



CRYPTOGRAPHY AND STEGANOGRAPHY

Department of Informatics

Session 2 – Difference Between Cryptography and Steganography

Ambros Magnus Rudolf Mekeng,
S.T.,M.T

Abdul Azzam Ajhari, S.Kom.,
M.Kom.



- In addition to encoding with cryptography, information can also be secured from unauthorized access using steganography.
- Steganography: the science and art of hiding secret messages in other media so that their existence is undetectable.



**Bomb exploded at
20.00 WIB**





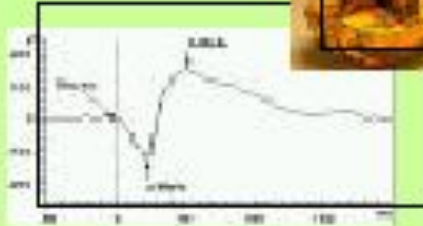
Difference Between Cryptography and Steganography

- Cryptography: hiding the content of a message
 - ☐ Purpose: so that the message cannot be read by a third party (opponent)
- Steganography: hiding the existence of a message
 - ☐ Purpose: to avoid suspicion (conspicuousness) from a third party (opponent)



Stego-data are
inconspicuous.
Steganography will **not be
detected**.

George obtains oranges yet eight's are
rubbish!



Encrypted messages are
conspicuous. They will be
detected as ciphertext or silly
data.

h1wDlwFpbAtjdf0BA/9KBX2jS17O5SRQsu2PF
caBqUXIQdyt1Fri/Wsg+eXoYsxnJ11Cn2JD7vjl
F2GH8GEr/vGQk8SQVCMYXzfPkgW0tr6RJX
AEIFF9rjnDB3kOmmVc1adrTQnLrqiC/15r&Us
ezowgZI82T/QVvk59YsuChd+Ce8vql/klCeqmv
w9J2amre3uxpWIOqCEQNzZyHx8HeYPf29k
Xu+uk1gekZZVdELmLD/Wa/xBKFTNUBr+16
ewoQBxQ8+3cTXSIGPTqdzDSasgQG17Z1sr
/Lhu0qzems4GY90OukeiCPvHJQuXZn2UW



Digital Steganography

- Digital steganography: the hiding of a digital message within another digital document.
- Carrier file: a digital document used as a medium to hide a message.

1. Text

“We are all brothers and sisters”

- Txt
- doc
- html

2. Audio



- wav
- mp3

3. Gambar (*image*)



- bmp
- jpeg
- gif

4. Video



- Mpeg
- avi
- dll

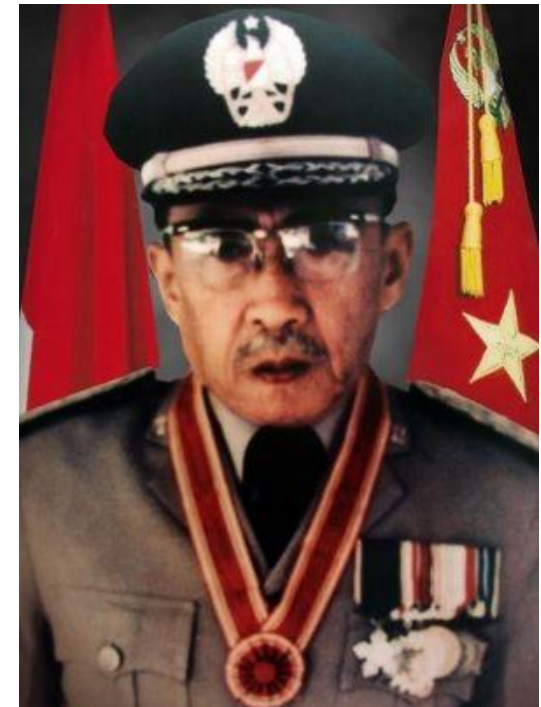


cryptography doesn't 'solve' protection issues but hopefully turns them into more simplified problems.

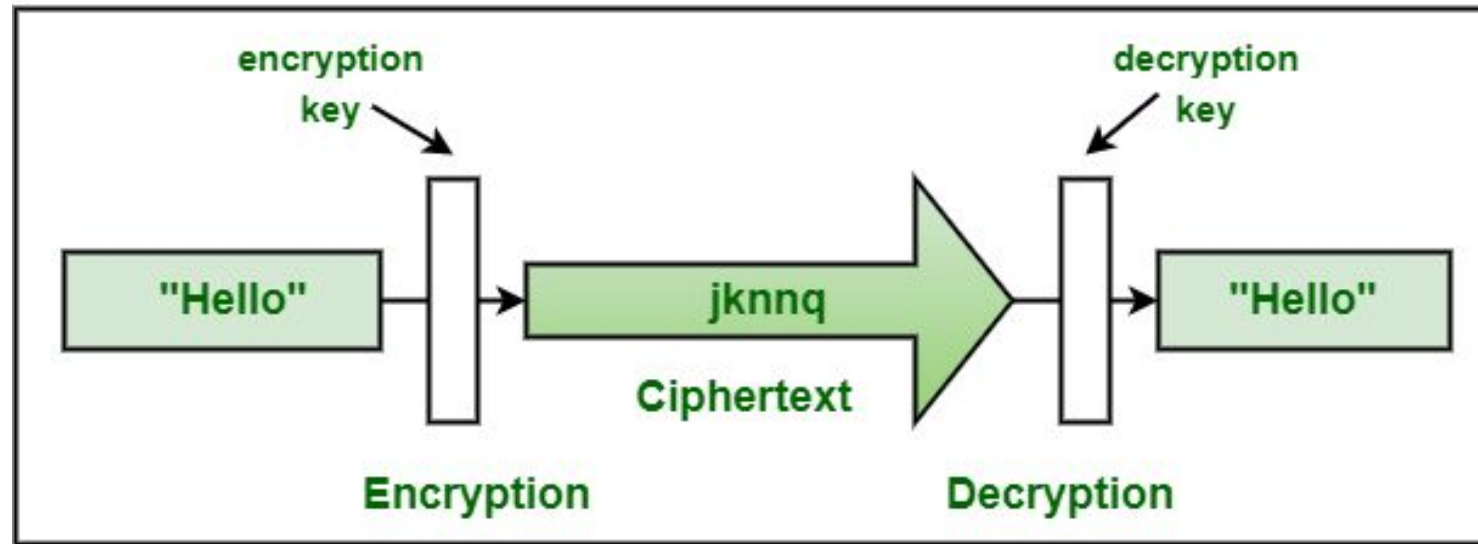
For example: by keeping just the key secret instead of the entire data secret when it is being stored or sent.



1964, Indonesia

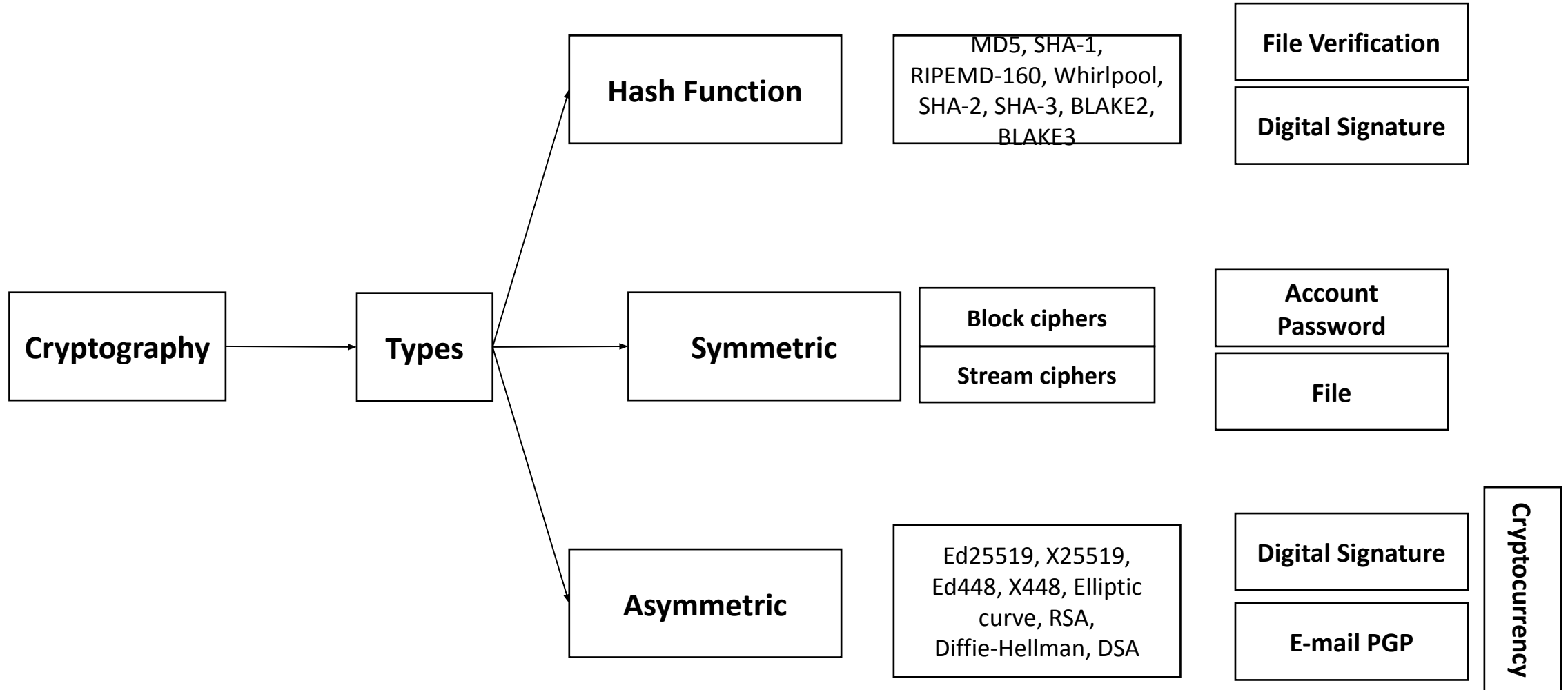


**dr. Roebiono
Kertopati**



hiding ← **Cryptography** → **writing**

Image from:
<https://geeksforgeeks.org>





Hashing



Plaintext



Hash Function

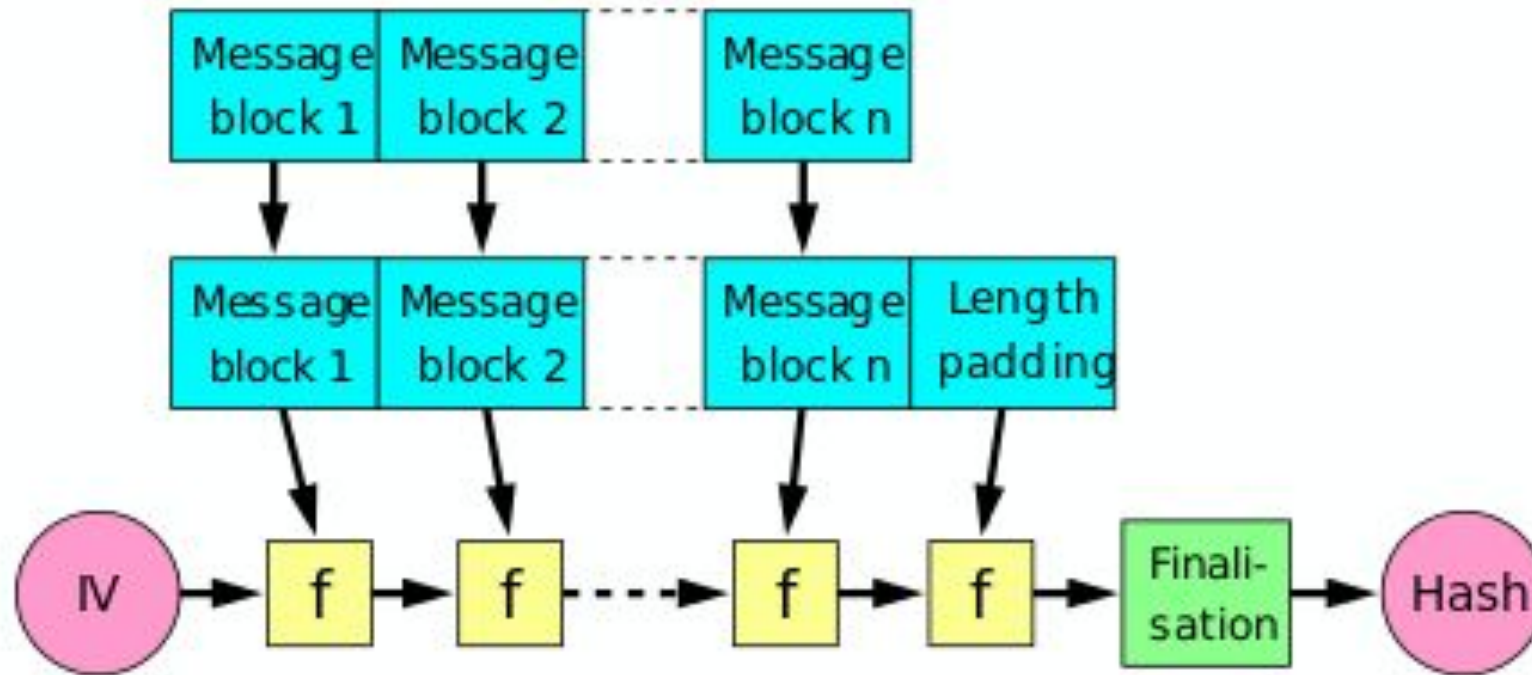


Hashed Text

Image from: <https://adilkazani.com>

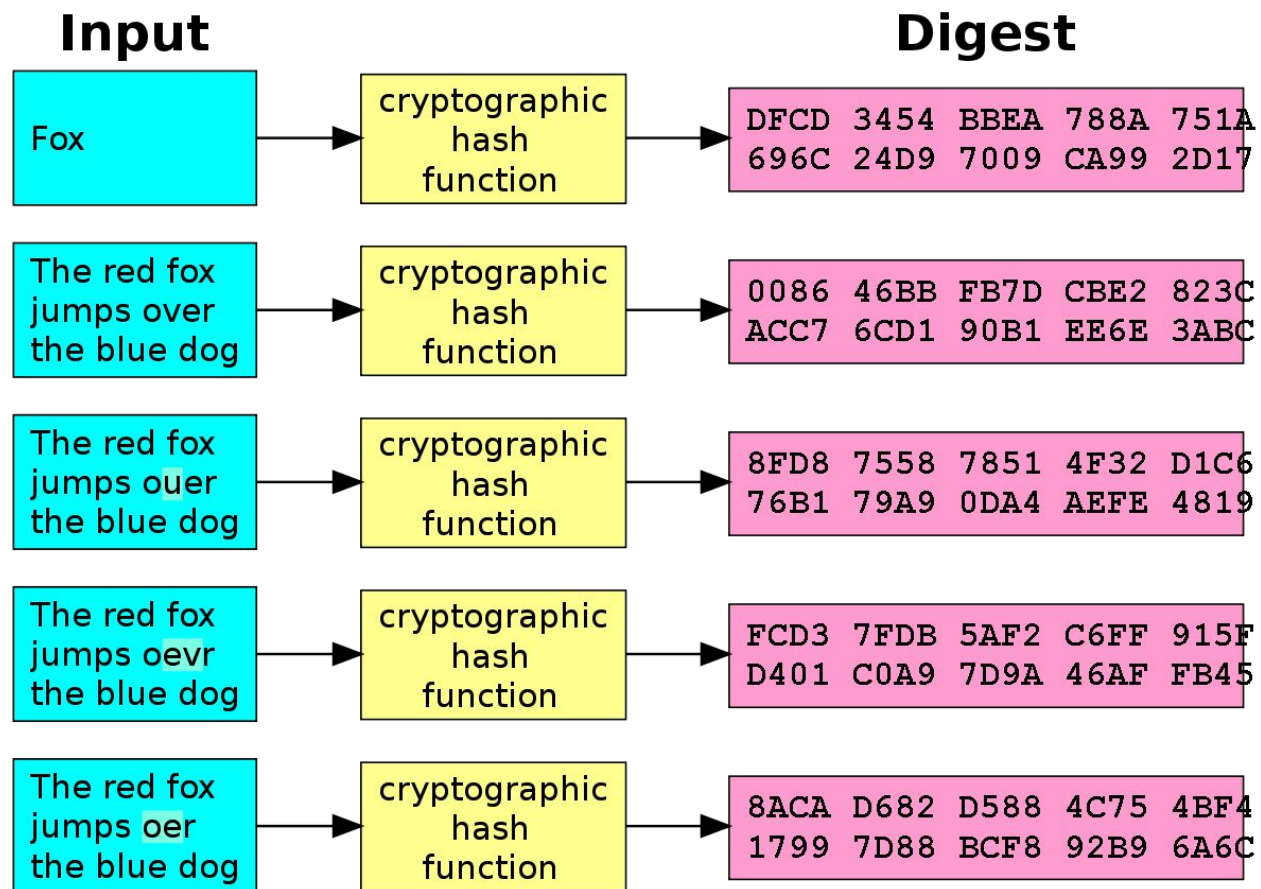


Merkle–Damgård construction





SHA-1





Is Hashing and Encoding the Same technique?

They will both transform data into another format.

Encoding is reversible (public algorithm), hashing is not preserve the integrity of data.



Symmetric Encryption

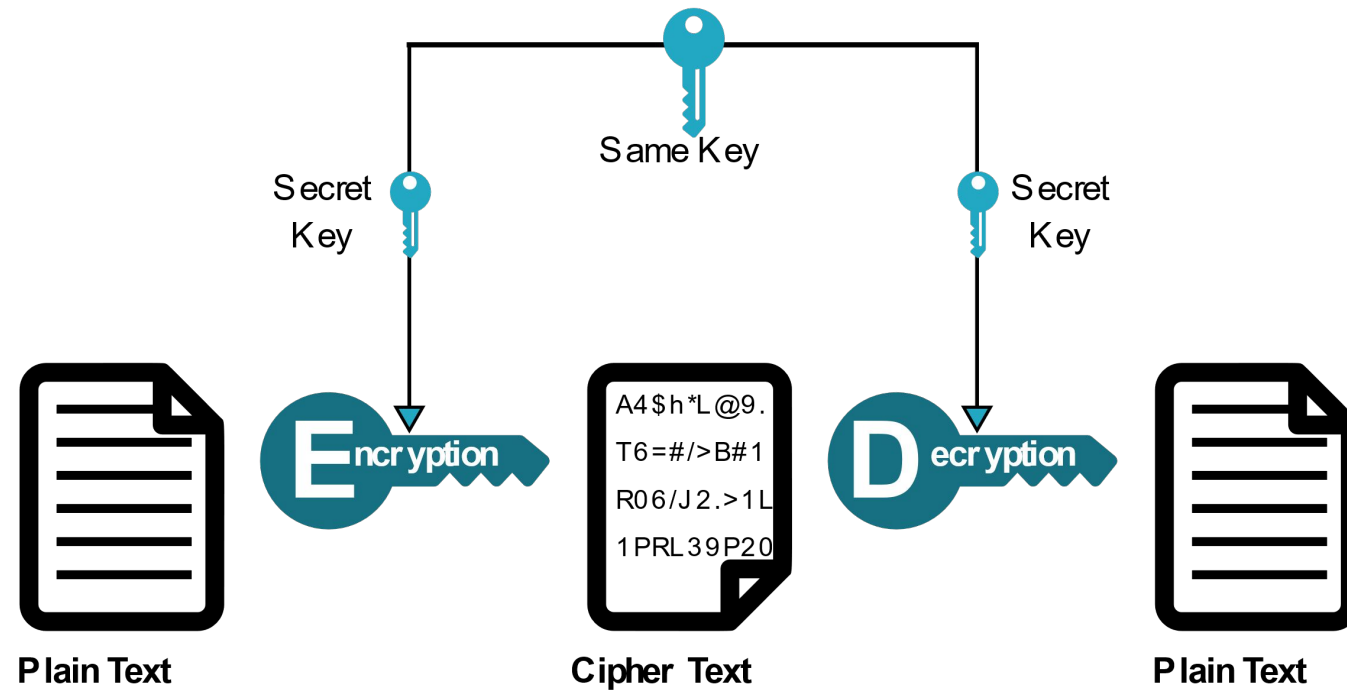


Image from: <https://aboutssl.org/>



Caesar Cipher

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA



Asymmetric Encryption

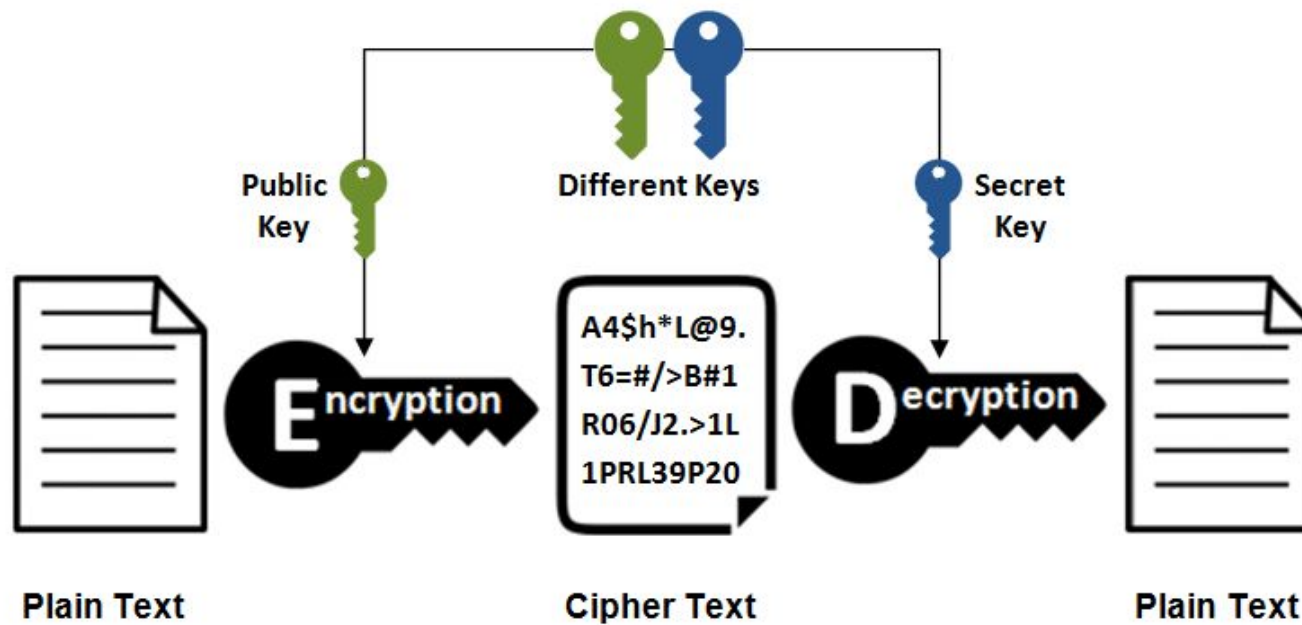


Image from:
<https://selembardigital.com>



Generate New Address

Print

Public Address



SHARE

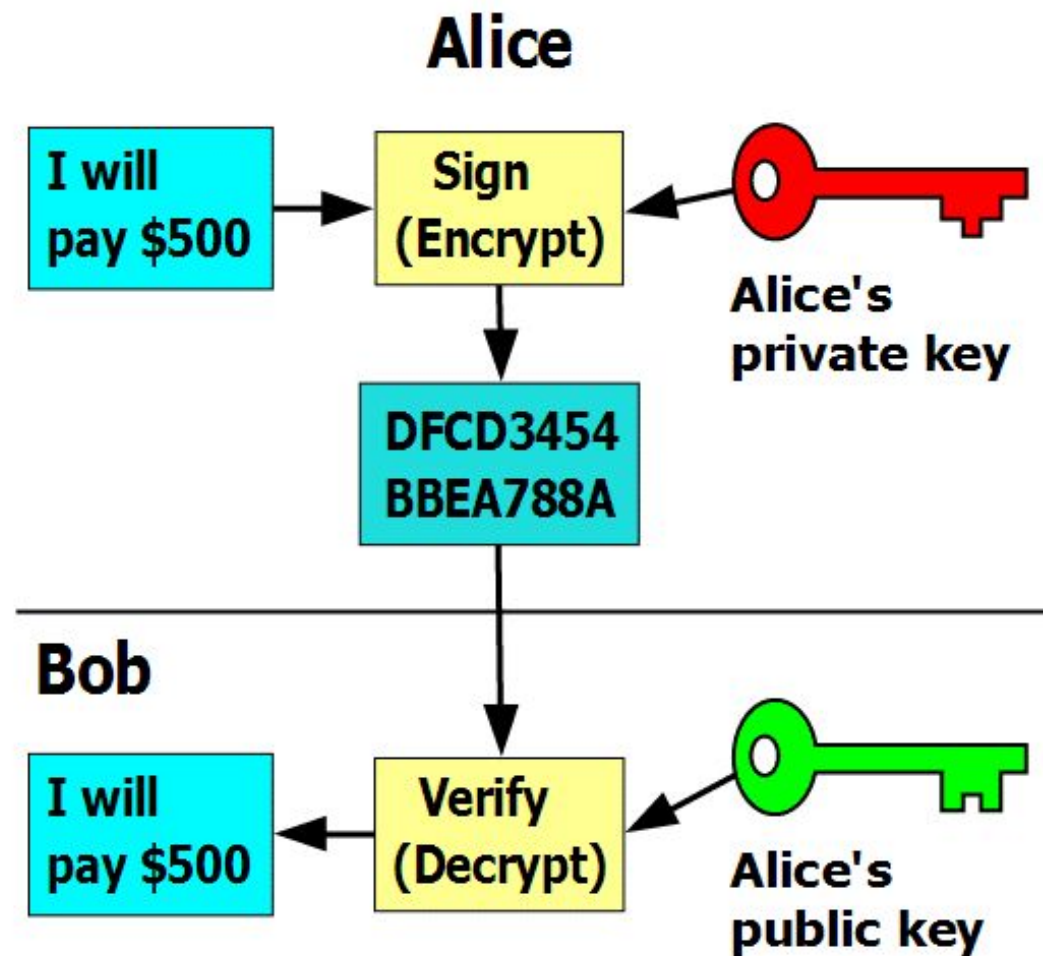
16NZD9iBCbj8NwWrDZnnyw[REDACTED]

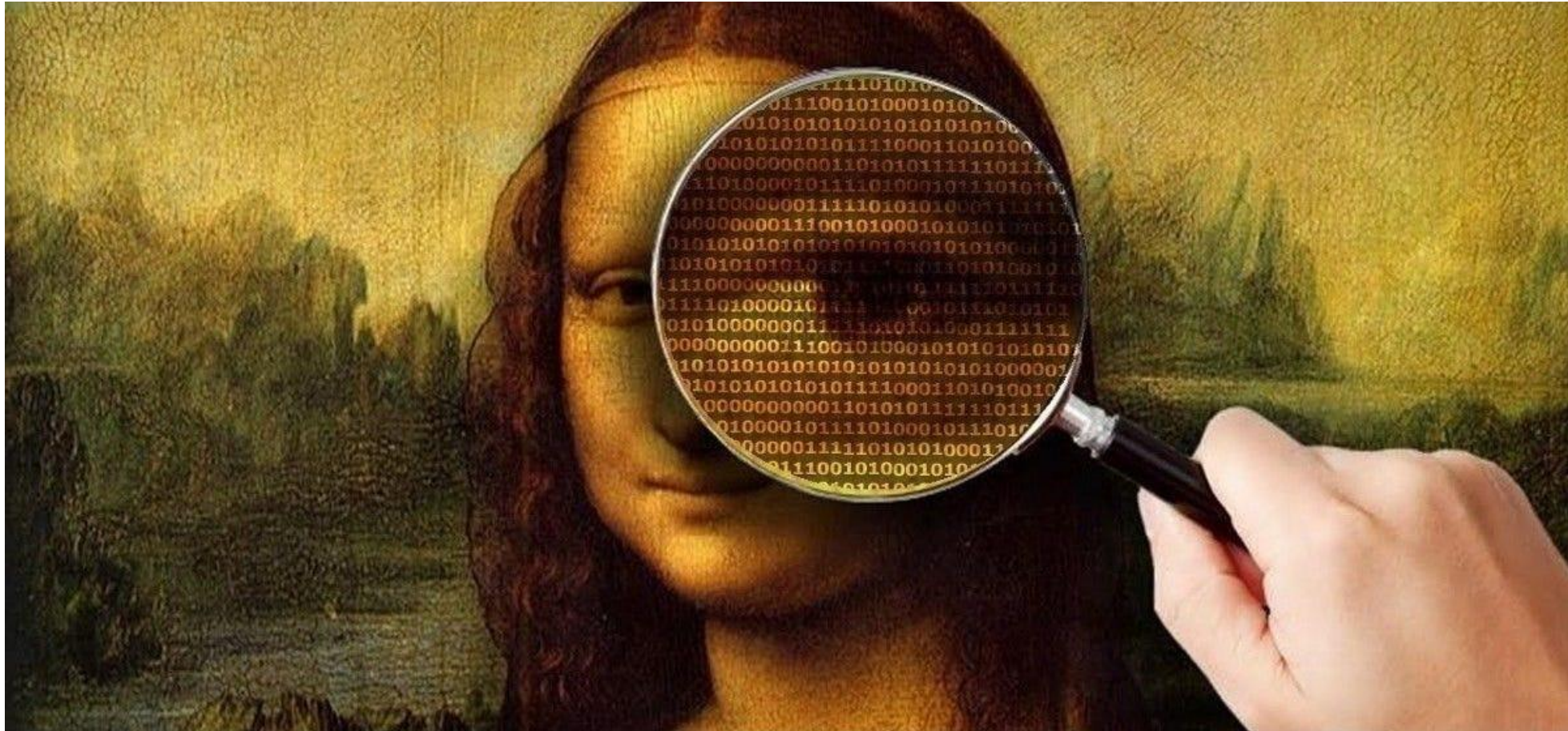
Private Key (Wallet Import Format)



SECRET

5JAG4cZ2JzQMezBd53z[REDACTED]GG7f5vaEuXgyFfH3DiSg







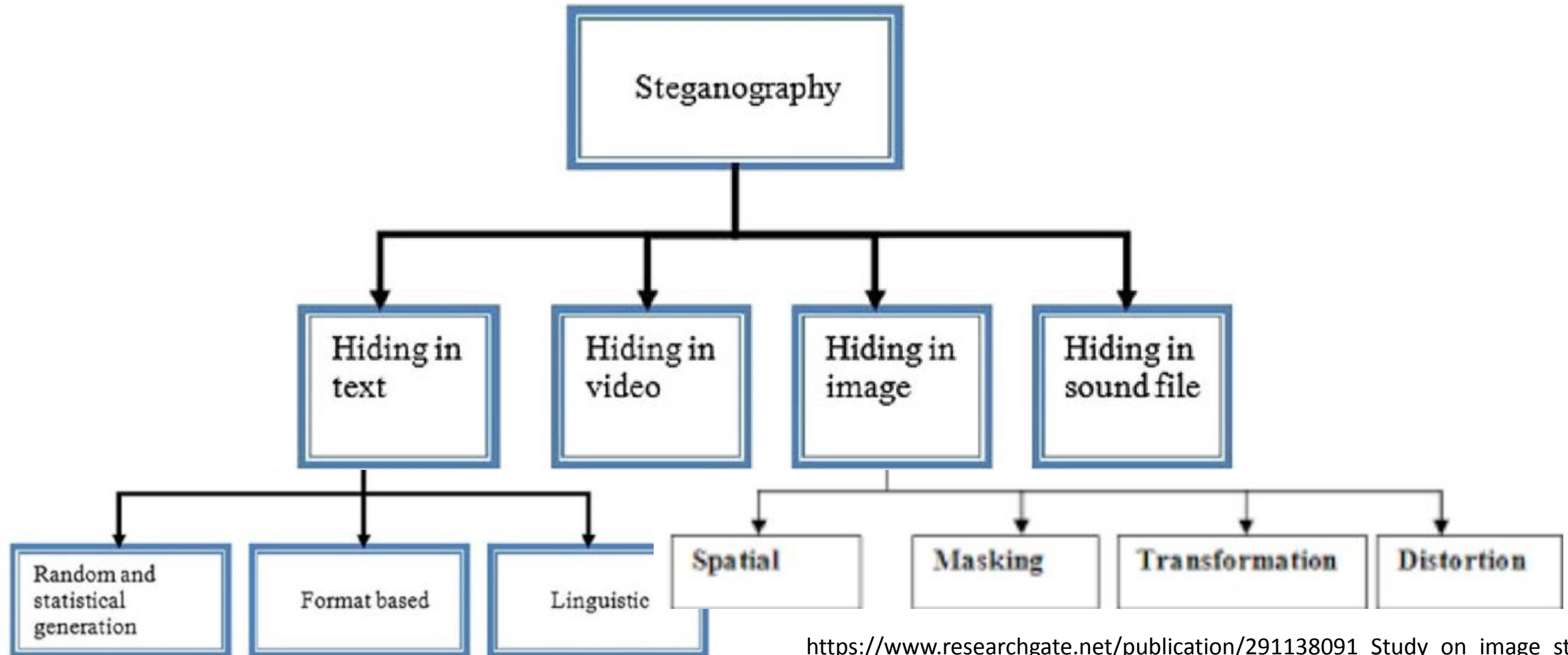
Yup, it is Steganography!

Covered or
concealed



writin
g

Whereas cryptography is the practice of protecting the contents of a message alone, **steganography** is concerned with concealing both the fact that a secret message is being sent *and* its contents.



<https://www.researchgate.net/publication/311772678> AH4S An algorithm of text in text steganography using the structure of omega network

<https://www.researchgate.net/publication/291138091> Study on image steganography techniques



ini adalah azzam

Result

S



Encode

Binary representation of your message

01101001011011100110100100100000011000010110010001100001011011000110000101101000001000000110000101111010011110100110000101101101



Result S



Choose file download.png

Decode

Hidden message

ini adalah

azzam



Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked (yet another layer of protection).

*(David Kahn, penulis buku **The Codebreakers - The Story of Secret Writing**)*



- Computer Security Principles and Practice Third Edition, William Stallings and Lawrie Brown, Pearson, 2012
- Introduction to computer security, Matt Bishop, Addison Wesley, 2005
- Computer Networking: A Top Down Approach 6th edition Jim Kurose, Keith Ross, and Addison-Wesley
- <https://www.ericsson.com/en/blog/2021/7/cryptography-and-privacy-protecting-private-data>
- <https://selembardigital.com/pelajari-semua-tentang-cryptocurrency-kriptografi-bagaimana-cara-kerjanya/>