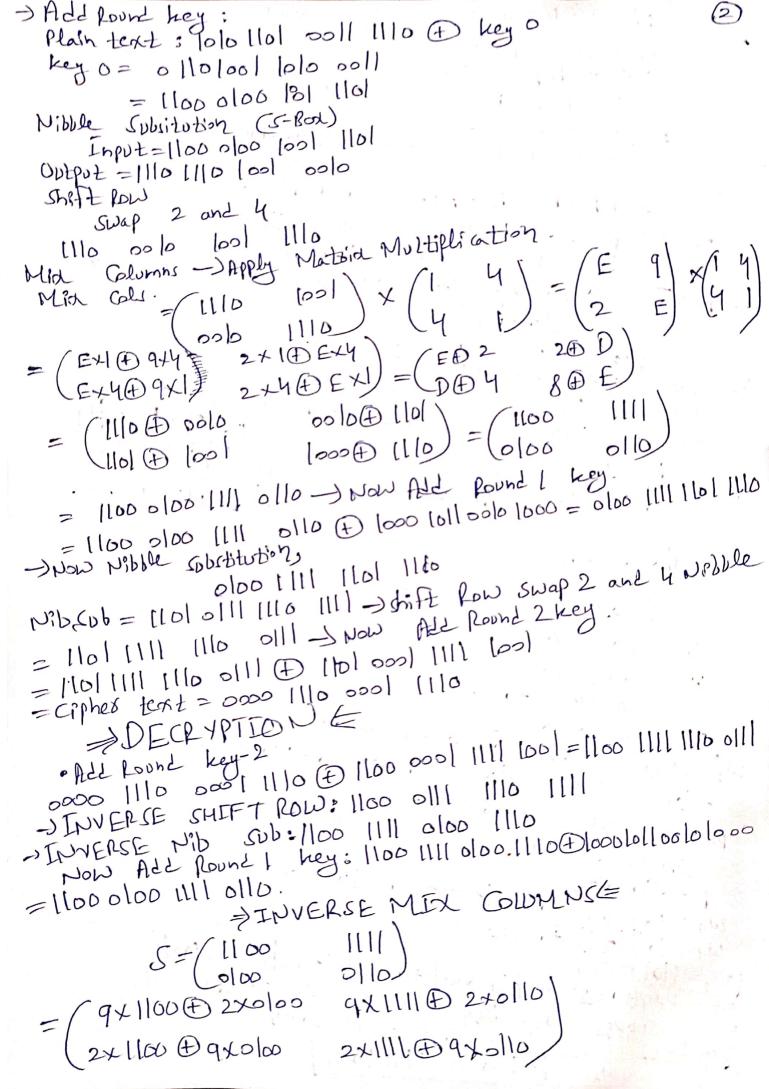
Name: Muhammad Shedjeel Hihtas Koll No: 20p-olol Subject: Information Security. Respected Six: Dx. Muhammad Ampho Section: BCs-7B Assignment No:02 Submmited -> SIMPLIFIED - AES ENCRYPTION & · 16-bit plaintext 1010 Hol coll 1110 16-bit key k: ollo Lool Lolo ooll -> Splitting 16-bit key into two words wo and wi w=01101001 W = 1010 0011 The first subkey he = wow = k Now to generate the other subkegu 2= W (+) 10000000 (+) 500 Hib (ROE Nib (W)) Rot Nob (w) = soll tolo by using 5-Box table osub Nip (Not (MI)) 01101001000000 (+) 01100010 11101001 + 01100010. W2 = 1000 loll W3 = W2 (W) = 1000/01/ 1000011 Wy = W2 (Oollowo (Sub Mib (Rot Mib (W3)). = 1000 1011 (F) 00 [10000 (F) Sub Nip (Rot Nip (00)01000) Rotnip (00/0/000) = 1000 00/0 SUBNIB (lossoslo) Wy = 1000 101 ()00 10000 ()0101010 W4 = 10110 [1 + 0110 1010 25 = Wy (+) W3 = 1[01000 (+) 00 101000 = [][[00] Now Subley axc: key == WoWI = 0/10/00/ 10/00/ 1000 1011 0010 1000) hey 2 = WyWs = 101 0001 1111 100



goo= (9×1100€ 2×0100) =(9xCD 2x4) = (608) = (01100 1000) = [110 S10=(92x(D 9x0l00)=(2+CD 9x4)=BD2=1011D0010 [=100] Sol= 9x1111 @2x0110 =9XFE 2X6 = EAC = 1110 D 1100 =5000 SII = 2×1111 @ 9×0110 S11=24FA 9+6 =DD 3 = 1101 + 0011 =[110] Outpot=1110 1001 0010 1110 Invesse Shift fow 21110 1110 0010 1001 NOW Inverse Nibble Sub =0/00 0/00 /00/ 0000 Now Add Round O key 0000 000 000 0000 0110 1001 1010 0011

[20010101011100