

PARSHWANATH CHARITABLE TRUST'S A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



	Academic Year: 2023- 2024 .
	Subject: C85
	NEEDHAM - SCHROEDER AUTHENTICATION PROTSOCOL: NEEDHAM - SCHROEDER AUTHENTICATION PROTSOCOL: Weense an wisewise
	NEEDHAM - SCHROEDER Secure as
	NEEDHAM - SCHROEDER AUTHENTICATION PROTIOCOL. The west a communication posolocol to secure an unsecure
	communication.
	There are a types:
	* NS protocol with symmetric key.
	* NS berotocol with daymine
	(1) NS protocol with symmetric hard honce - Randonly generated
	Server String which is valid on by
	de sometime
	aleman actives
	New order 2
	Nessage 3.
	Machine Message 4. Machine
1	A Memory B
	A→ Machine A. B→ Machine B.
	KAS -> Symenetric key known only to An S.
	KBS -> Symmetric key known only to B nS.
1	
	1 a all I a ammunicalità
	KAB -> Symmetric key (cor) session gkey wed for comme
	between A and B.
	Message 1: A -> S: {A,B, NA }.
	1 2 to S, telling the server she
	A tachigies mersey and so by charing NA.
	Message 1: A -> S: {A,B,NA 9. A identifies herself and B to S, telling the server she wants to communicate with B. by sharing NA.
	S -> A: INA, KAR, BYKAR, AY, Y
	S -> A: PNA, KAB, B&KAB, AgkBS J KAS key to B.
	Subject Incharge: Prof. Sarala Mary Page No. 4 Department of CSE-Data Science APSIT

PARSHWANATH CHARITABLE TRUST'S



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

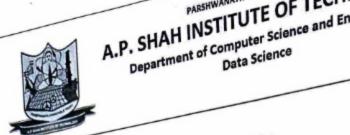
Data Science



7	Academic Year: 20 93-20 29
Semester: VI Subject: CSS	wanted Kan with Key to B.
* 8 sends KAB to A and also	energy
* All are encupted using Kas	her and
* All are encrypted using Kas an * A will decrypt using Kas an send encrypted key to B.	d get RAB for are
send energipted key to B.	
Mossages A -> B : 1k A4kas.	
Bwill deught wing KBs	and get KAB.
Now both A and B got 1	YAB "
V	· · · · · · · · · · · · · · · · · · ·
Message4: B - A : ENBY KAB. *B will encupt his nonce v	alue ustrig
*B proves hinself to A. *A decrypt No using KAB h	Par necesveel.
*B proves him young KAB W	hich she has
* A decuypt IVB	
Message 5	
A->13: &NB+19KAB.	have herself to AB.
This step is performed to	sammunicates that she holes
She has verified Band she	prove herself to AB. communicates that she holds
the same key.	

A.P. SHAH INSTITUTE OF TECHNOL Department of Computer Science and Engineering





Academic Year: 2023-2024 -

Subject:_

KPA -> Public key of A. (A,S) KPB -> Public Key of B. (B, 5) Mss -> , Sever secret key.

known by S, A, B.

A wants to communicate with B. So A will suques! Meseage 1: A -> 8: A,B.

Bé public key forom S.

Messagea: S A: { KpB, B} hos.

-> Server sends the public key of B by encryptiong wing

-> A will decrypt using KSS and neceive KpB.

message 3: B > S: B, A

Brequest As public key from the serves

message4: S -> B : & KPA, Ag KSS.

-> Server sends the public key of A by encrypting using

-> B will deaypt wing kiss and neceive kpa-

Message =: A -> B : {NA, A} APB.

dencyptis his naunce wing public key of B.

B decrypti and necetives W Subject Incharge: Prof. Sarala Mary Page No. 3

Department of CSE-Data Science | APSIT



PARSHWANATH CHARITABLE TRUST'S

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science**



Semester : VI Subject : CS.8 Academic Year: 20 28-2024 , Message 6: B -> A : {NA, No } KpA. Bencypts NA and NB using kpA and sende to A. A decrypts and using his own private key and receives. NA, NB. In this step B has proved himself to A. Message 7: A → B: {Ne} kpp.

In this step A proves himself to B, by sending No to B.