PARSHWANATH CHARITABLE TRUST'S



A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering



Data Science

Semester: Subject : C&S Academic Year: 2023 2024 HMAC -> Hash Based Message Authentication Code.

* HMAC is used to mountain the integrity of the messages sent by the sender.

Notations Used:

MD -> The message digest/hash function used. (eg. MDs/SHAU4).

M -> The input message.

L-> The no. of blocks in the message.

b -> The no. of bill in each block.

K-> The shared symmetric key.

ipad -> A string collolio repealed b/8 times.

(eg) lif b = 16 bils then b/8 = 2. The string is repeated a times.

Dollollo Dollollo.

opad -> A string co1011010 repeated b/8 times. leg) if b=32 bits then b/8 = 32/8 = 4. The string is repeated 4 times.

01011010 01011010 01011010 01011010,

Sleps in HMAC:

Slep 1: Make the length of K equal to b.

Step 2: XOR K with spad to produce SI.

Step 3: Append Mto Si.

Step 4: Apply Message Digest Algorithm.

Step 5: XORK with opad to produce 82.

Step 6: Append H to 82.

Step 7: Apply Message Diget Algorifm.
Subject Incharge: Prof. Sarala Mary Page No. 1

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: Subject : ____C.C.C Academic Year: 2023-2024 . Slip 1: Make the length of k equal to b. There are 8 cases, if KLb, K>b, K=b. length of K<b Compare Length of length o-Do nothing Add obite to left of k 80 that ili length = b Hash K to reduce the length of bills Slepa: XOR K with spad to





A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering
Data Science



Semester: Subject: CS.S	Academic Year: 2003-2024
Slep 4: Apply Message Digert Algorithm.	2
Apply. Message Digert Aly.	
S1 Original Mag(M)	
H	
Slep 5: XOR K with opad to produce S2	
K X S_2	
opad	
Slep 6: Append H to 82	
S2 H	- у
Slip 7: Apply Message Diget Algorithm.	
Apply MD Algbrithm.	
1	-, At
Sa H	
Talla Ta Mareaga I	Lathentication
MAC Message +	tuthentication Code.

PARSHWANATH CHARITABLE TRUST'S



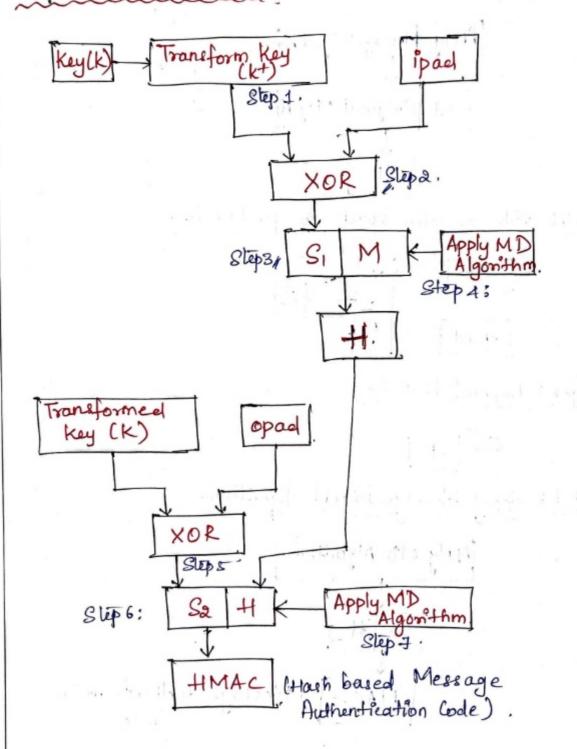
A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering
Data Science



Semester: _______ Subject: ______ Academic Year: 2023-2024 .

Complete HMAC Operation:



Subject Incharge: Prof. Sarala Mary Page No.

Department of CSE-Data Science | APSIT