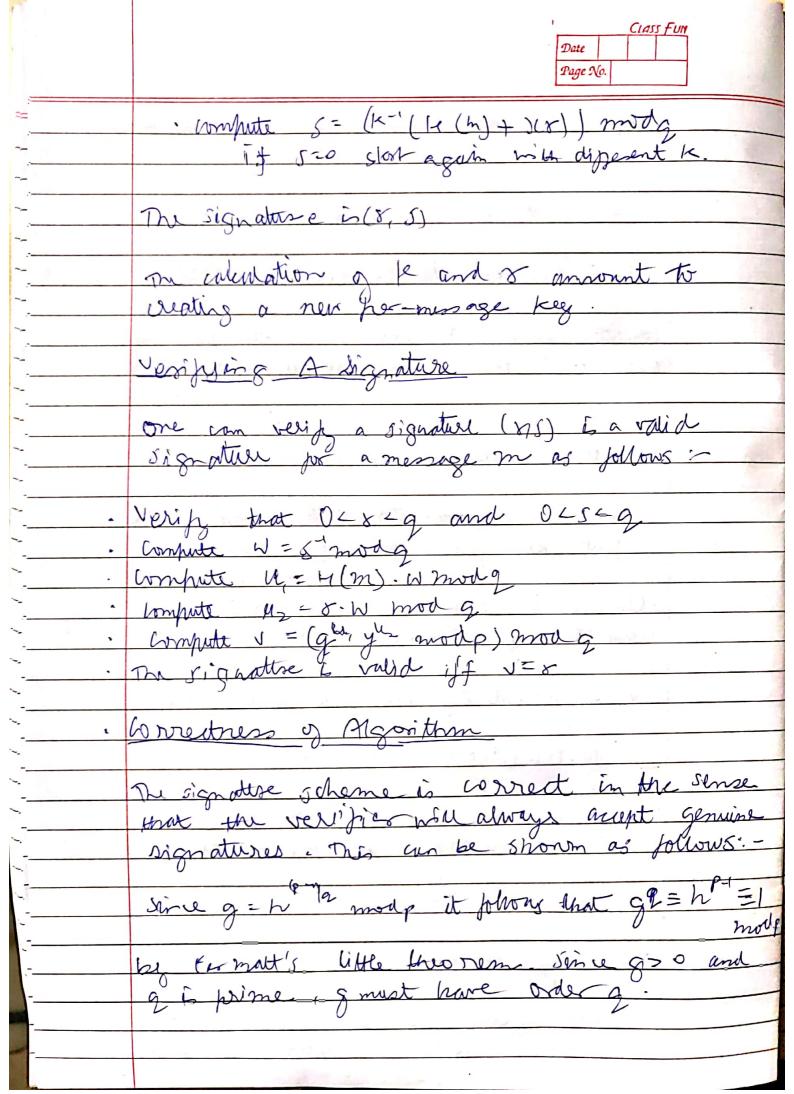
	Date Page No.
- 1	Chopse modulus fungth N such trox NEL
	moore N'ist prime q
1	grove in tiger h fandonly from 2, p-23
	complete q = h 1/4 mod p. In the rare case
	compute $g = h^{(p-1)}k$ mod p . In the rare case that $g = 1$ they again with diperent h
, JA	
-	Per User key
	i to set or hagemeters the second phase
1	computs key-pairs for single uses.
	· Chrose ar in leger je sandomly from 21 q.B. · Compute y = gr mod p
-	and the state of t
	It is private key and y is presic key.
	ky Distribution
	The signer should publish the hublic keep of signer should keep the private key of signet.
14	Signing
<u> </u>	A menorge m in signed as follows:
	· (more integer & xandomly from \$1



3	Class Fun
	Page No.
	Tige 50.
	The signer computs
100	
	5=k-1 (4(m) + xx) 2nd g
	Trus
7	
5/2	K= H(m)5-1 + JUSS-1
VA Y	= hem w + dow bond gs
7.00	
	Since of has order of mod p we have
1 1	H(m)W a SLAN
	gk = gH(m)W g SL8W = gm (h)w g = gm ayuz mod p
	5 m, y 8
	= g g = mon p
1 -	Ei all the concertnes a osa lathours land
	Finally, the woodtness of PSA Jollows from
	8 = (gk mode) mode
	= (g k modp) modg = (g u g u2 modp) mod g
	=V
	a particular of a contract of a
1.60	
44	