

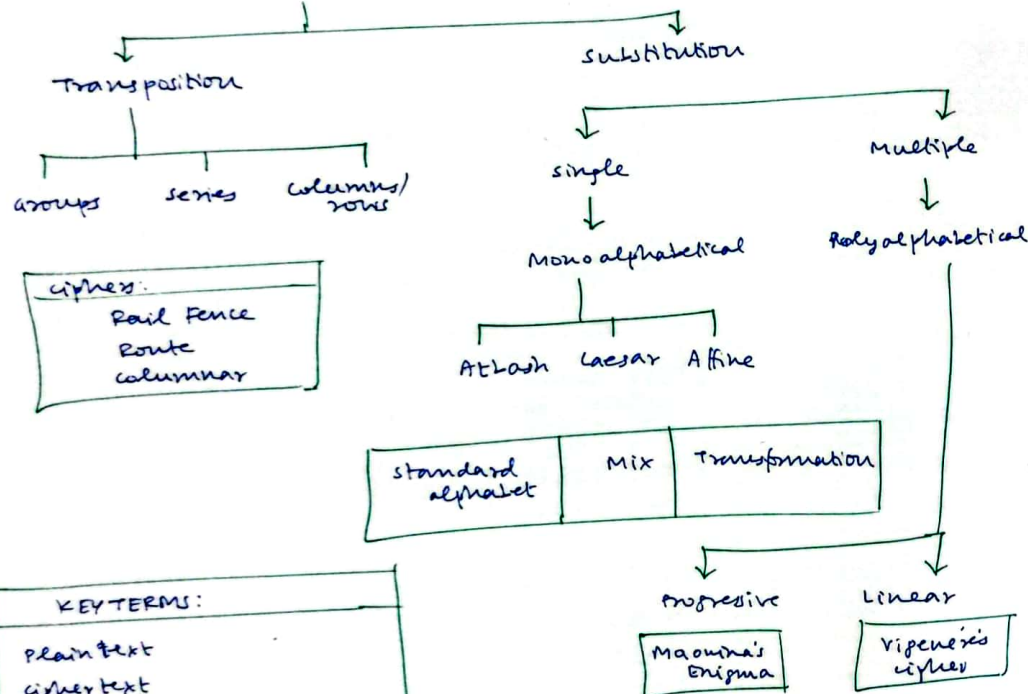
CRYPTOGRAPHY

OBJECTIVES

CONFIDENTIALITY	INTEGRITY	AUTHN & AUTH'Z PROOF OF ID	OBFUSCATION SENSITIVE DATA	NON-REPUDIATION ORIGIN & DELIVERY
-----------------	-----------	-------------------------------	-------------------------------	--------------------------------------

METHODOLOGY

CLASSICAL



ciphers:

- Rail Fence
- Route
- columnar

standard alphabet	Mix	Transformation
-------------------	-----	----------------

progressive

Maumina's Enigma

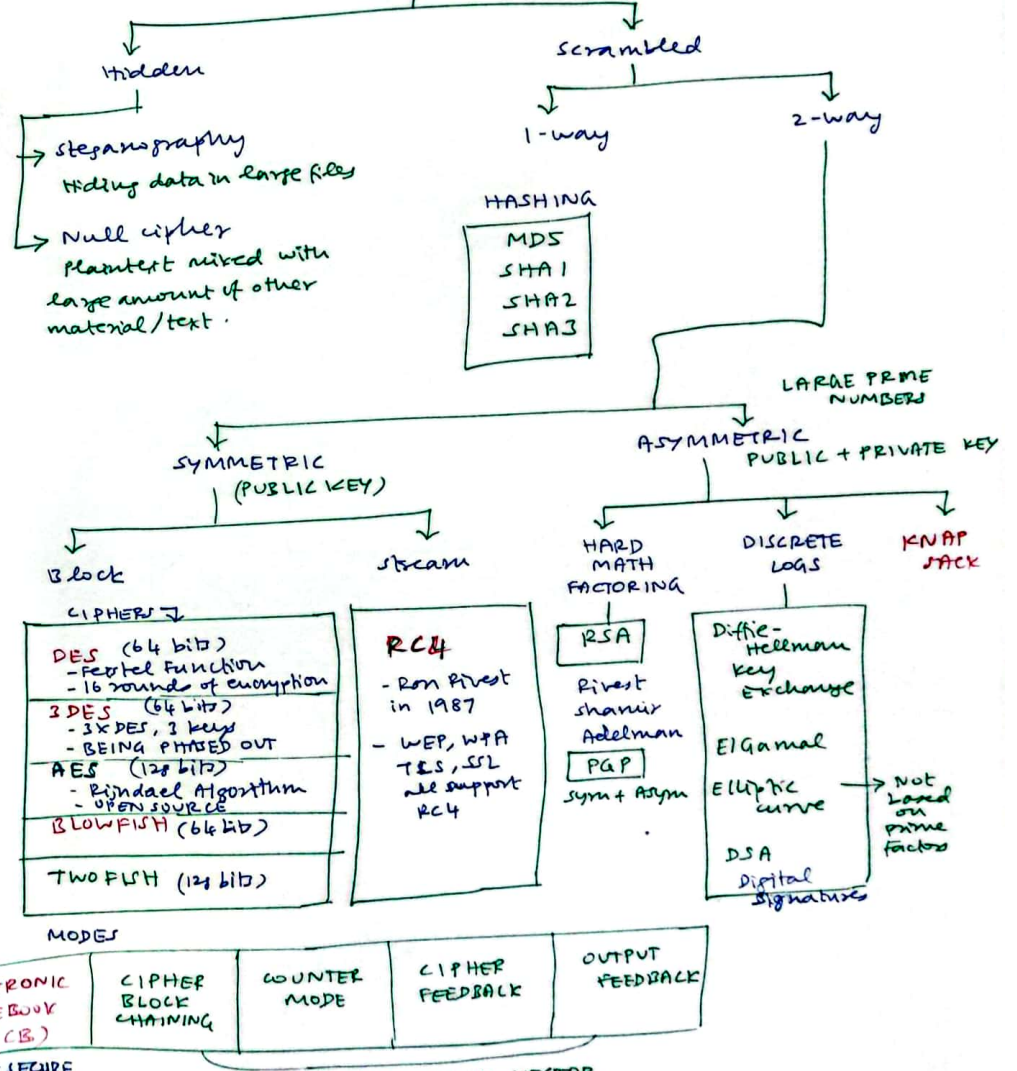
Linear

Vigenere's cipher

KEY EXCHANGE

out of land	In land
- meet outside	- Diffie-Hellman
- Face to face	- key escrow
- USB drives	- HSM

MODERN



MODES

ELECTRONIC WORKBOOK (ECB)	CIPHER BLOCK CHAINING	COUNTER MODE	CIPHER FEEDBACK	OUTPUT FEEDBACK
---------------------------------	-----------------------------	-----------------	--------------------	--------------------

LEAST SECURE
BUT FASTEST

USES INITIALIZATION VECTOR.

KEY TERMS:

Plain text
cipher text
key/cryptovariable
Encryption
Decryption
Work factor
Initialization vector
confusion
Diffusion