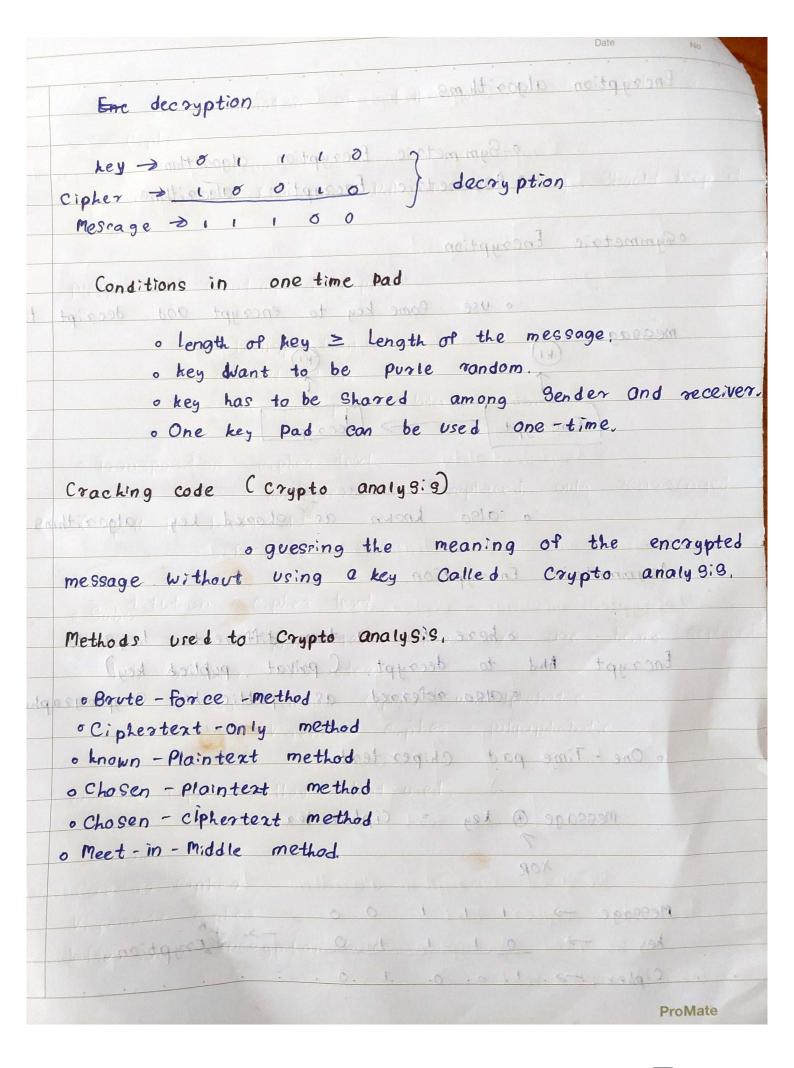
Cryptography CICS) - Lec or · Cryptography meoning Converting am message to a Unrecdable format is called Crypto graphy. decrapt Encrypt meggage original Services can be archeived by Cryptography. · Authentication · Integrity · Confidentiality that code acit cogenost baptages has perfored poly acardeted onin as (Ashersond 19) Happy than original message - dear text, plain text the leading the start plant to the start with a start of the start of Plain text photodalouda Decryption. Encryption · We need encryption algorithm to convert a plaint text to cipher text, · We need decryption algorithm to Convert a pr ciples text to plain text. ProMate

Combination of E.A and D.A is Called as Cipher. o Cayptogangly medicing Sourcestages each E.A and D.A was a key. Should keep it Secret. Enersyl (missen Methods of creating a Cipher. Transposition by detailed has persone o Substitution. Punta maindon o One - time pad. - later will learn will One key pade con the wed propostations o Transposition cipher text. - no letteres are replaced only rearrenged. (Spell it backward). treg : LOES + 3DESDE DE DE DE DE DE LA PROPERTIE DE DES o Substitution Cipher text of a spoon betaging - Plane text characters are being replaced With another character. Eg: Caegar Cipher monoalphabatic Vigenere cipher, - polyalphobatic. Langer - Plaintext melestapes (19) asityposas Variouse cipher methods that used. Scytale Mille meller trail Caesar Cipher mell copte astquesas been sul Vigenere cipher Jefferson's encryption device **ProMate**

Francis	Olace No
enc syption	algorithms,
	o Symmetric Encryption algorithms.
v = (8) 42 - 10	Agymmetric Energption algorithms.
	9001116 2000 PRESIDENT
Symmetric	Encryption.
and the state	Conditions in one time had
	o use some key to encrypt and decript th
message.	ten that to be shared a gooden
han not	o key has to be shared amana the
(E	ncrypt > decript
	Caretrag code (coupto analysis)
	o also known as shored key algorithms
the enc	to guesting the coloning of
o Agymmetr	rie Encryption, and a paint traited some
Encoupled,	Inestinger ciples 1851
r .	o here use a two different key 9 to
thcrypt	And to decrypt. Cprivat, public key) o also referred as public key Cryptographi
	bottom who testes of
a One -	Time pad Chiper text 11000 to the angle
o one	o chasen testarate models
Mess	sage 1 key = Cipher tex
	o Meet in middle method
	XOR
We	
Me99ag e	→ 1 1 1 1 0 0
Me99age	\rightarrow 0 1 1 0 0 \rightarrow t_{ec}^{n} t_{ec}^{n} t_{ec}^{n}



			Date	No
- 0- 10 Com	mod4 1	· · · · · · · · · · · · · · · · · · ·		,
o Brute-force	Attacker tries	011 0000:11		10
untill find the		au possible	metro	1 3
on the That The	Any message	is vulnerable	to ho	rute-force
attack.	ring mestage	vointe vointe		
· vac e.				
<u> </u>				
				71.1