Submission Hundout PAZ

			10)
	Subject : Ulen	Ket palpheten t	Server Ket Public Key
AP.			Server Ks+ Public Key Ks- Private Key
protoco l		Encrypted Nonce General	toh GORG
		Encrypted NONCE	S) (S) ALS (S)
	ķ.	M-44K, (Nonce)	
		Give me certicuteoryned by CA	470 house
		by CA nicute signed	>
Der	hypted	CHANIE	
	ation e)	terrequire very	
extr	all Ks'	V	NO113/11/11
COM		If there early consecur	mean (Many)
che	egiral to	If the Ch arrived	13/7 - 53/7
	nance	Handshake the Cla	>
		Handshake the file upload	

Sensity loophole of AD problem solved:

The loophole is that an intruder can record and send the message back to the givent and act as the server if the user always sends the some message / unencaypted message. A nonce generated will be able to solved this preplay attack.

CPI protocol Subject : Mignif Server Kst publickey Nonce private Key K (Nonce) - need cert DET KST cert (heck H failed close connection (blyck) sugged. Serd Delryptusing after last cluse connections CPI protocol K& publizhey Server client Nonce Ks private keey session Key K-(Nonce) Symmeth Need cert cert Decrypt get Ket, chilewhnedian geneater, Kct(K) pery pt mengks, K(fillerome), K(b) send files last file sent, close connection (A)

