	Page
	C33-1AT-2
92)	8)
a T	re SSI/TLS pandshake involves a
slie	s of stops through which both the parties at and server, varidate each other and
Clien	it and server, validate each other and
start	one communicating through the secure 851/71
Ju	
2 A	TIS nandshake takes place whenever a
u	1 navigates to a mebsite our HTTPs
and	the browner first begins to guny, the mebsited origin where
Stop	mebates organis wirver
(3) DI	ving the course of a PLS Landshake, a client and sorver together will do the
tu	1r[[h.d]]
	i) specify which version of TUS will be used
	will be used
	ii) Decide on which cipher suites
	ii) Devide on which cipher suites they will use
	III) AUTHURITIONE THE IDENTITY OF THE
	server via the server's public key and-the SSL certificate authority's
	and-the SSL certificate authoritys
, M	digital signature
	14) Generate lession Ruys in order to
	une symmetric energiption after the hardstake is complete.
	hand shake is complete.

E PROPERTY IN	Rebecca Dias 182027/19	Classmate Date Page Representation	
	9-TAI - 22) /O COO		
		(8 1 4 9	
North Con	1. Client sunds hello, cip and client random	hu suite	
217 \ 121	Client 2 the server landom & 851 certificate SS		
	LOHURA	SOME SOME	
T Ag	The 4. Pre-master Key general	Ald T. A. O.	
	client using public key	5. The server	
	sst cutificate o pre-prested key deco	THE REAL PROPERTY OF THE PARTY	
	SSL certificate G. Pre-muster key deco	dient certifiate	
aut I	Lather the property of the same of the same	The Wall Control of the Control of t	
	7. A martin key of marten-		
4	secret is in place non		
- U	8. This master ky is a encryption I decryption	sed for	
DIA	the withness and shortnesstar (U)		
KET.	sitting invenes and our courses		
	and the SSL certificate author		
4	SSL Hand 8 hake	frocess.	
	14) Generate Lessin trup in orde		
astr.	the symmetric sounding ofthe		
	ford data is saviplate		