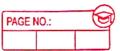
	Name: ddwait Purao
Ϋ́	UID: 2021300101
1	BE-COMPS B CSS-Batch=V
~	Exp. Sa - Report writeup
	eten:
	Steps:
2)	
1)	Select Plaintent:
3 14	m: 10101100 10001101 10100001
	00101110
	here m(lingth) = 32 l'(blacke lingth) = 8
2	Generate Inffalization Vector:
	La variation of the Contract o
	IV: 1101 0011
	in a mark marting and with the mark a cided
3)	Isx spad & opad values
	The time to make with with a fill and at month
	JV: 1101 0017
	are the seal of planting the thoronous and the
4)	DEVEde plaintext ento chunka
y	William Control of the Control of th
	m, = 1010 1100
	$m_2 = 1100 101$
	$m_3 = 10100000$
	$m_4 = 0010 1110$
5	C= + + + 112 2 2
	Compute 20 = IV XOR grad
	for chunk 1
	$m_1 = 0 0 00$
	4pad = 00110110
	KX OR = 100/10/0



c	Concatonate ell itis
	Concatenate with IV: Z, = Zoi m,
	: Z1 = 1101 0011 10011010 10101100
	•
	1001 1011 0011 0011, - =
	Compute z=11010010100110 11001101
<u> </u>	Repeat for remaining chunks
	1101 0000 0111 0101 2 20
	$Z_3 = Z_2 \mid m_3$ $Z_4 = Z_3 \mid m_4 = 1131 0311 0311 0311 0311$
	$Z_{4} = Z_{5} $ [man 121 0.11 0.011 - 2
	0001 5300
2	Compate Zx+1 = 12 1001 0001 0000 - 1
	compate 20+1 - 2011 0100
	here d= 32 lets, : L= 0010 000
io)	Compute P=IV / (kxor opad)
	for the 1st churk:
	$m_1 = 1010 1100$
	opad = 0101 1100
	KXOR opad = 1111 0000
	The open in
	£44 ±17
	Concatenate with IV
	11 (1.100
	P=IV (KXOR opad)
	J. P = 1101 0011 1111 0000
(i)	Compute r=q Zx+1
	r= 0000 1000 1001 0111

	C6)
12)	Ifnal HMAC dag (t):
	00100111001 11101 1110
	30 11 ct = 0010101110
	1001 1011 0011
	CO = 1100 000.0°
1011	212 0000 moll 1100
	$z_3 = 0100 0000 0101 0100$
	Zq = 1000 1110 0000 1011
	29 = 1000 11110
	D = 1100 1100 1011 0011
	q = 0000 1000
	r = 0000 1000 1001 0111
	t = 0010 1110
	1 = 52 18 18 18 1 1 = 0010 000