STEGANOGRAPHY

Basic idea → information hide / covered writing.

It is the practice of concealing messages / file / image (i.e, any type of information) within another file, message or image / video.

Note → Later, we will extract it at its destination.

It is derived from Greek words steganos meaning covered or concealed. & graphia which means writing.

IMP

(*) Steganography is different from cryptography but, using both together can improve security of the protected data/info. and prevent the detection of the secret communication.

In cryptography, we make the data unreadable (by encryption)

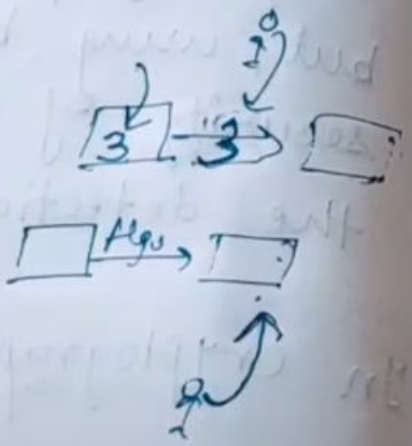
In steganography, we are hiding the existence of data.

data.

Various forms of steganography are :

1) Text Steganography
2) Audio "
3) Video "
4) Images " (hiding the data in the img. file)

∴ in short steganography can be used to hide/conceal any type of digital content (including text, img, video, audio).

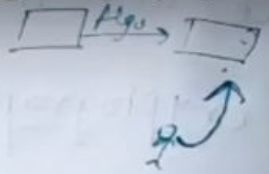


ganography,
erts confidentiality
and authentication.

DIFFERENCE BETWEEN

CRYPTOGRAPHY	STEGANOGRAPHY
It is a kind of known communication.	It is a kind of hidden communication.
It is a technique to convert the secret msg into an unreadable form.	It is a technique to hide the existence of communication
It alters the overall structure of the data	It doesnot alter the overall structure of the data
Key is necessary	key is optional but if used, provides more security.

result obtained



eganography,
ports confidentiality
and authentication.

It alters the overall structure of the data

Key is necessary

The final result obtained is called ciphertext

Attack → cryptanalysis

Once, it has been discovered, no one can easily get the secret data.

more popular approach

It doesnot alter the overall structure of the data

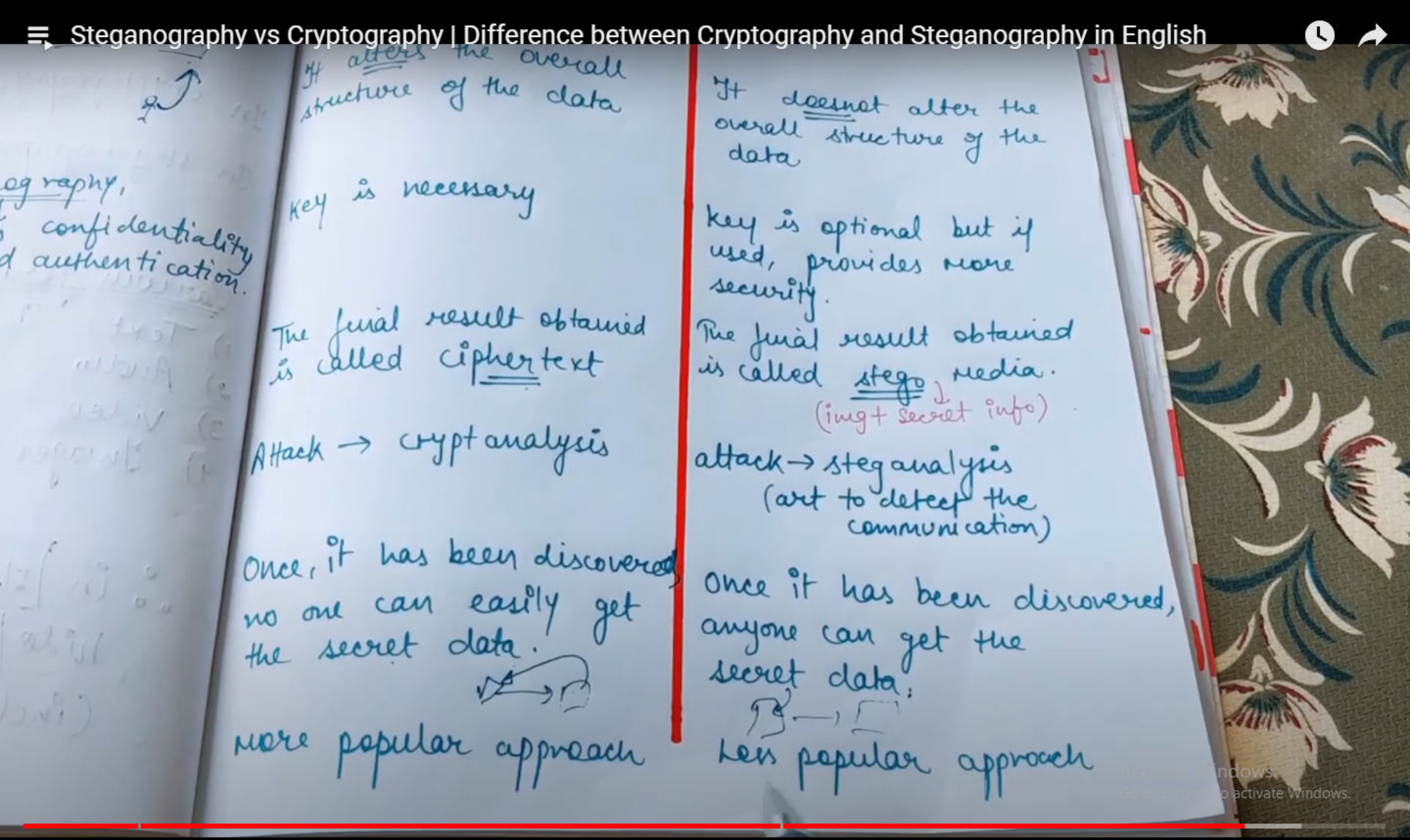
Key is optional but if used, provides more security.

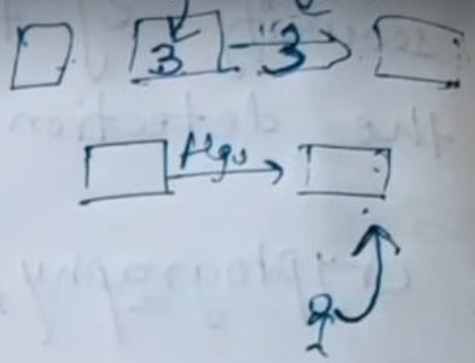
The final result obtained is called stego media.
(img + secret info)

attack → steganalysis
(art to detect the communication)

Once it has been discovered, anyone can get the secret data.

Less popular approach





In cryptography, we have confidentiality, authentication, data integrity and non repudiation

In steganography, it supports confidentiality and authentication.

unrea

It alters structure

Key is

The

is

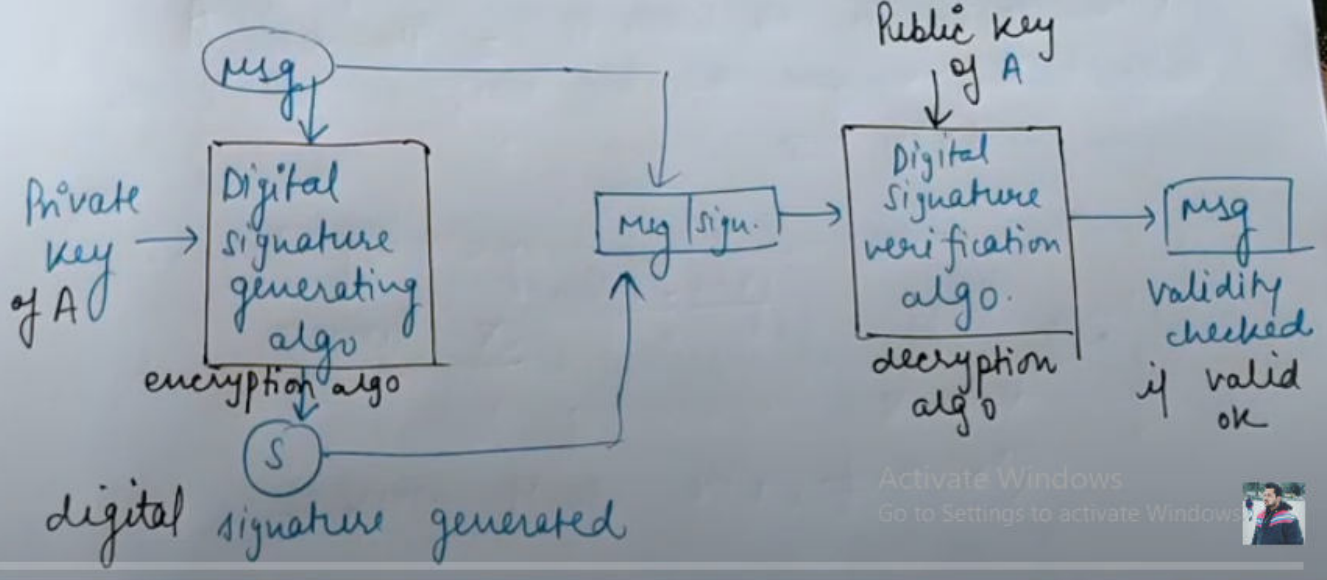
Attack

ll give you
Ri
ecember

B

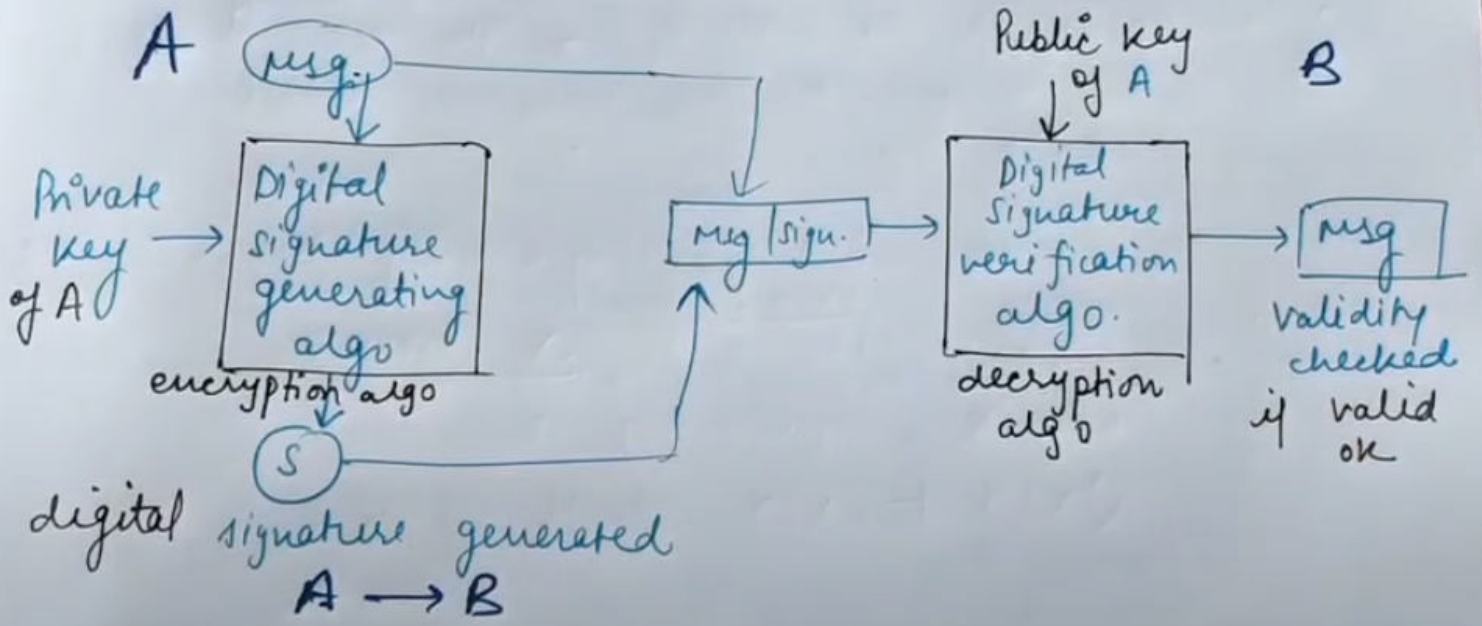
Digital signature

→ vimp role in e-commerce, online transaction, etc.
→ based on asymmetric key cryptography
encryption → private key
decryption → public key
→ used for msg authentication & non repudiation & msg integrity
→ not used for confidentiality



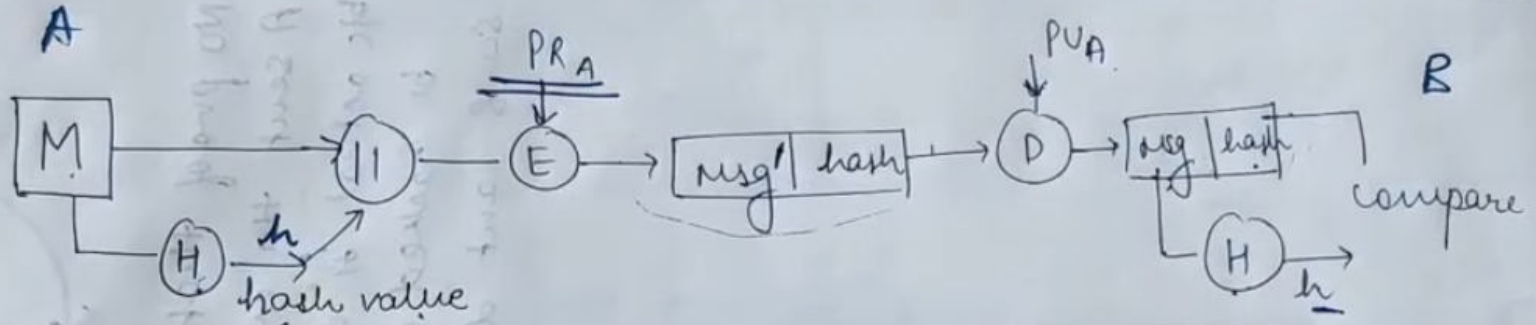
decryption → private key
decryption → public key

→ used for msg authentication & non repudiation & msg integrity
→ not used for confidentiality



→ also provides msg integrity
b/c if msg changed then at receiver

∴ private key of Alice is used.
∴ authenticity achieved.

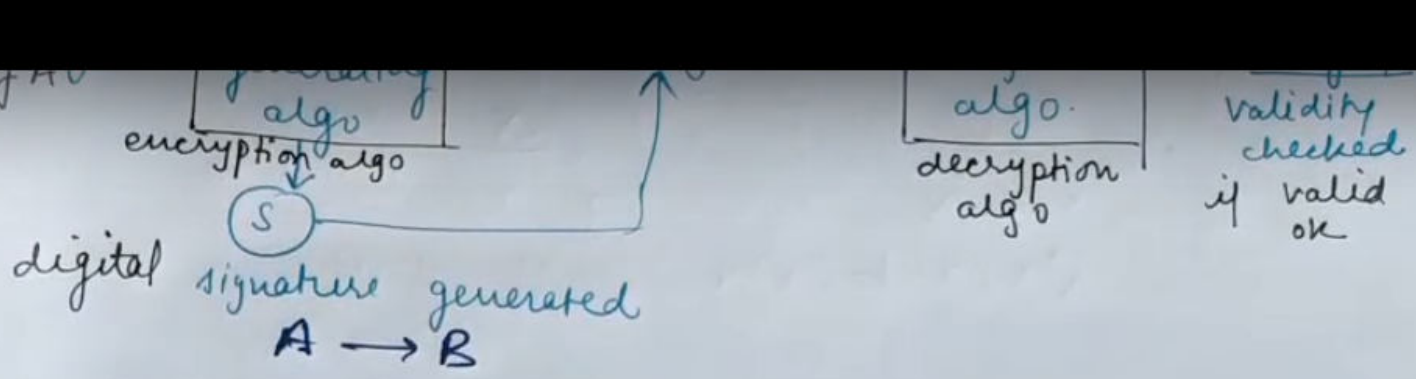


general concept of digital signature

H → hash fn
h → hash code
|| → append

Note → The signature must use some info. unique to the sender to prevent both forgery & denial.

Digital signature



→ also provides msg integrity
b/c if msg changed then at receiver side, we will not get the exact msg.
↓
achieved using Hashing concept using msg digest / hash values

Note → When we sign a document digitally,
= we send the signature as a separate document.
Sender sends 2 docs → msg & signature.

Non repudiation
achieved by using a trusted 3rd party

pg 351
pg 352
confidentiality

Digital Signature

→ signature must use some info unique to the sender, to prevent forgery & denial.
→ It must be easy to produce digital signatures.
→ " " " " to verify & recognize " " .
→ we need (i) key generation algo → to generate private key
(ii) Signing Algo i/p → M and Private key, o/p → Digital sign
(iii) verifying algo → using public key & sign.