique features: no individual person with a share

knows the secret information, and more people with a share results in more security. That is exactly the opposite of sharing the secret itself, where more people means more risk.

With Secret Splitting, more shares will put the responsibility for disclosing the secret information in the hands of more people. One single reliable person can prevent the disclosure of the information, even when all other people involved prove to be unreliable. Moreover, more people will increase the chance that reliable persons prevent disclosure of your information.

As with any human interaction, more people increases the chance that people disagree, and that is just what we need. Of course, we strive to distribute as many as possible shares to trustworthy people, but we only need one honest person to keep things safe. Giving all shares to unreliable people is obviously not a good idea, but we wouldn't do this in the first place.

Some possible applications for Secret Splitting are the protection of secret passwords to access confidential computer data or encrypted files, a digital lock to a room or to operate a device. A most common example is a computer login password. The most extreme example would be a nuclear missile launch site, where at least two people check the received order, and must both also agree upon using the code to push the Big Red Button.

Secret Splitting can also be useful to reduce the risk of interception when you send passwords or codes over public channels. One person could for example send a code through different media to the recipient. A code, split into four shares, could be sent by e-mail, post, mobile phone (SMS) and by telephone; each at different moments in time. An eavesdropper would have to monitor and intercept all these channels at the same time and for a long period, requiring vast SIGINT-like recourses. If the eavesdropper missed only one share, it will be impossible to reconstruct the original information.

How Secret Splitting Works

The principle of Secret Splitting is based on one-time pad encryption and it is very simple but effective. One-time pad offers the absolute security required to create the individual shares. One share is truly random, and one share is the result of the random share subtracted from the original information. All calculations are performed by hand, with pencil and paper. Therefore, Secret Splitting is easy to apply by everyone, without special knowledge of cryptography.

Let us show the principle in a little example:

Charlie wants to split the secret number combination 21 46 03 88 of his safe deposit box and give one share to Alice and one to Bob. He selects 8 random digits (see ‘Creating Secure Shares’ section). Next, he subtracts the random digits from his combination, digit by digit, without borrowing. Without borrowing means that if you need to add 10, you don’t get that from the next-left digit, you just add 10. Each digit stands by itself.

```
 21 46 03 88  Charlie’s combination
-25 01 77 61  the random share
--------------------------------
 06 45 36 27  the result share
```

We now have two shares: the random share and the result share. Alice gets the share **25017761** and Bob gets the share **06453627**. It is mathematically impossible for both Alice and Bob to retrieve the original information unless they put their shares together.

Retrieving the original secret combination is done by simple addition of the two shares, digit by digit, without carry. Without carry means that if the result is more than 9 we don't carry a 1 to the next-left digit (7 + 5 = 2 and not 12).

```
 06 45 36 27 Bob's share
+25 01 77 61 Alice's share
-------------------------------------
 21 46 03 88 Charlie's combination
```

Because we used subtraction to create the shares, it does not matter in which order we add the shares together to reconstruct the original information.

For each additional share that we want to distribute, we must create an additional random share. If the secret information is to be split into five shares, we need four random shares and one result share. In that case, all random shares must be subtracted from the original information to get that last result share.

Let us show this with an example with four shares:

```
 21 46 03 88 Charlie's combination
 52 11 73 69 random share 1
 58 91 06 17 random share 2
 44 31 58 94 random share 3
-05 00 41 37 random share 4
-------------------------------------
 82 13 45 91 result share 5
```

Again, we can reconstruct the original values by adding all shares without carry.

Splitting Text

We can also split text. To do so, we first have to convert the text into numbers. One possible way is to assign a two-digit number to each letter. You could use 01 to 26 for the upper case letters A to Z, 27 to 52 for lower case a to z, 90 to 99 for the digits 0 to 9 and 00 for a space. Of course, this system can be expanded to your requirements with additional symbols or special characters. This method is most suitable to split passwords that contain a mix of lower case, upper case, numbers and symbols.

```
  I  N  V  I  N  C  I  B  L  E  your secret password
 09 14 22 09 14 03 09 02 12 05  converted into digits
- 52 71 30 94 52 86 62 13 81 29  the random share
-------------------------------------------------------
 57 43 92 15 62 27 47 99 31 86  the result share
```

Alice's share: **5271 3094 5286 6213 8129**
Bob's share: **5743 9215 6227 4799 3186**

We wrote the shares in groups of four digits, just to make it easier to read them, but you can write them in any desired format. This doesn't affect the result. To reconstruct the secret information we simply add the shares together, again without carry, and re-convert the numbers back into letters.

There is no need to keep the conversion table secret. You may distribute the table together with the shares, to enable the share owners to retrieve the original information, if necessary. The conversion method does not affect the security of the system in any way. An example of a conversion table is found in Annex A.

Theoretically, another possible way to calculate the letters, without the use of numbers, would be a Vigenère table. In this case, the random shares and the secret information itself can only contain the 26 alphabet letters. However, because of its flexibility and simplicity, the system with conversion of two-digit values is preferred over a letters-only system.

Creating Secure Shares

Secret Splitting is based on the principles of one-time pad. To retrieve the plaintext (original information) we need the key (random share) and the ciphertext (result share). If we don't have ciphertext or key, it is proven mathematically impossible to retrieve the plaintext. With one-time pad, we send the ciphertext and destroy the key after use. With Secret Splitting, we keep both 'ciphertext' and 'key' on a physically separated and secure place. However, as with one-time pad, there are two important rules to obtain unbreakable shares and absolute security: true randomness and physical security.

The random share must be truly random. To generate true randomness there are several practical solutions. Whatever method you use, always make sure that there is always exactly a 1 in 10 chance for all digits to occur. A good random source is a lotto system with balls, or balls or marked coins in a pocket, numbered from 0 to 9. After extracting a number, that ball must always be mixed again with the other balls before extracting the next number. Another method is to use ten-sided dice. Never use normal six-sided dice, as they are statistically unsuitable to produce values from 0 to 9

Random numbers that are generated by computers are often insecure. Functions like RND are generally initialised with a small seed or no seed at all and the various algorithms to produce the random numbers are seldom cryptographically secure. Since we work with passwords and codes there's no need to produce many random digits and manual systems are more than sufficient for our purposes.

The second rule for absolutely secure splitting is of course the physical separation of the individual shares. It should be impossible for any of the share owners to obtain other shares without consent or approval of the owner of the other share. Again, more shares will increase security because it will be harder to obtain, acquire, find or to steal all necessary shares. For security reasons, the owner of a share could even decide to split his own share further into two new shares. This way, his share would only be usable if his two sub-shares are joined together.

In normal circumstances, it is sufficient that each share owner stores his share on some hidden or locked place. However, it could be useful to protect the shares in such way that a compromised share would be noticed. One possible way to do so is using a small well sealed (glued) plastic container that needs to be broken in order to get access to the share (wrap the folded text in aluminium foil). Seals can be glued into the transparent container. A damaged container and thus compromised share would be noticed immediately. Of course, the plastic container must also be stored in a physically secure place. The owner could always perform security verification and demand the owners of the shares to show their undamaged share.

If the rules of randomness and physical separation are followed, the secret information will be completely secure. It is a fact that there's no way to retrieve the secret information, other than getting your hands on all required shares. Of course, if you have split the code to a cheap five dollar lock, you will have five-dollar-security. It's useless to protect the code of a cheap safe if a

simple crowbar can wrench it open. On the other hand, if you split the combination of a safe deposit box, located at your bank, you can be absolutely sure that no individual share owner can access that safe.

Finally, Secret Splitting has another very important property. Since this system is unbreakable, the loss of one share will always result in the definite loss of the secret information, unless the owner still has a copy of the original. There is no way back if a share is lost or destroyed by accident! Therefore, it might be useful for the owner to have an extra copy of the original information, or for the share owners to have a copy of their share, somewhere in another secure location. And of course, when you have split secret information into shares and you intend to destroy the original information, be sure to double-check the shares, and check them once more, before you destroy the original!

Other Types of Secret Sharing

There are different types of Secret Sharing. Secret Splitting, as described in this paper, requires all shares in order to retrieve the secret information. This will cause problems when one share is lost. If you want to enable the reconstruction of the secret with fewer shares than the total number of shares, you will have to work with subsets. If, for example, Alice, Bob and John have shares, but two of them should be sufficient to retrieve the secret, you will need 3 different subsets (combinations of people) of 2 shares: Alice-Bob, Alice-John and Bob-John. Of course, each subset requires its own random shares. The downside of subsets is that this quickly becomes impractical when the number of participating persons increases. For 3 out of 5 shares you need 10 subsets and for 3 out of 6 you already need 19 subsets. Therefore, this scheme is only suitable for a single set or a limited number of subsets. The advantage of this basic scheme, based on one-time pad, is that it can be performed with pencil and paper.

Secret Sharing with threshold allows the reconstruction of shares with a fixed number of shares which is less than the total number of shares. You don't need subsets and each person receives a single share. If, for example, you have 5 shares with a threshold of 3, you will be able to retrieve the secret information with only 3 shares. Any 3 persons of a group of 5 can decide to disclose the secret. In contrast to Secret Splitting, the loss of one or more shares will not make reconstruction impossible, as long as at least the threshold number of shares remains. The threshold sharing schemes are either based on polynomial interpolation (Adi Shamir) or hyperplanes (George Blake). Unfortunately, these schemes required quite complex calculations and therefore are not suitable for use with pencil and paper.

ANNEX A

SECRET SPLITTING
CHARACTER TO DOUBLE-DIGIT CONVERSION TABLE

_ 00	J 10	T 20	d 30	n 40	x 50	. 60	[70	^ 80	0 90
A 01	K 11	U 21	e 31	o 41	y 51	: 61	] 71	% 81	1 91
B 02	L 12	V 22	f 32	p 42	z 52	, 62	{ 72	# 82	2 92
C 03	M 13	W 23	g 33	q 43	53	; 63	} 73	$ 83	3 93
D 04	N 14	X 24	h 34	r 44	54	? 64	+ 74	£ 84	4 94
E 05	O 15	Y 25	i 35	s 45	55	! 65	- 75	@ 85	5 95
F 06	P 16	Z 26	j 36	t 46	56	‘66	* 76	86	6 96
G 07	Q 17	a 27	k 37	u 47	57	“67	/ 77	87	7 97
H 08	R 18	b 28	l 38	v 48	58	(68	< 78	88	8 98
I 09	S 19	c 29	m 39	w 49	59	) 69	> 79	89	9 99
Values 53-59 and 86-89 are free to determine									