

PARSHWANATH CHARITABLE TRUST'S

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering
Data Science



^	
Semester: Subject: Cgg	Academic Year: 2028-2024
KERDEROS:	2029
It performs the following tasks:	
* Kerberos login	
* Kerberos Ticket	
- herberd.	
(a) generale SA.	
and the cartesian series of	
100 CAX	
Ni ord and vi	N
35 30 30	
6. A sende ticket to B	
B	
7- B proves Himself.	
Stept: Kerberos logio.	
KDC -> Key Distribution Center.	
SA -> Session key of A.	
TGT - Tickel Granting Ticket	
Ka -> Symmetric key of A.	
KB -> Symmetric key of B.	
to a least of the A and B.	
KAB > Session key for both A and B.	
Step 1: Kerberos Login. A Login, KDC	1
and login kno	
A - A - A - A - A - A - A - A - A - A -	word.
h[password] => KA is derived from put	he basewood
Ky is the hash value of	The pursue
Ke is known by A and KDC.	
h[password] => kA is derived from pass kA is the hash value of the kash value of th	

PARSHWANATH CHARITABLE TRUST'S



Subject Incharge: Prof. Sarala Mary

A.P. SHAH INSTITUTE OF TECHNOLOGY

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



Department of CSE-Data Science | APSIT

	Academic Year: 2023 2024
	Semester:Subject :
	Alli A logins kDC generates session key for A.
	SA is encrypted using the
	A will decupt with ka? (Receiver end)
	TGT = E ("A", TGIT, SA) -> TGIT is energyted using SA (Sen) -> A will decaypt using SA and get TGIT (Receiver end). Slep 4: Request
	=> At will decrypt using SA and get TGIT (Receiver end).
	Slep 4: Request A gends request to TGIT => A wants to communicate with & REDUEST = (TGIT, authenticator).
	10000
	authenticalor = E(timestamp, SA)
1	= E (TGIT, & (timestamp, SA))
	KDC will decreypt using SA and will receive timestamp
	and (61).
	Steps: Reply -> kDC i'ssues a ficket to A and B. Reply = E("B", KAB, Ticket to B, SA).
	Treket to B = E ("A", KAB, KB).
	Rooly = E(B, KAB, E(A, KAB, KB), SA)
	A will decrypt with SA, he will get KAB and
	A cannot decrypt Ticket to B, because he don't have
1	Ka ·



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Semester: Subject: CSS	dent v
Sleps: A sends ticket to B	demic Year: 20 2용 20 2박 .
A -> B. (Ticket to B, authenticator).	
(E("A", KAB, KR), E Gimestamp & K	Class
1. B will decrypt using kg and ad KAB.	
1. B will decrypt using ke and get KAB. 2. B will decrypt using kap and get times Class. B prover Himself.	lamp.
Slep 7 : B prover Himself.	
Now both gol KAD.	
E (timestamp + 1 - Kag).	
B will send the timeslamp by encupting u A will decupt using KAB. B proved that he got the same session has got Now they are ready to communic	eing KAB.
A will decupt using KAB.	
B proved that he got the same session	key as A
has got Now they are ready to communic	ate.
0 0	o a sufa