KRIPTOGRAFI DAN STEGANOGRAFI

Program Studi Informatika

Sesi 2 – Perbedaan Kriptografi dan Steganografi

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

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

- Selain melakukan penyandian dengan kriptografi, informasi juga dapat diamankan dari *unauthorized access* dengan menggunakan steganografi.

- *Steganography*: ilmu dan seni menyembunyikan pesan rahasia ke dalam media lain sehingga keberadaannya tidak terdeteksi.

Ledakkan bom pukul
20.00 WIB

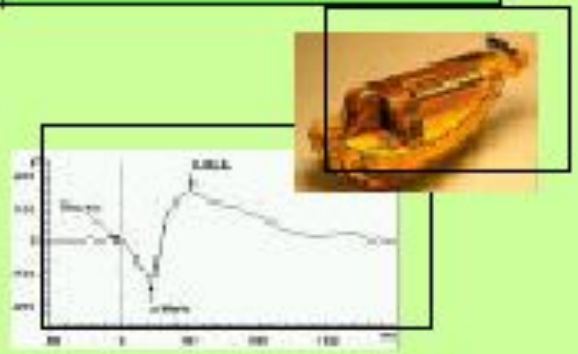
Perbedaan Kriptografi dan Steganografi

- Kriptografi: menyembunyikan *isi* (*content*) pesan
  - Tujuan: agar pesan tidak dapat dibaca oleh pihak ketiga (lawan)

- Steganografi: menyembunyikan *keberadaan* (*existence*) pesan
  - Tujuan: untuk menghindari kecurigaan (*conspicuous*) dari pihak ketiga (lawan)

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

George obtains oranges yet eights' are rubbish!



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

hIwDIwFpbAtjdf0BA/9KBX2jS17O5SRQsu2PF
caBqUXIQdyt1Fri/Wsg+eXoYsxnJI1Cn2JD7vjl
F2GH8GEr/vGQk8SQVCMyXzfPkgW0tr6RJX
AEIFF9rjnDB3kOmmVc1adrTQnLrqiC/I5r/kUs
ezowgZI82T/QVk59YsuChd+Ce8vqI/kICeqmv
w9J2amre3uxpWIOqCEQNzZyHx8HeYPf29k
Xu+uk1gekZZVdELmLD/Wa/xBKFTNUBrI+16
ewoQBxQ8+3cTXSIGPTqdzDSasgQG17Z1sr
/Lhu0qzem64GYY0OukeiGPvhHJQuXZn2UW

Steganografi Digital

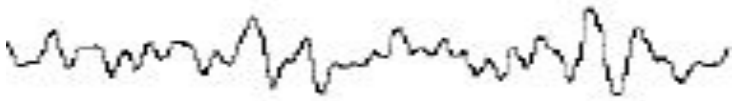
- Steganografi digital: penyembunyian pesan digital di dalam dokumen digital lainnya.
- *Carrier file*: dokumen digital yang digunakan sebagai media untuk menyembunyikan pesan.

1. Teks

"Kita semua bersaudara"

- Txt
- doc
- html

2. Audio



- wav
- mp3

3. Gambar (*image*)

- bmp
- jpeg
- gif

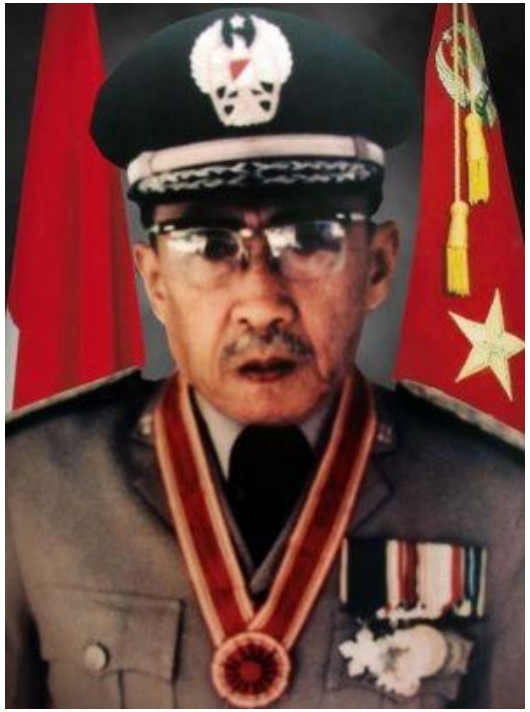
4. Video

- Mpeg
- avi
- dll

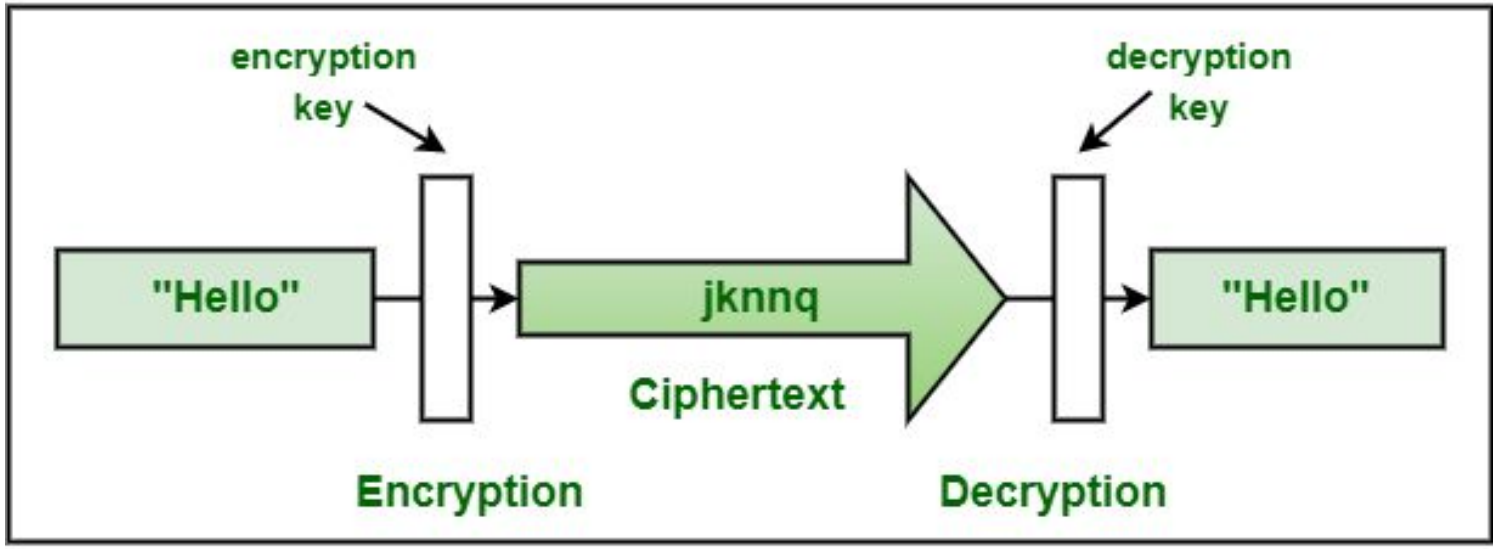
cryptography doesn’t ‘solve’ protection issues but hopefully turns them into more simplified problems.

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



Cryptography

hiding ← → **writing**

Image from:
https://geeksforgeeks.org

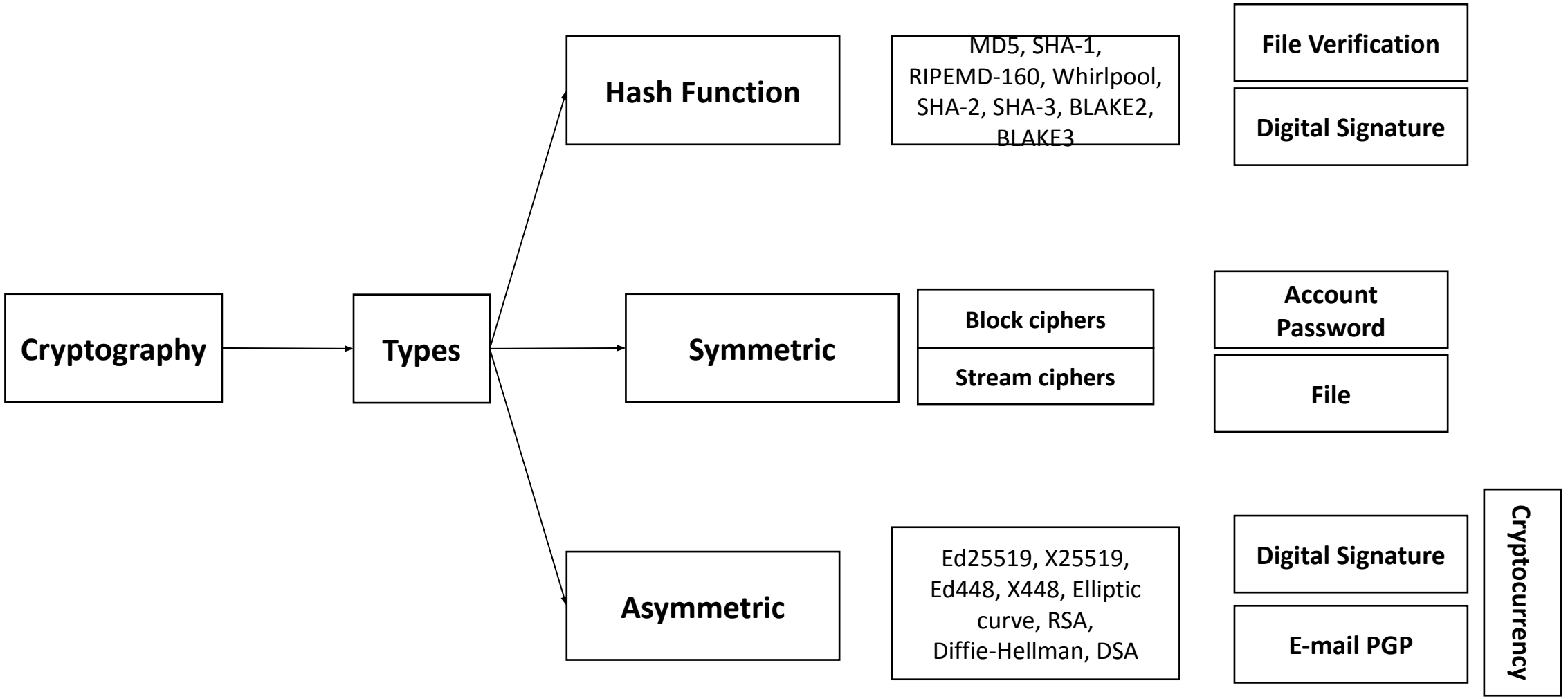
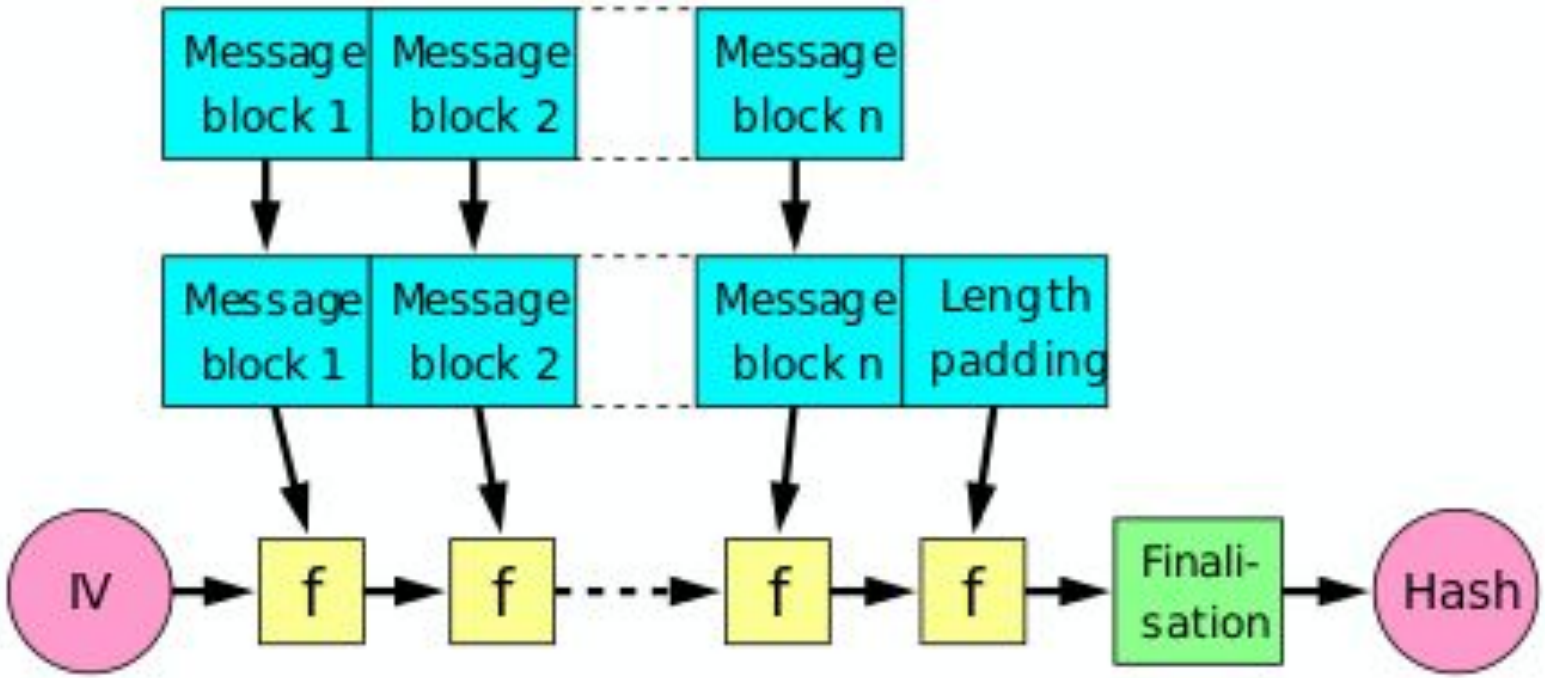
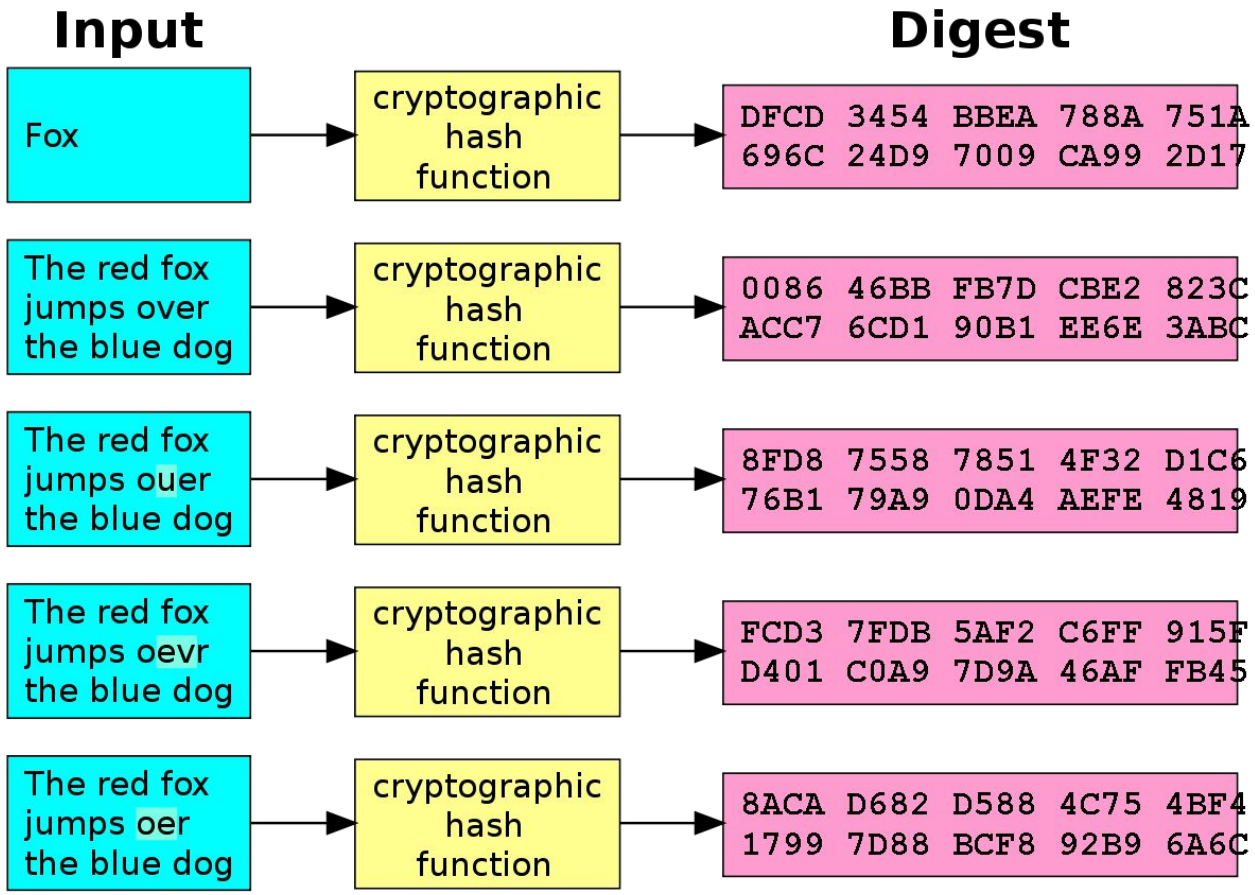

Cryptography
Types
Hash Function
MD5, SHA-1, RIPEMD-160, Whirlpool, SHA-2, SHA-3, BLAKE2, BLAKE3
File Verification
Digital Signature
Symmetric
Block ciphers
Stream ciphers
Account Password
File
Asymmetric
Ed25519, X25519, Ed448, X448, Elliptic curve, RSA, Diffie-Hellman, DSA
Digital Signature
E-mail PGP
Cryptocurrency

Image from: https://adilkazani.com

Merkle–Damgård construction



SHA-1


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C

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

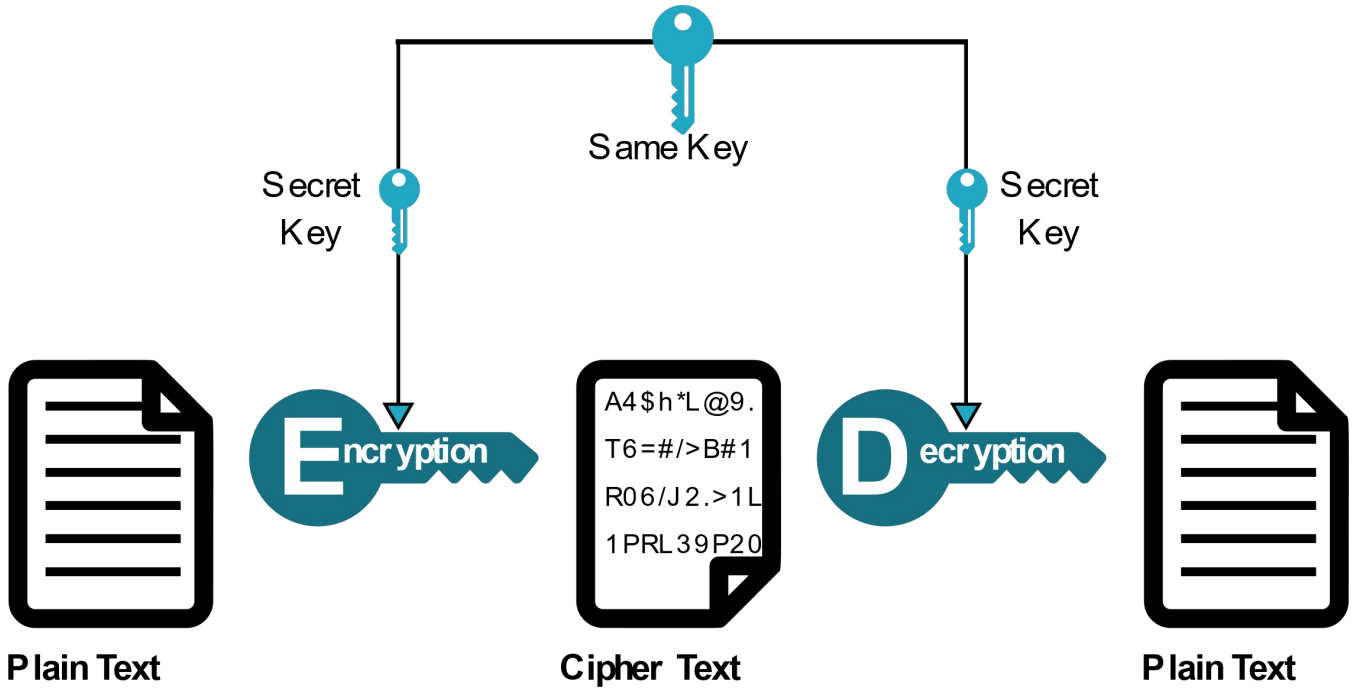


Image from: https://aboutssl.org/

Caesar Cipher

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext:  ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```

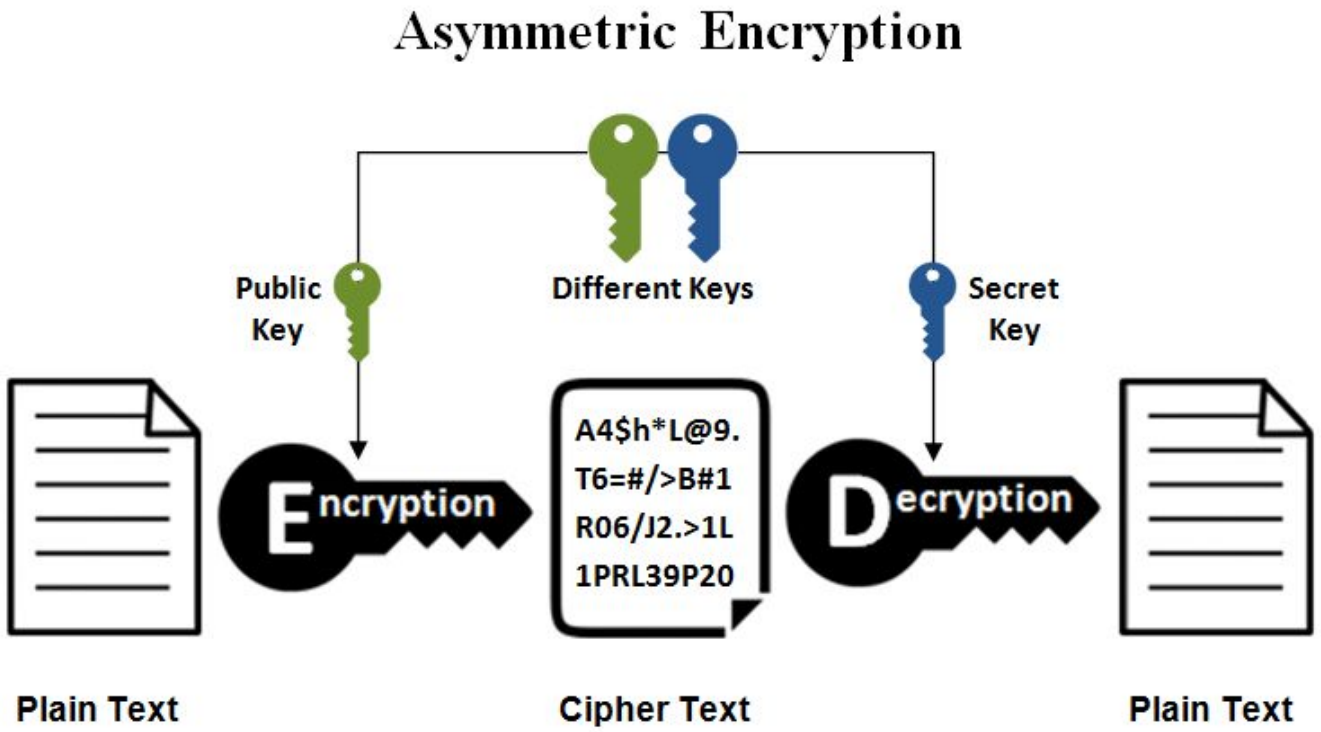
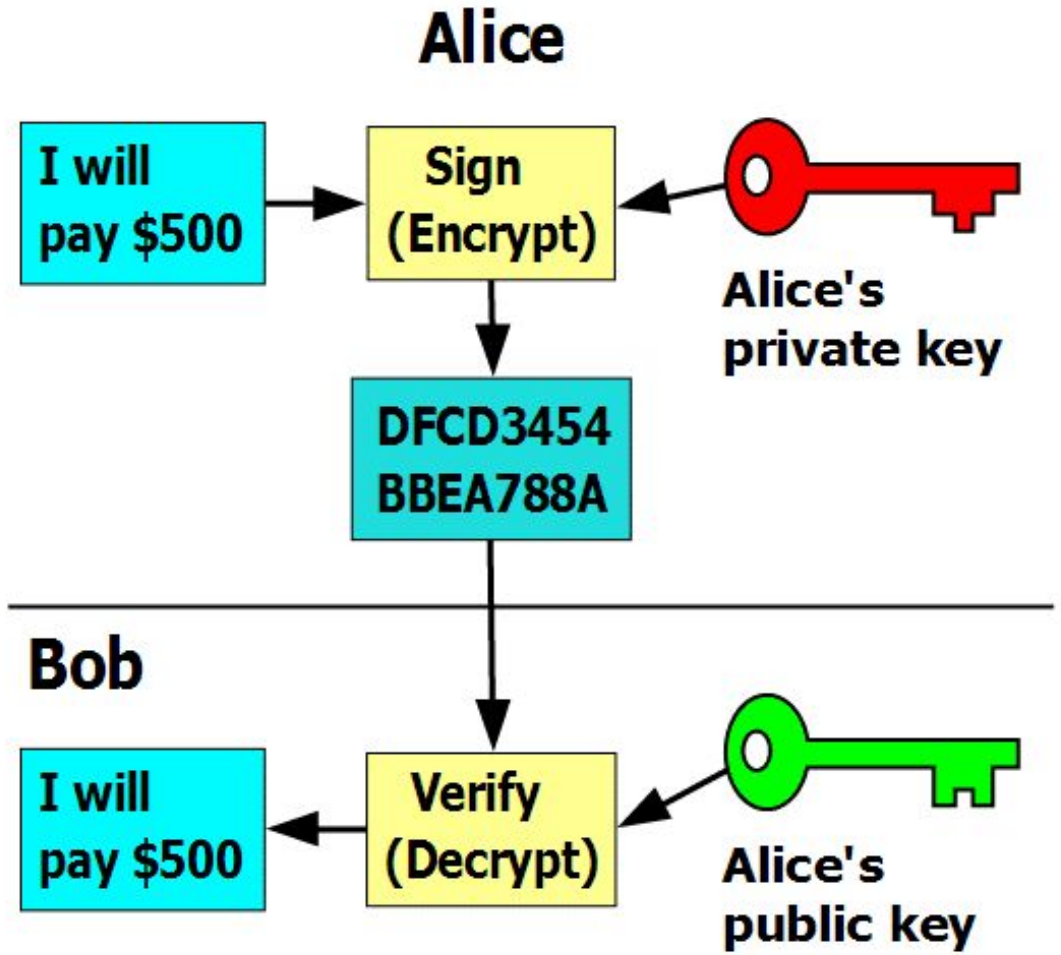
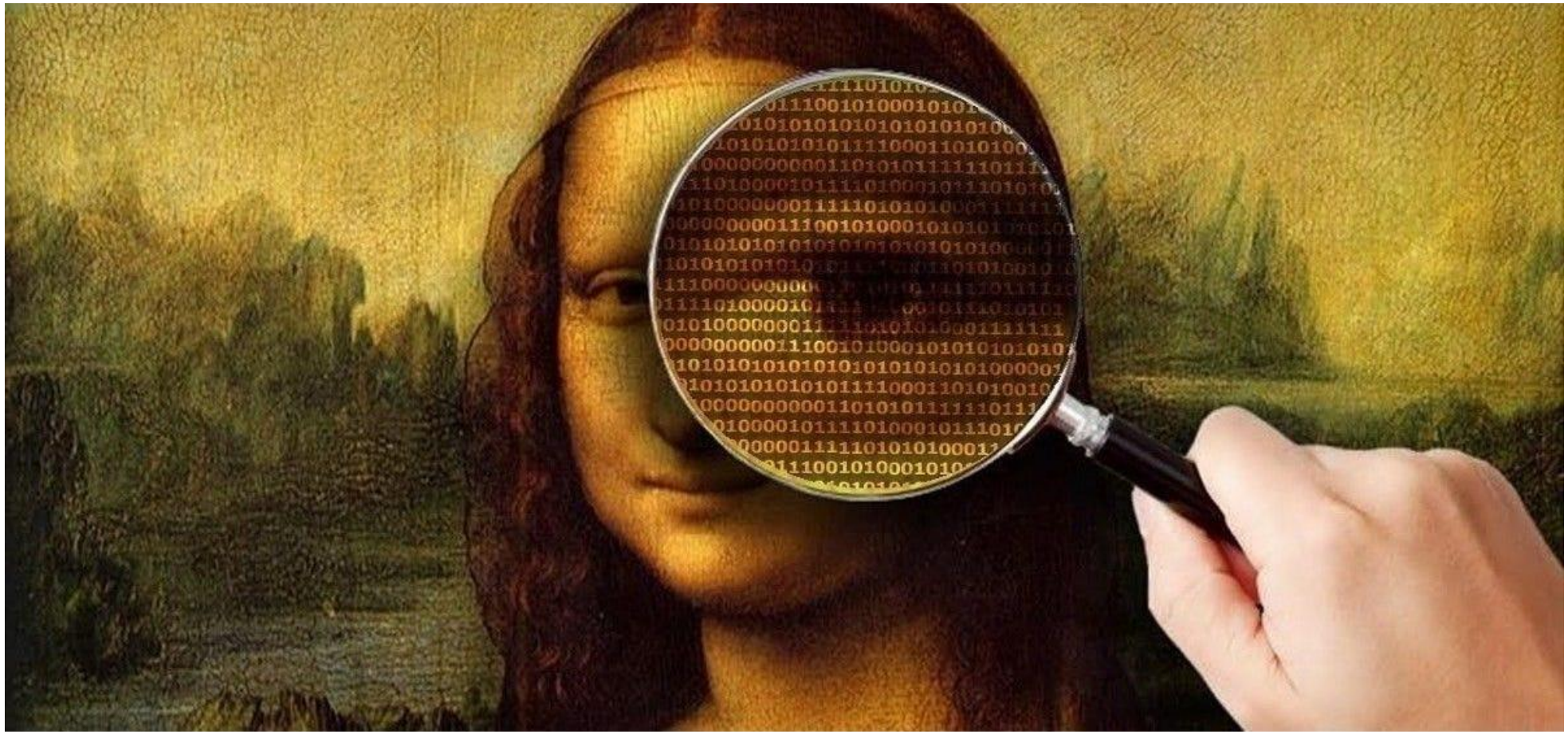


Image from:
https://selembardigital.com

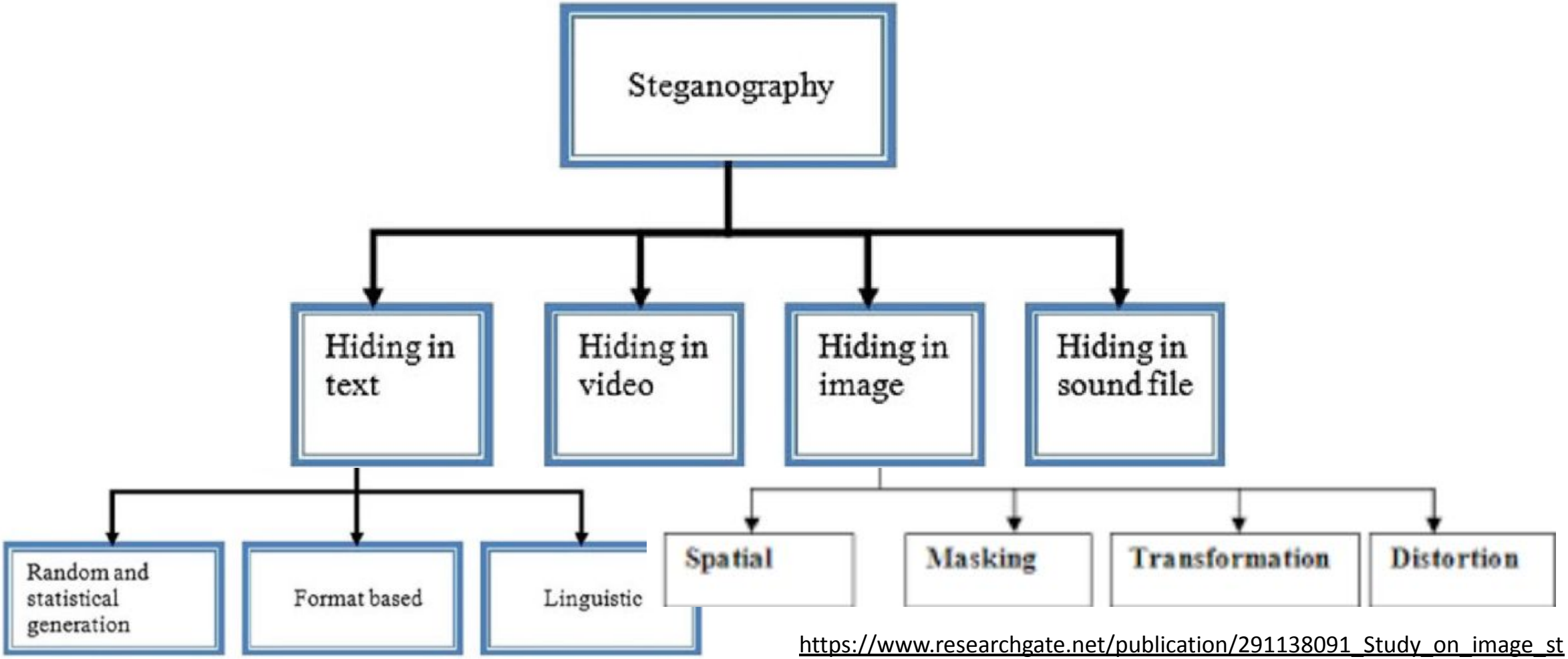
Generate New Address
Print
Public Address
SHARE
16NZD9iBCbj8NwWrDZnnyw
Private Key (Wallet Import Format)
SECRET
5JAG4cZ2JzQMezBd53z
GG7f5vaEuXgyFfH3DiSg


Alice
I will pay $500
Sign (Encrypt)
Alice's private key
DFCD3454 BBEA788A
Bob
I will pay $500
Verify (Decrypt)
Alice's public key



Yup, it is Steganography!

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

Results

ini adalah azzam

Encode

Binary representation of your message

01101001011011100110100100100000011000010110010001100001011011000110000101101000001000000110000101111010011110100110000101101101

Results

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/