SECURE CODE SPLITTER (SCS)

With the provided templates you can give a secret code (combination lock, safe deposit box, electronic key code or password) in the custody of multiple persons without disclosing the secret code itself. Retrieving the secret code is only possible when all persons involved agree on putting their shares together. This method provides absolute security. Retrieving the secret code, even partially, is mathematically impossible without having all shares. More shares and more people involved provides more security as there is more chance of having at least one reliable person that refuses unauthorized disclosure of the secret code. This is the opposite of sharing the secret itself, where more people involved means more risk of disclosure. This method is ideal to grant access or disclose a secret code only in specific situations like emergency access to a building, alarm system, computer or safe during you absence. This system is based on the principle of unbreakable one-time pad encryption, where the information is encrypted multiple times with random keys, and encryption and random keys are used as shares. More information at the Cipher Machines and Cryptology website: http://users.telenet.be/d.rijmenants/en/secretsplitting.htm

INSTRUCTIONS

1. Write down the secret series of digits in the CODE row of the calculation sheet. Use pairs of digits if the code consists of separate numbers (combination lock code 37-5-81-9 is written as 37058109). If the code consists of letters, punctuations or symbols, write the letters in the TEXT row and convert the letters into digit pairs according to the conversion table at the bottom of the calculation sheet template. With the provided templates you can produce 2, 3 or 4 shares containing up to 20 secret digits or 10 characters. Never mix straight digits with letters, digits or symbols that are converted with the table, as user cannot distinguish them.

2. Share 2, and optionally share 3 and 4, are filled with truly random digits without any meaning or order. The use of truly random digits is essential for the security of the system! You can use ten-sided dice, a lotto bowl with 10 balls or numbered coins in a pocket. Put the extracted number back with the rest before mixing and extracting the next number. Never use normal dice as they are statistically unsuitable when simply adding the dice values! Never use a computer to generate the digits as computers are deterministic and cannot produce truly random digits.

3. Share 1 is calculated by subtracting the random shares 2, 3, and 4 from the secret code, column by column from left to right, without borrowing (modulo 10). In the example calculation sheet's fourth column, 5 – 9 – 7 becomes (1)5 – 9 = 6 and (1)6 – 7 = 9. If you only need 2 shares, simply leave shares 3 and 4 blank.

SECURE CODE SPLITTER – CALCULATION SHEET																					
TEXT																					1) Use code directly or convert text into digit pairs with help of conversion table. 2) Fill all used shares with truly random digits, except share 1. 3) Calculate share 1 by subtracting shares 2, 3 and 4 from the code without borrowing.
CODE	3	7	0	5	8	1	0	9													
- SHARE 2	5	5	8	9	4	3	2	5													
- SHARE 3	1	0	6	7	3	9	8	9													
- SHARE 4	/	/	/	/	/	/	/	/													
= SHARE 1	7	2	6	9	1	9	0	5													

4. Verify all subtractions by adding all shares together without carry (e.g. fourth column 9 + 7 + 9 = code value 5, not 25). The sum should be the secret code digit at the top of that column. An error will make reconstruction of the shares impossible!

5. Use the SCS template to create a personal share for each shareholder, containing only his row of digits and the names of all other shareholder. Note that the share no 1 is now at the top of the table! Strikethrough all unused shares. The example below shows John's share no 2 out of 3 from the combination lock code in the calculation sheet example. The fields of shares 1 and 3 are ready to be filled with the information from William and George if they all agree upon disclosing the code. Once all shares are entered in the proper fields, you simply add them together from left to right without carry and enter the result in the CODE row.

If required, you convert the CODE row digit pairs into text with the aid of the conversion table at the bottom and fill the resulting text in the TEXT row.

SECRET		SHARES																				SHAREHOLDERS	SECRET
	SHARE 1																					*William*	
	SHARE 2	*5*	*5*	*8*	*9*	*4*	*3*	*2*	*5*													*John*	
	SHARE 3																					*George*	
	+ SHARE 4	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/		
	CODE																					*Combination of safe deposit box No 25063 Bank of London*	
	TEXT																						
	To retrieve secret code, collect all existing shares, fill their digits in your form and add all shares together without carry (e.g. 7 + 8 + 3 + 5 = 3 and not 23) To retrieve secret text, convert code digit pairs according to conversion table																						

IMPORTANT NOTES!

- Destroy your calculation sheet after you finished creating and checking the shares.
- All shares must be stored on a secure location by the shareholders to ensure that they are inaccessible to the other shareholder. The secrecy of the code depends entirely on the physical separation of all existing shares.
- The shareholder should notify you immediately if their share is missing, as it could be used to disclose the secret code without collective consent. A new secret code should be created and implemented.
- Actual loss of a single share always results in permanent loss of the secret code for all shareholders. The owner of the secret code should have a backup or ask all shareholder to back up their share.
- The secret code is no longer secret after being retrieved by the shareholders and a new secret code must be chosen, set on the device, and new shares must be created.

The next two pages contain a calculation sheet template and a Secure Code Splitter template. Print as many SCS pages as there are shareholders.

SECURE CODE SPLITTER – CALCULATION SHEET

TEXT																								
CODE																								
- SHARE 2																								
- SHARE 3																								
- SHARE 4																								
= SHARE 1																								

1) Use code directly or convert text into digit pairs with help of conversion table.
2) Fill all used shares with truly random digits, except share 1.
3) Calculate share 1 by subtracting shares 2, 3 and 4 without borrowing from code.
4) Create individual shares

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

WARNING! Never mix straight digits with letters, digits or symbols that are converted with the table, as the users cannot distinguish them. Destroy your calculation sheet after you finished creating and checking the shares. All shareholders must store their share on a secure location to ensure that they are inaccessible to the other shareholders. The secrecy of the code depends entirely on the physical separation of all existing shares. The shareholders should notify you immediately if their share is missing, as it could be used to disclose the secret code without collective consent. A new secret code should be created and implemented. Actual loss of a single share always results in permanent loss of the secret code for all shareholders. The owner of the secret code should have a backup or ask all shareholders to back up their share. The secret code is no longer secret after being retrieved by the shareholders and a new secret code must be chosen, set on the proper device, and new shares must be created.

SECURE CODE SPLITTER

SECRET **SECRET**

	SHARES																			SHAREHOLDERS
SHARE 1																				
SHARE 2																				
SHARE 3																				
+ SHARE 4																				
CODE																				
TEXT																				

To retrieve secret code, collect all existing shares, fill their digits in your form and add all shares together without carry (e.g. 7 + 8 + 3 + 5 = 3 and not 23)
To retrieve secret text, convert code digit pairs according to conversion table

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

WARNING! Your share must be stored on a secure location to ensure that it is inaccessible to the other shareholders. The secrecy of the code depends entirely on the physical separation of all existing shares. Immediately notify the owner of the secret code if your share is missing, as it could be used to disclose the secret code without your consent. Actual loss of a single share always results in permanent loss of the secret code for all shareholders. The owner of the secret code or text should have a backup or ask all shareholders to back up their share. The code is no longer secret after being retrieved by the shareholders and a new secret code must be chosen, set on the device, and new shares must be created and distributed.