

SECURE CODE SPLITTER

With this system and according templates, you can give a secret code (combination lock, safe deposit box or electronic key code) in the custody of multiple persons without disclosing the secret code itself. Retrieving the secret code is only possible when all involved persons agree on putting their shares together. This method provides mathematical absolute security. Retrieving the secret code, even partially, is absolutely impossible without consent of all persons. This method is most suitable for authorising access in case of emergency. More persons provide better security as there is more chance of having at least one refusing reliable person. This is the opposite of sharing the secret itself, where more persons involved means more risk of unauthorised disclosure.

1. Write down the secret series of digits in the 'Secret code' row of the calculation table. Use pairs of digits if the code consists of separate numbers (combination lock 37-5-81-9 is written as 37058109). If the code consists of letters, write the letters in the 'Secret text' row first and convert the letters into digit pairs (A = 01, B = 02... Z = 26).
2. In this template, you can create 2, 3 or 4 shares. Fill each of the share rows 2, 3 and 4 with series of truly random digits, as long as the secret code. Make sure to pick truly random digits without any meaning or order!
3. Share 1 is calculated by subtracting the random shares 2, 3, and 4 from the secret code, column by column, without borrowing (modulo 10). If the first column contains the digits 3 – 5 – 1 the result is 7 because $13 - 5 = 8$ and $8 - 1 = 7$. If, for instance, you only need 2 shares, leave shares 3 and 4 blank.
4. Verify all subtractions by adding all shares together without carry ($5 + 8 = 3$ and not 13). The sum should be the secret code digit at the top of that column. Even a single error will make reconstruction of the shares impossible!

Your Calculation Table

Secret text (optional)										
Secret code (converted text)										
- Share 2										
- Share 3										
- Share 4										
= Share 1										

Example of calculating 3 shares

3	7	0	5	8	1	0	9			
5	5	8	9	4	3	2	5			
1	0	6	7	3	9	8	9			
7	2	6	9	1	9	0	5			

5. On the next page, copy the individual shares to the appropriate share in the according row of that share. Optionally, you can add the name of the share owner and additional information on the secret code or access details. Fill unused shares and fields with an X. Cut the different shares and give them to the according persons.

Example of share 2 out of 3 (example from above) with the fields of shares 1 and 3 ready to be filled if received.

		SHARES										OWNER			
SECRET	SHARE 1											X	X	William	
	SHARE 2	5	5	8	9	4	3	2	5			X	X	John	
	SHARE 3											X	X	George	
	+ SHARE 4	X	X	X	X	X	X	X	X	X	X	X	X		
	CODE TEXT														Combination of safe deposit box 25063 Bank of London
		To retrieve code, add all shares together without carry ($7 + 8 + 3 + 5 = 3$ and not 23)													
		To retrieve text, convert digits in pairs (01 = A, 02 = B...26 = Z)													

Some advice: Use only truly random digits for shares 2, 3 and 4. You can use ten-sided dice or a lotto system with 10 balls or numbered coins in a pocket (mix the extracted number again with the others before extracting the next number). Never use normal dice as they are statistically unsuitable! Loss of a single share always results in permanent loss of the secret code. Make sure to backup the secret code or ask all persons to backup their share. The secret code is no longer secret after being retrieved by the share holders and a new secret code must be set on the device and new shares must be created. Each share must always be stored on a secure location!



SECRET	SHARES										OWNER										
	SHARE 1																				
	SHARE 2																				
	SHARE 3																				
	+ SHARE 4																				
CODE																					
TEXT																					
To retrieve code, add all shares together without carry ($7 + 8 + 3 + 5 = 3$ and not 23)																					
To retrieve text, convert digits in pairs (01 = A, 02 = B...26 = Z)																					



SECRET	SHARES										OWNER										
	SHARE 1																				
	SHARE 2																				
	SHARE 3																				
	+ SHARE 4																				
CODE																					
TEXT																					
To retrieve code, add all shares together without carry ($7 + 8 + 3 + 5 = 3$ and not 23)																					
To retrieve text, convert digits in pairs (01 = A, 02 = B...26 = Z)																					



SECRET	SHARES										OWNER										
	SHARE 1																				
	SHARE 2																				
	SHARE 3																				
	+ SHARE 4																				
CODE																					
TEXT																					
To retrieve code, add all shares together without carry ($7 + 8 + 3 + 5 = 3$ and not 23)																					
To retrieve text, convert digits in pairs (01 = A, 02 = B...26 = Z)																					



SECRET	SHARES										OWNER										
	SHARE 1																				
	SHARE 2																				
	SHARE 3																				
	+ SHARE 4																				
CODE																					
TEXT																					
To retrieve code, add all shares together without carry ($7 + 8 + 3 + 5 = 3$ and not 23)																					
To retrieve text, convert digits in pairs (01 = A, 02 = B...26 = Z)																					



IMPORTANT NOTE: each share must be stored a secure location to ensure that it is inaccessible to the other share owners. The security of the system depends entirely on the physical separation of the shares! Notify the owner of the code if your share is missing.