

VASANTDADA PATIL PRATISHTHAN'S COLLEGE OF ENGINEERING & VISUAL ARTS

Page No._

	Experiment No. 03
	the state of the s
	Aim: Study of different Hashing Techniques: HMAC and CMAC
Sala A	TITIME ONG CITIME
	Ild beinggor off biles write Astropi
	Theory:
	OHMAC (Hash Message Authentication Cade):
	@In HMAC, a hashing function is used as a
•	MAC function to calculate the MAC value
	(B) The hashing function sold to
24,9 7	1 The hashing function could be general hash
11 4	functions such as MD5, SHA-1 or SHA-2.
	Sender Receiver
	The state of the s
	Message Key Message MAC value No Reject message
- 4	
	Hash function Message key
	15 equal Yes Accept
	MAC Value Hash Function Message
8	
	Send Message and MAC Value
	MAC
	(a) Variables Hell and the HMAC
	as follows:
	MD = Message Digest / hash function
	M = input message who's MAC is to be
	calculated.

	L= No. of blacks in the message M
	b = no. of bits in each block
1000	K = Shared symmetric key
	A A Y LAND A ME
	ipad = A string oollo 110 repeated b/8 times
12	opad = A string olollolo
	Steps -
	1) Make the length of k equal to b
4	- If k = 1 is a will ald as a many a bits
	- If k < b; we will add as many 0 bits as required to the left of k and call
	this K as modified key k*.
1 1 1 1	a the same and a second
1.5	- If K=b: no action required goto step2.
7.5	The state of the s
	- If k>b; we need to trim the k and so
	pass it through Message Digest Algorithm.
100	
	2) XOR K with ipad to produce S1:-
	K X
	0 3 51
	ipad > R
	Tpac III
	(3) A 1 M 1- C1-
	3 Append M to SI-
	(SI) + Original Message =
	SI Original Message (m)

THE LEGISLE CHEST OF STREET

VASANTDADA PATIL PRATISHTHAN'S COLLEGE OF ENGINEERING & VISUAL ARTS

Page No.____

	D Message Digest Algorithm: Now the selected message digest algorithm is applied to the output of step 3 which produces an output H.
	Now the selected message diaget algorithm
	is applied to the output of sten 3 which
	produces an output H.
	· · · · · · · · · · · · · · · · · · ·
	(5) XOR K with spad to produce Sz -
	K
1	Opad R
	(A) () () () () () () () () () () () () ()
	@ Append H to Sz:
	(S2) + H = S2 H
	(7) Massar Di I Ol III
	(7) Message Digest Algorithm!
	Now the selected message digest algorithm
	produces final MAC.
	produces timal MAC
	· Hither than the reserve to the second of t
- Try - 1-3	
	(2) CMAC (Cipher based Message Authentication
	Code):-
	G) T C (44.6 T)
	(a) In CMAC, a symmetric block cipher
	encryption function is used as the
	MAC function to calculate the MAC
	value.
	(B) CMAC 'cally II
	© CMAC is typically calculated using. AES-128 algorithm and provides strongest form of
	algorithm and provides strongest form of

