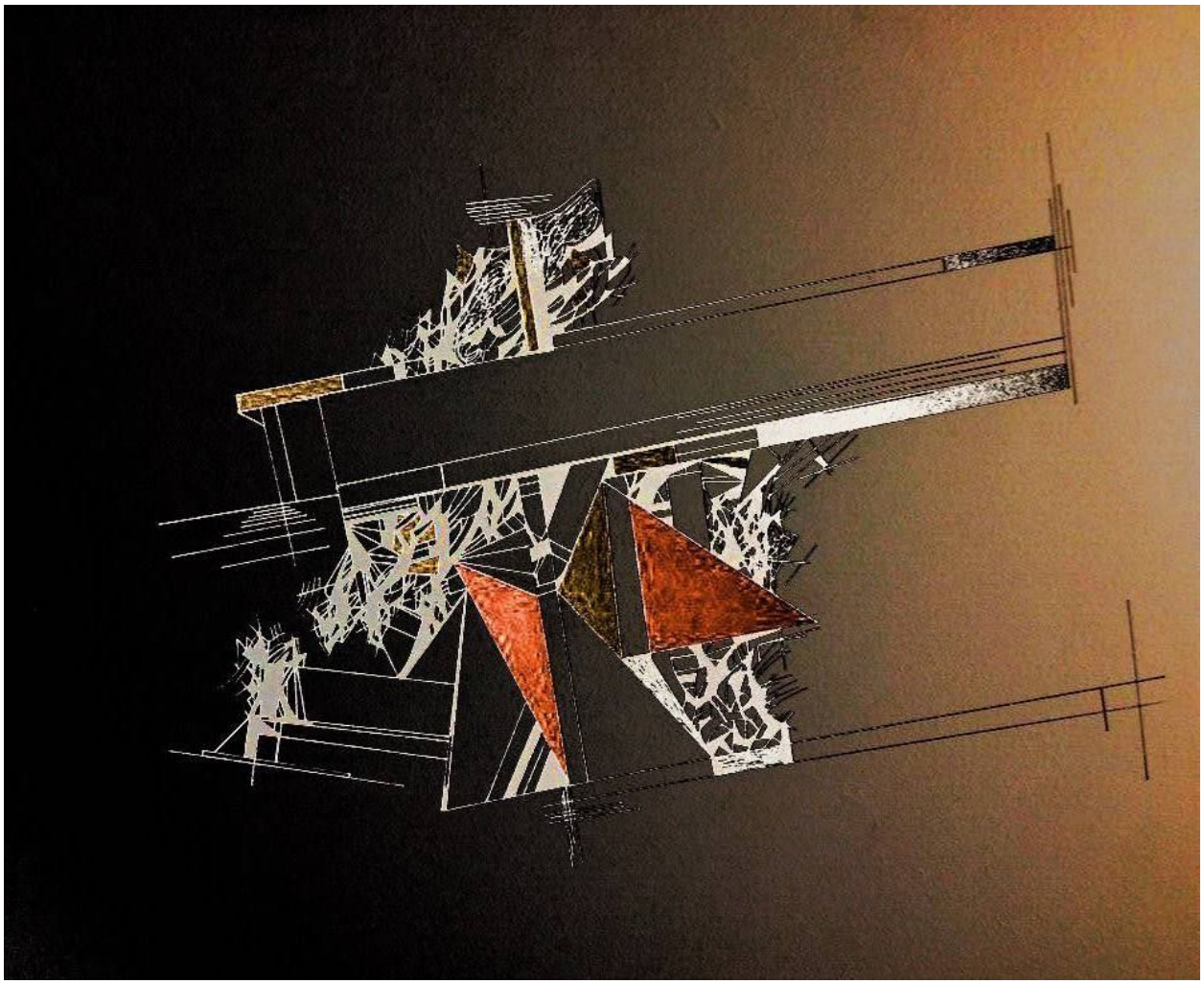
A CIA Agent's Guide to Steganography, Fooling the KGB, and Protecting Your Crypto



Greetings dear readers! Today I would like to discuss with you an important thing, but to understand the topic, please read my previous articles first, especially about the OpSec view through history. As you might have guessed from the title I would like to immerse you in the world of spies and KGB agents leading an eternal confrontation, then to tell you about the very essence of our conversation - Steganography.

We are gonna learn about what it is, how it was used in ancient times and how hackers and ordinary users use it now, and most importantly, for what and why. And we will finish

with a discussion of how we as normal people and average internet users can apply the above-mentioned methods to secure our crypto or fiat assets, passwords and make our lives easier in general.

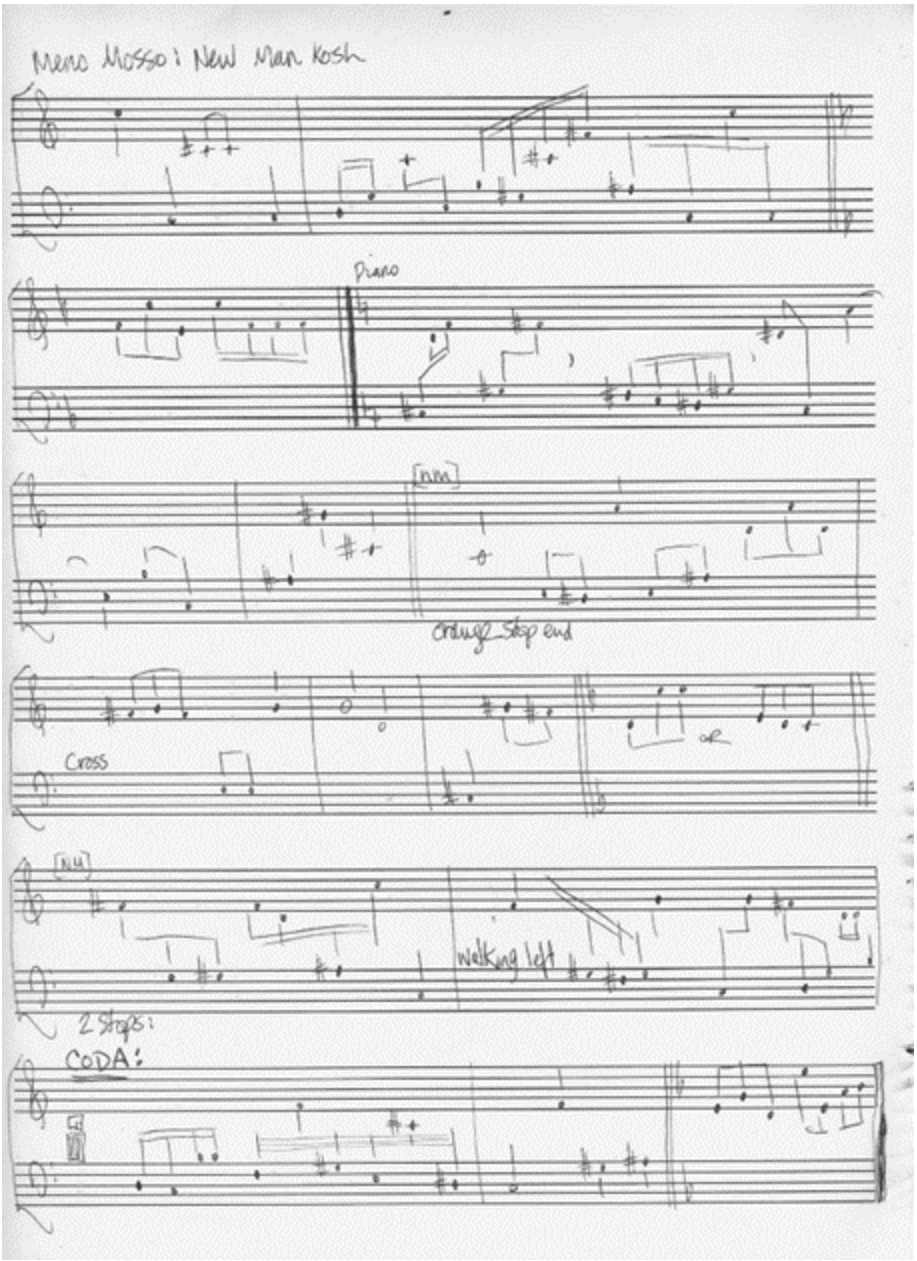
The cover for this article was done by my good friend and artist — RegulLion. I would be very happy if you buy NFTs from him on OpenSea — they are all classically hand-drawn, and all the money raised will go to our joint public good project. We know each other well so in case I disappear, he'll have the exact details of me. Consider this my canary.

#I - Mission Impossible: Fool the KGB

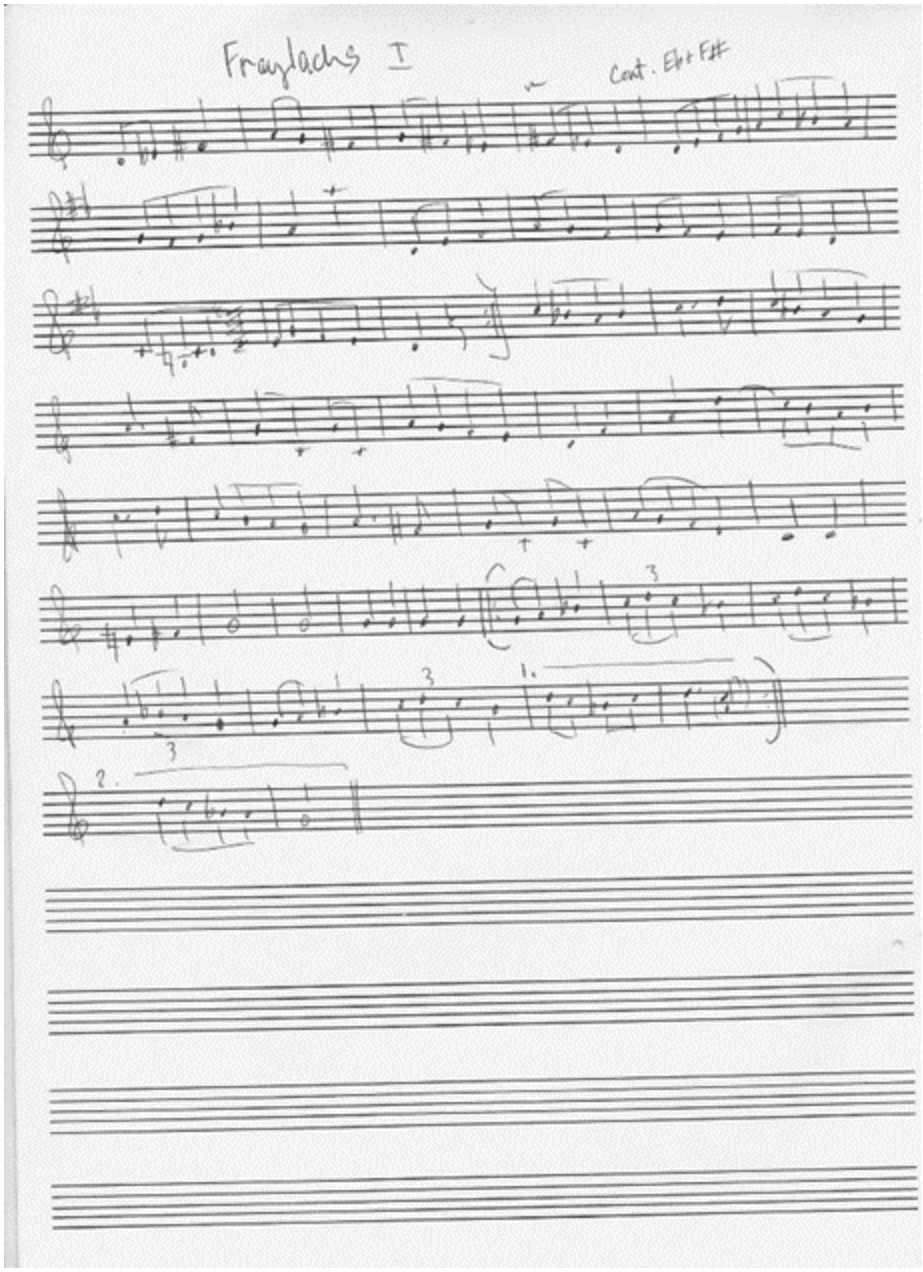
Those who restrain desire do so because theirs is weak enough to be restrained". - William Blake, The Marriage of Heaven and Hell

---

In 1985 saxophonist Merrill Goldberg flew to Moscow with three musicians from the Klezmer Conservatory Band. Goldberg had a lead sheet and instrument accessories with her. In one notebook Merrill Goldberg kept hidden information.



The saxophonist herself developed a note-based cipher that contained names, addresses, and other details the band needed for the trip. The cipher looked like a real lead sheet and contained secret information. The secret notes were on several pages of the book mixed in with the real compositions. Such secrecy was due to the fact that the band did not want to tell Soviet officials the details of their trip. The musicians were going to meet with the Phantom Orchestra.



The Phantom Orchestra was a dissident ensemble that Goldberg described as an association of Jewish refuseniks (Jews who were not allowed to leave the USSR), Christian activists, and Helsinki observers who secretly monitored the Soviet Union's compliance with the [1975 Helsinki Accords](#).

The Klezmer Conservatory Band's trip was financed and coordinated by [Action For Soviet Jewry](#), a non-profit organization that provided humanitarian aid to the USSR and helped Soviet Jews immigrate to Israel and the United States.

The trip was a rare opportunity for American and Soviet musicians to meet in the USSR and make music together. The visit also allowed the American musicians to pass

information to the Phantom Orchestra about helping Jews and their future plans. And the ensemble shared information about people trying to flee the USSR.

Goldberg and her colleagues traveled to Moscow separately in pairs so as not to arouse suspicion. They were trained in proper interrogation behavior and told to expect surveillance by Soviet officials throughout the trip. But first, Goldberg had to get her laptop through border control.

"When we arrived, they immediately took us aside and went through everything in our luggage. It was crazy. The border guards even opened a notebook. If there was a musician there, he would have figured out the catch. They looked through all the pages, and then they gave the notebook back," Goldberg said.

The names of the musical notes consist of letters from A to G, so they don't provide the full alphabet. To create the cipher, Goldberg assigned the letters of the alphabet to notes in a chromatic 12-tone scale, adding note keys, ranges and rhythms. In this way, Merrill was able to add verisimilitude to the coded music. According to Goldberg, her code allowed her to preserve information about people or details that could help Jews emigrate from the USSR.

After a stop in Moscow, the band came to Yerevan to meet the Phantom Orchestra. The musicians got to know each other and even gave some small concerts. During their eight days in the USSR, Soviet agents constantly monitored the musicians and repeatedly interrogated them.

After their stay in Yerevan, the American musicians planned to go to Riga, Leningrad and Paris. During the trip, KGB agents caught the musicians, took them to Moscow and confiscated their passports. Then a decision was made to deport the band to Sweden. Accompanied by security guards, the musicians were taken to the plane. According to journalists, the group was not told the reason for the deportation.

According to Goldberg, the group was able to help some people leave the USSR permanently. Merrill Goldberg's note cipher was not difficult to crack. However, the obfuscation proved to be an elegant and harmonious encryption scheme that facilitated the fulfillment of great plans and goals. *Yes, they were caught, but how would the story have ended if the agents had found out the information? Fortunately, no secrets were revealed from a lead sheet with notes and so the case was limited to deportation.*

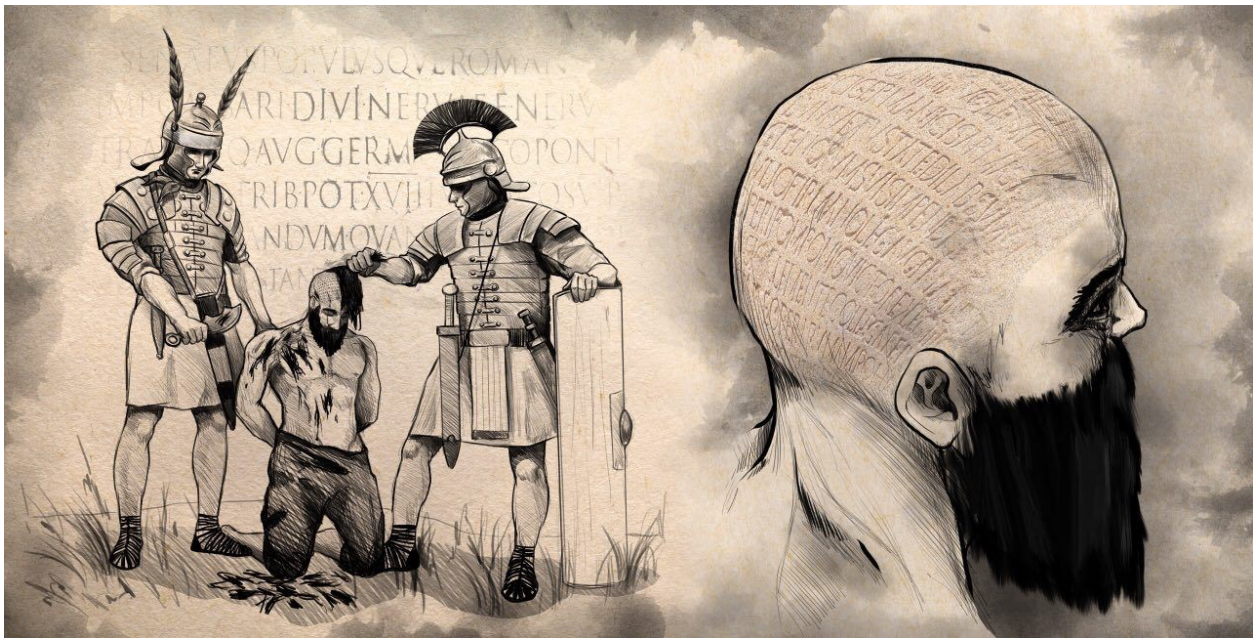
Many admire their courage when they hear about this story and that is undoubtedly correct, but we researchers have always been attracted only by the details and I want to draw your attention to them. Merrill and her friends were successful because they were

well versed in the ancient science of covert transmission of information - steganography. But what is it? Let's get to the bottom of it.

II - What is Steganography?

Steganography (from Greek. στεγανός - hidden + γράφω - writing; literally "cipher") - a science that allows you to hide the transmitted data in a certain container, thus hiding the very fact of information transfer.

Unlike cryptography which hides the contents of a secret message, steganography hides the very fact of its existence. Steganography was first introduced in 1499, but the method itself has existed for a very long time. Legends have brought us a method that was used in the Roman Empire: a slave whose head was shaved was chosen to deliver a message, and then text was applied with a tattoo. After the hair grew back, the slave was sent on the road. The recipient of the message would cut off the slave's hair and read the message.



If following [Hew Dawson](), a SERM Consultant, throughout the XX century, both steganography and the science of determining the fact of embedded information in a container - stegoanalysis (in fact, attacks on the stegosystem) - actively developed. But today we see a new and dangerous trend: more and more developers of malware and cyber-espionage tools resort to the use of steganography.

Most anti-virus solutions today do not protect against steganography or do not protect well, meanwhile, we need to understand that each container is dangerous. It can hide

data that is exfiltered by spyware, or malware communication with the command center, or new malware modules.

Hiding data is a common practice among hackers. They hide their sensitive data in the secure host area (HPA), Slack space and alternative data streams (ADS). as these areas are not included in any search parameters. They can also use steganography techniques to communicate covertly, transfer software licenses, bypass leak controls, and more. However, in addition to attackers, steganography techniques may well find application in information security in both everyday and professional activities.

Today scientists have developed and tested various algorithms and methods of steganography, we will note the following:

- **LSB-steganography (a message is hidden in the lower bits (one or more lower bits can be used) of the container. The fewer bits involved, the fewer artifacts the original container receives after implementation.**
- **The method based on hiding data in discrete cosine conversion coefficients (hereinafter referred to as DCP) - a kind of the previous method, which is actively used, for example, when embedding a message in a JPEG container. Other things being equal, such a container has a slightly smaller capacity than in the previous method, including the fact that the coefficients "0" and "1" remain the same - it is impossible to introduce the message into them.**
- **The method of hiding information using lower bits of the palette - this method is essentially a variant of the general method of LSB, but the information is embedded not in the least significant bits of the container, and the least significant bits of the palette, the obvious disadvantage of this method - low container capacity.**
- **The method of hiding information in service fields is a fairly simple method based on the use of service fields of the container header to store the message. The obvious drawbacks are low container capacity and the ability to detect embedded data using common image viewers (which sometimes allow you to see the contents of the service fields).**
- **Embedded message method - is that the message is embedded into the container and then extracted using a scheme known to both sides. It is possible to embed several messages into one container, provided that the methods of embedding them are orthogonal.**
- **Broadband methods, which are subdivided into:**

a) Pseudo-random sequence method; a secret signal is used which is simulated by a pseudo-random signal.

b) Jump frequency method: the carrier frequency changes according to a certain pseudo-random law.

Why do malware authors increasingly use steganography in their developments? We see three main reasons:

- **It allows them to hide the very fact of uploading/downloading data, not just the data itself;**
- **It helps to bypass DPI systems, which is important in corporate networks;**
- **The use of steganography can bypass checking in AntiAPT products, because the latter can't process all the graphic files (there are too many in corporate networks, and the analysis algorithms are quite expensive).**

For the end user, steganography can be a non-trivial task. For example, let us give two containers: empty and filled, as which we use the standard image for Lenna graphical studies.

Take a close look at these two images. Can you tell them apart? They are the same in size and appearance:

However, one of them is a container with an embedded message. Both images "weigh" 786,486 bytes, but the top contains messages from the first 10 chapters of [Nabokov's Lolita](#).

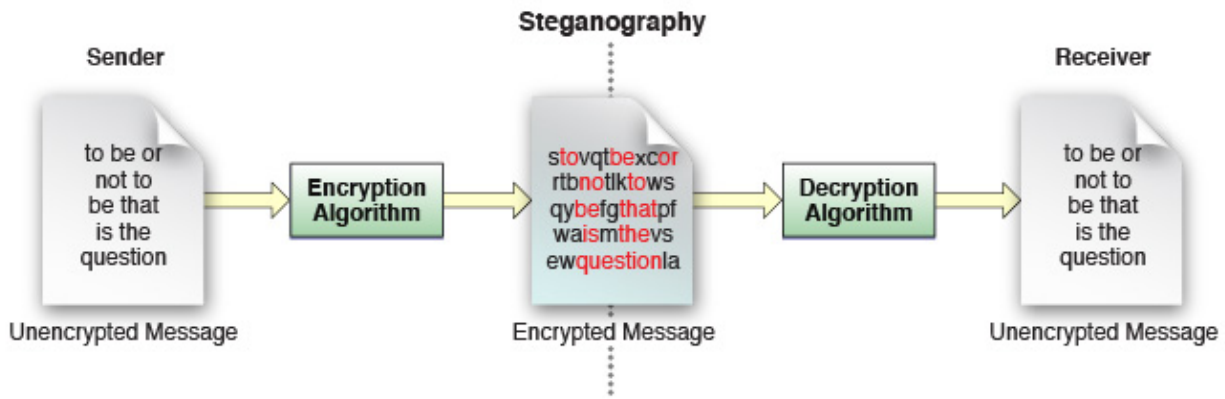
III - StegaCrypto: Closer than it seems

Let's take a look at how the above methods will help you protect your cryptocurrency! To begin with, let's stipulate that in this article I'm going to break down how you can hide - seed phrase/private key, file, audio and picture. This should be enough for you to get started. It is important to mention that the text generated by steganography method out of your seed encodes exactly the same information as the original seed, and should be treated with equal care.

You wouldn't go pasting your wallet seed around the Internet and expect not to have your money stolen, so don't do it just because the seed is hidden steganographically. Why

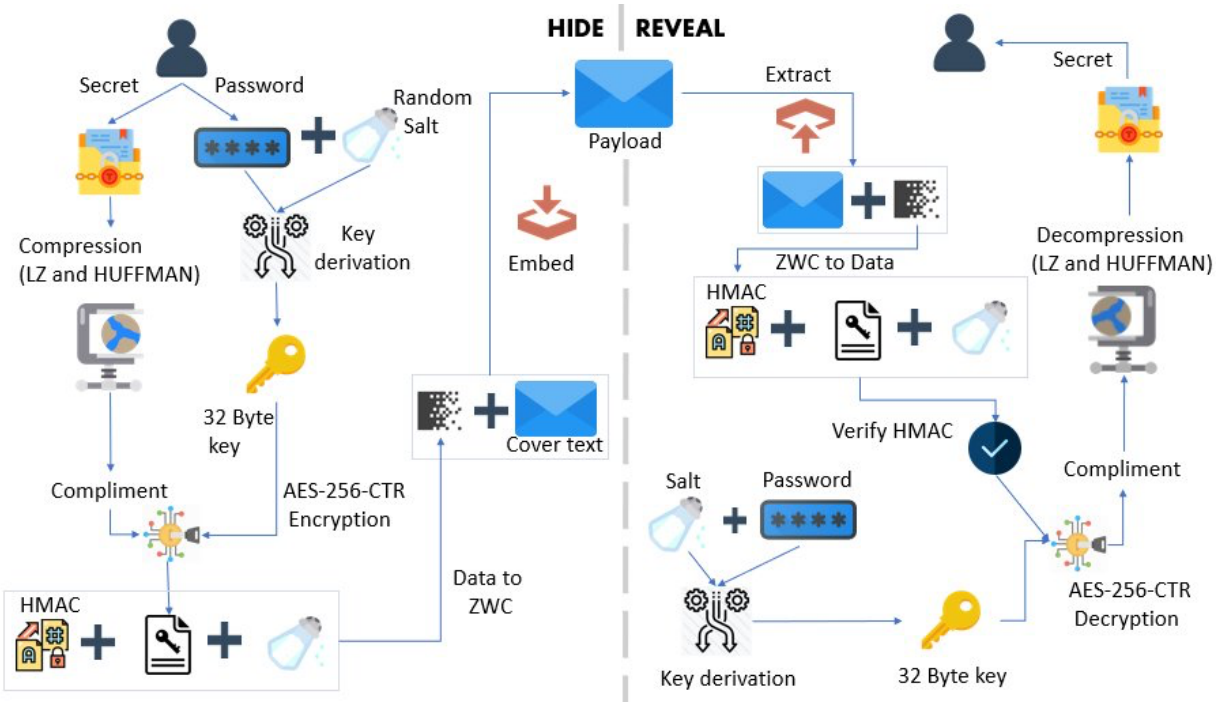
you may ask? Because such tools exist as well and you can test your steganography with them as well.

But it might help you if you have to hide your seed on paper in your house and you don't want a casual burglar to guess what it is. Or if you have to carry it on your person through an area where you might be searched by somebody who might want to steal your money.



Pay attention to this project, which I highly recommend as it will help you do what you want faster and easier than anything else: visit incoherency.co.uk/stegoseed and check out Author's writeup on it.

Also check out this awesome OpSec service which is a pure JavaScript steganography module designed in functional programming style, to hide secrets inside text by compressing and encrypting the secret before cloaking it with special unicode invisible characters.



There is also a way more hardcore option for true OpSec lovers: just store your crypto wallet seed phrase securely & publicly in a tattoo, [use this tool which creates an SVG](#) and PNG of the encrypted phrase, the decryption key, and a QR code for coin deposit and do not speak too much about it.

For a perfect OpSec illogical actions are always a definite advantage - think at least of the logic bomb method, when in order to turn on the computer you need to perform several non-obvious actions or even connect the chips in the right order! You can hide your phrase by inserting it into a track of your least favorite rapper and encrypting it with these programs:

- **github.com/danielcardeenas/AudioStego**
- **github.com/Buggaboo/LSB-steganography-audio**

...Or you can insert it into a file with GTA V and post its compressed version on YouTube with this great program. By the way, this way you can get absolutely free and unlimited data storage - all the data will be available only to you, as you will have the decryption key.

As you can see, the use of steganography is very widespread and its presence makes the system more secure, but do not overdo it - here I advise you to read my previous article, its topic is strongly related to our current subject of discussion.

If you are interested in the question of secure storage of cryptocurrency then I advise you to read the following articles:

- **Master of OpSec Masters: A View Through the Prism of Time**
- **OpSec in Crypto: Thoughts**

And study my OpSec Guide as well as all the links and references in it. Stay safe!

#IV - Conclusion & References

What's the bottom line? In the end, we learned about a really important ancient secret that has passed into our world with almost no significant transformation, and combines so well with our reality that it can even be used to protect your cryptocurrency or to create yourself eternal free file storage!

Remember that everything new is the overlapping of the old and in this context we take the experience of our ancestors and adapt it to ourselves. I have faith in you! Be careful and check out my other works!

References:

- **www.edureka.co/blog/steganography-tutorial**
- **www.linkedin.com/pulse/steganography-pro-level-hew-d?trk=portfolio_article-card_title**

Additional list of tools:

- github.com/Paradoxis/StegCracker
- github.com/TryCatchHCF/Cloakify
- incoherency.co.uk/image-steganography
- stylesuxx.github.io/steganography
- manytools.org/hacker-tools/steganography-encode-text-into-image
- sourceforge.net/projects/anubisstegano/files/latest/download
- www.softpedia.com/get/Security/Encrypting/DeEgger-Embedder.shtml#download
- jpinsoft.net/DeepSound/Overview.aspx
- sourceforge.net/projects/hallucinate
- sourceforge.net/projects/jhideapp
- download.cnet.com/windows/openpuff-team/3260-20_4-10146585-1.html
- tool.geoimgr.com
- http://www.openstego.com
- paranoiaworks.mobi/ptepc
- github.com/KuroLabs/stegcloak
- github.com/StefanoDeVuono/steghide
- github.com/solusipse/spectrology
- github.com/jklmnn/imagejs

Blockchain + Steganography:

| Note: Steganography is best used not instead of cryptography, but together with it. This combination allows you to hide both the information itself and the fact of its storage or transmission.

| Note: The main difference between cryptography and steganography is that steganography methods allow you to hide/conceal information inside media such as images, audio recordings, spam, etc., and hide the fact that there is any data there at all, while cryptography methods consist of encoding the content in an unreadable format using algorithms such as RSA, AES, DES, etc.

- medium.com/@zenon.network/the-new-nft-standard-when-cryptography-meets-steganography-9e356007dcaa
- mdpi-res.com/d_attachment/sensors/sensors-21-04078/article_deploy/sensors-21-04078.pdf?version=1623581808
- www.researchgate.net/publication/348380022_Blockchain_for_steganography_advantages_new_algorithms_and_open_challenges
- www.researchgate.net/figure/A-double-steganography-model-combining-blockchain-and-IPFS_fig3_351292756
- ieeexplore.ieee.org/ielx7/6287639/9312710/09520396.pdf?tp=&arnumber=9520396&isnumber=9312710&ref=aHR0cHM6Ly93d3cuZ29vZ2xlLnJ1Lw==
- www.sciencedirect.com/science/article/pii/B9780323858540000095?via%3Dihub
- www.academia.edu/73123346/A_Novel_and_Robust_Hybrid_Blockchain_and_Steganography_Scheme
- arxiv.org/pdf/2101.03103.pdf

Support is very important to me, with it I can spend less time at work and do what I love - educating DeFi & Crypto users!

- **Check out my GitHub**
- **Track all my activities**
- **All my Socials**
- **Join my TG channel**

Use dangerzone.rocks if you are working with PDFs and please follow OpSec Guide!

• How to store crypto securely - tips from CIA_Officer

• 2 Violent attack vectors in Crypto: a detailed review

• OpSec in Crypto: Thoughts

If you want to support my work, you can send me a donation to the address:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU - BTC**
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**

Thank you! ❤️

Also published here.