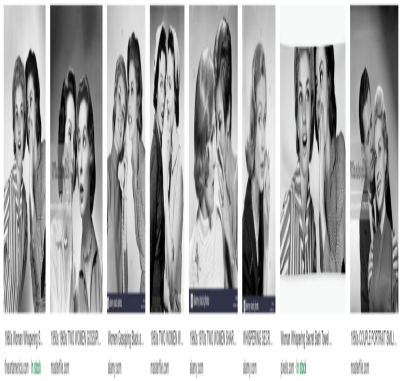

# Sociable encryption: The secret of the five keys

## Description



Will encryption save us? Social psychologist Shoshana Zuboff explains in detail the methods employed by Google and other digital giants to track our clicks, sell our data, and auction targeted advertising slots to monetise our private on-screen experiences.

Our online behaviour is the resource. We are the product, not the consumer. Googleâ??s clients are advertisers and third parties who buy this data, i.e. our data. We depend on the services Google offers, but â??there is no exit, no voice, and no loyalty, only helplessness, resignation, and psychic numbingâ?• (94). All we can do is hide:

> â??**encryption** is the only positive action left to discuss when we sit around the dinner table and casually ponder how to hide from the forces that hide from usâ?• (95).

If, by this dramatic account, encryption is the only action left, then itâ??s worth giving it another look.

## Simple secret delivery

Encryption has many applications, not least it enables the confidential transmission of information, and enables cryptocurrencies to function. Encryption is a way of codifying secret information and passing it through networks so it can only be read by the addressee but not by anyone else. Recipients with the coded message, and the decryption software and the decryption key can then read the message.

As Iâ??ve been thinking about secrets I was drawn to secrets.dyne.org, in particular the black and white stock photo on the front page showing two women apparently sharing a secret, with one whispering into the ear of the other. The picture shows a one-to-one model of secret sharing. But dyne.org demonstrates a more sociable method. Hereâ??s my interpretation of the challenge.

## Confidants

A spy (intelligence agent) tells a confidant: â??If something bad happens to me then contact Colonel Nutmeg at the embassy. Heâ??ll know what to do.â?• If the confidant is trustworthy then he or she is equipped to carry out the action as needed. But if some misfortune befalls the confidant then the message is lost.

The confidant may also be coerced or tortured to reveal the secret message. One solution is for the spy to tell several people the secret message. But that increases the risk of betrayal or careless disclosure of the secret message.



Another solution is to deliver part of the message to a number of people, none of whom have the complete message. On the spyâ??s demise they come together and resolve the puzzle of the message.

Thatâ??s as if the spy were to give each member of her trusted circle of friends a fragment of a torn up letter, or a map. (Did I see the map scenario in *Jumanji: Welcome to the Jungle*?)The full message is revealed when the pieces come together. Iâ??m sure Iâ??ve seen this in several adventure films: the fragments of a talisman are brought together as a key to open a secret door to a treasure. Thatâ??s a familiar mystery story trope.

## Sharing secrets

The application demo at [secrets.dyne.org/share](secrets.dyne.org/share) provides an interesting model for sharing secrets. The site contains instructions and a single entry field. You type a few sentences into the field. e.g.

> â??If something bad happens to me then contact Colonel Nutmeg at the embassy. Heâ??ll know what to do.â?•

The program then returns 5 character strings (secrets). These are in code and look like random sequences of characters. These string are even longer than the original message. (I include these in the notes below.)

The idea is that you email or message these five secrets to five of your trusted friends. As the secret is opaque to those friends or anyone else itâ??s not a high security item. The secret doesnâ??t need to be hidden or invisible.

On some signal or other these friends come together. The five secrets serve as a key to unlock your original message. In fact, the entire message is in the secrets. Thereâ??s nothing stored in a database.

The encoding is such that only three of the secrets are required to unlock the message. Thatâ??s smart. It supports the possibility that one or two of your friends may not be available to reconstruct the message, or may have lost their secret, or missed the call to action.

Thereâ??s a web page to â??combine secrets.â?• Three of your friends paste their bit of code in the fields and the message appears intact and word for word. If even one character out of the three secrets is misplaced then the message will not be reconstructed.

Of course, you have to trust that the website isnâ??t storing your original secret message. To use this in earnest you and your friends would need to run the coding-decoding software on their own computers, and thatâ??s available for download on the website.

## Human-centred encryption

The dyne.org website explains the application of the method.

> â??Secrets can be used to split a secret text into shares to be distributed to friends. When all friends agree, the shares can be combined to retrieve the original secret text, for instance to give consensual access to a lost pin, a password, a list of passwords, a private document or a key to an encrypted volume.â?•



As explained in a 1979 article on this encryption-sharing method, the method could be used for authorising a group decision where the majority decision is to prevail, e.g. over half the executives on a board have to agree before attaching a digital signature to a cheque. The 3 out of 5 rule means that the cheque could be signed off digitally by the majority (quorum) and not vetoed by the minority. The method could presumably be extended to larger numbers of participants, different sized quorums, and other voting contexts.

## Trust me

Thatâ??s arguably a human-centred, sociable approach to trust. You have to organise your friends to agree to this method, and how they will come together. The secrets are not human-centred though. No one could commit those secrets to memory, and they could be lost in the secret keepersâ?? file systems.

There are ways to make the secrets more memorable. Itâ??s more complicated, but you could deliver secret words (e.g. â??dragonfly,â?• â??magenta,â?• â??moonbeamâ?• â?¦) secretly to each of your friends.

These words in turn act as decryption keys to decode each of the secret-keeperâ??s coded secrets. A string of code that has been encrypted can also be encrypted, and decrypted with its key. There are online tools for encrypting and decrypting messages with a key: codebeautify.org/encrypt-decrypt

Once encoded, the secrets could then be stored in multiple locations. No one could convert them into the sequence that could work in the share secrets application until they are converted using the secret-holderâ??s key.

A string of code that has been encrypted can also be encrypted, but you wouldnâ??t know immediately if that stage in the process was successful. Itâ??s as if you were converting one unmemorable random string of alphanumeric characters into another unmemorable random string.

Manipulating code sequences requires concentration, motivation, opportunity, organisation and alphanumeric cognitive agility â?? not always present in an environment of informal sharing, as we â??casually ponder how to hide from the forces that hide from us.â?•

One of the nice thing about the secrets.dyne.org method is that if you received a random string of characters from your (spy) friend, then you would at least know itâ??s a code. Thatâ??s a bit like someone handing you a key, or a fragment of a map, or whispering in your ear. At least you know thereâ??s a secret in play, even if you donâ??t remember it or yet know why you are being told.

## References




- Sandbeck, Sune, A.T. Kingsmith, and Julian Von Bargen. 2020. The block is hot: a commons-based approach to the development and deployment of blockchains. In Massimo Ragnedda, and Giuseppe Destefanis (eds.), *Blockchain and Web 3.0: Social, Economic, and Technological Challenges*: 15-29. London: Routledge.
- Shamir, Adi. 1979. How to share a secret. *Communications of the ACM*, (22) 11.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books


## Notes

The five secrets encoding the message: â??If something bad happens to me then contact Colonel Nutmeg at the embassy. Heâ??ll know what to do.â?•

- WLMFNP33Q52RSGRZERPP7TXX86LE9WC74Q787MZFKPDV84VNBXZ3Z63NUM
  9L9LL63UVWXDENQ2BK9KQ4869UQ2RQE7P9HLXZ3GV6XHK8X8RZ57H6D277
  DKPSMMEVE368B8WPMXVN2HWREVP73C6G799L57HX73Q7GG7ANEDXWMGZ
  FWM54XPP3FKENK726H87LLQWGPA5N25V58UW43P7XD2CQQGV254LA7
- X83HRGPMZ28NA6D2WWGQXU3VDDPXR7FPV3ZKN2MTXG8XVWEGAVDRLDV4
  KHE9MR5EXRAWV657L2XSPZ37GXZ3SGQKRPGW6UG96M7RRPB42D8MDZQA5
  7KN2MVRC9MPWR6X5SNXVW87LKSE5PL99XQFM42L57Z4UZ8G9NRWXSX35Q
  M6X5HP9EVWG2KAP378NGEGA7PK453VKCZ5MXKNXC5MG54KLGU2X8ZNM44
  HP
- 7N5TK38V965GFV77V9RNDCKR8QM5GWU6K75L4XEA2GQPGK4RSWN55X2Z4
  H9QN67LD7UE3ZR9KR4FK3D4R7ZLUVN8G7M4XADN35PP2WHL98GEZ65H4N4
  4K2K2UPX533X3WSMX6P5X36U3MKXK9X3UZ67ZWZZQTL9XW928GSPLRW8Z
  W5UMLXM2ZKKCEMK39R6WFDQE7PG24SDEMNP6EFMV6NKE5ZUELG5MZXKU
  6
- 8KDA2X7835X4U2G5G9X6ZU27QPXPP9HL29P8964T2PWWK2E6EC6PQKPQ3N
  TGLX9ZQNDU4973WXRWT348DP9RMA59G6LG2RTXWKMQE93UV8QKX389MU
  G6552R9NA7LR87M44H5L96EX95AK3ZD682QHMEDKP5MVCMZPDVP6MH7KE6
  D39PH598Q473VEAQW6EL56VC3P3N95N7UEX8LR5WC696GM4RPTLZ5X4D4V

TL

- NNWT9VVX4MPRT9NKMZ73QS7649943PSK26XM7MDUMP7D973ZDHL37RPND
  MS5DRX96Z5CDMEVR6LLBKVDE9MDRMURG723VGLSPPDMWE9ZUGQ6RE5RQ
  MCM4XMV2LGWCL5565583AQZDPL293RCKGVN6DX5B3PV779PMA4K9VEPX8R
  U7WKE4PL8EUD2VZPZ2RWSNV9325EMFMN52G844HZRVM875VCMG6M2NGR
  UR5N7DWZRPBK

(Iâ??ve insert line breaks so these strings donâ??t run off the page.)

Hereâ??s a simpler set of 5 secrets to combine at https://secrets.dyne.org/combine.

2GGBL79NM7REBKPW4ER9BNXD5ZP6XB83DD4KDS58RPP93SRXZ5NRZWTM
VRRBMDLQZR26BGELV8XLPAXL23GKRZHD4DE2LWHMPNG5EQNHR8LWM9W7AQ
ZEEBZ47KMRV7HMVEKQL3ZC6ML6VMPPA59XK8ZNDS64XP43KXA6K98L8WWBV
W88BPVDWQEKKSZGMGZ7MQAMW2X2Q9ZU76EX2ZE7S4G9MPPXNFG773X7GMSD
VRRBDREE5KMEFE23EER9GFKZVP7PL6U339NLNK4BKND57487C5MVDWZ4PHG



**Category**

1. Society

**Tags**

1. encryption
2. secrets

**Date Created**
January 18, 2020
**Author**
rcoyne99