Assignment -2 10 ×n+1 = (axn) mod 2⁴ Let us consider a random real 181 Long : 18 emod 16 /= } let us assumé a goli : x, = 3 madib = 300 = 10 X2 = almodile angli : , x il let us assume a = 5 23 = 27 mod Hor = ? 11 = 1 x1 = 5 mod 16 = 5 xy 333 mod 16 5 1- 1 75= 3 mod 16 = 3 12=25mod16 =9 \$3:90 m= n- ; KJ N3=45mod16=13 24= 65 mod 16 =) (iii) Assume a = 7 25=5 mod 16 = 5 += x = + mariber + 11: 31/ = of all mod 16 15 1 {5,9,13,1, - - · } F = 1/2 = 7 mod 16/1= 7 MASSume a = 11 3 = 81 /2 7113 = E.x. } x,=11 mod 16 = 11 € Assume a=13 x2 = 121 mod 16 = 9 x, = 13 mod 16 = 13 74 = 33 mod (6 = 1 - 3 //11 / 2 = 169 mod (6 = 9) 23 = 99 mod 16 = 3 211,9,3,1,--.35101-1 mod 235117-mod 16,=5 ins? 213,9,5,1, - -3-El Lom of F= 1+0x d) Max period obtained is 4 b) a can be 5,3,11,13 for 20=1 It should be relatively prime with 16, 1.e. ((co(a,16)2). (Restrictions on seed

Assignment - 2. Poobs.4 2n+1 = 62, mod 13. faborn (nxE) = 1+nx let xo = 0 1. X, = 6 mod 13 F 6 2 makeur a relience so to x2 = 36 mod 13 = 10 en en del () x3 = Bomod 13 = 8 1 3 di Bom & x 4 = 48 mod 13 = 90 = 3x (i) Let us assorne a=5 25 =154 mbdd3 = 2 = 8x X = 12 Mbb13 & 62 px 2 = 21 bom2 = 1x x = 72 mod 13 & 72 X x = 25 modis = 9 17 = -42 mod 13 2 63 Nos 45 modile = 13 ty= 65 mod 16 = 1 2 = 18 mod (3 = 511) 2 = 31 loom 2 = 2x 2100730 mod 13 = 4 1,81,7,23 12 iv 5 24 mod 13 =11 F = 2/2 = 186 mod (3 = 1 II = D smoda A @ (X13 = 6 wood 13 = 6 11 = 11 bom 11 = 1x S Acesume a=13 P = 01 boinvisi = K X, = 13160m8 = 13 E = 91 hom pp = x {6, 10, 18,1965, 13,7,3,8, 4,11,1,6 - L= 23 mod (b/=) -Peniod has all numbers from 1-to12[(b) xn+1=12, p, E1 } feling period objected is t 2,=7 mod 13 =7 =1 (11, 5, 2, 3) m. e. (1) 10 (0) p) a) = 49 mod 18 = 10 to so not like in . E. E(co(a) 10) = 10 touzero militaria. 232170 mod 13 = 5 or at Edwards to our xy=35 mod 13 =9

X 5 75 6 32 mod 83 = 14, /=[1]2, 0 10] word 12 0 0001 76=27 mod 13=12 J 25 boin ([i] + Ci) + (i) + i) xy = 84 mod 13 = 6 19^{-1} beginned en en son [i] 11^{-1} 129 = [2] med 13 = 8 = [i] r nort o : i li o : i d. 2,0=[56 modis=2=[i]T nont 1=1 ti, 1=1 rot 411=128 mod13 = 2[i] = ::) Skiz Ester midd 13 3 FR = [i) + month s = i ti, s = i rot 12 (325 \$ mod (3) = A. S = Cole: () { 7.10, (8)9, 11, 12, 19, 13, 28; An 2011, 7 672 3: Period has all numbers from 1012.

So it is of full period.

Prob8:6 We have s[0]=0,s[i]=1, += =\$ [255] = 255 x j=(j+sCi)+TCi]) mod 256 = El hom +6 = 0K for j= i the sci] remains unchanged. for i = 0, if j = 0 then TCi] = 0 = i-e kCo] = 0 for i = 1, if j = 1 then TCi] = 0 = i-e kCj] = 0 (:: s Ci]= [:]= 0 \$1 + 0 = D for i= 2, if j=2 then + Ci]=255 & iten & C27 =355 (::s(2) = 2, j=(1)+(2) + 255) god 256) for 1 = 3 , if j = 3 +then Tei] = 254, Fire. 12 (3) = 254 ; (: 5[3]=3, j=(3)+(3)+(3)+(3)) mod 2563 j=3) for i = 255, if j=255 then T(i]=2, i.e. k (255]=2 (··· 2 (522) = 522 (14(824) + (522) + 2) mod 226 3 (522) i. tay has to be of length 255 with below volues bos to remain unchanged i o of to such lettint & KCol= KCil=10 Dis Jack Hill K(2) 21256, K(3) = 254, - K(255) = 2. for i=0,1 pCi]=0 (i)=0=3 = (0)=1 for i= 2 to 255 kCi] = 256-SCi]+1 Prob 8.7: a. We can store only i jands -> This requires 8+8+(256 +8) = 2064 bits

(b) Number of states (256 + 2562) 121700 -> (1200 bits are

Probabation values of 19 & the next colles with 8.8 dong rosbog Ve 2,80, bit value vil. pele ris si si pres A smel 100 the E 128 bit value of to souler proposition of os C = RC4 (VIII) &m a, Retreiving 'm' from oll contrar did of it of Taxefirs tero bits of solle, that gives 19 Fig. Mond not 1/ Endro 3, Calego somprer og .. Bob & Alice can communicate 200 menages bestores the bestores the leaf storeams repeats truice - - (2)11.00), (1)11.00), (1) tey stream (Random) to pour is to sular Adversary can perform m. D.S. to get teystramby: ob here 280 mersager can be self-100,m m2 @ C2 = k2 mn & Cn = En if any two mit (& mj t () yield same till by then adv knows same beystream is used. (C) 19 - 18 obits -) append 48 zeros to make it 128 bit. for 1= 0+0127 for 120+0124 i = (i +1) mod 128)=()+18(P]+ K[i]) mod 128 j=(j+v [i])mod 128 Swap (vo (i3, vo (i3)) ([i] or [i] ex) gows t = (so [i]+v[j]) modila K = 20[t] Dc[i].

C, for a given value of voz & the RCA (2011 k) will abelian Some As trey k is already fined, likely stream dependson is So for different values of 20 the RCA generates diff key Streams o is so hit values sile most im' grinisotal, a, So possible too of valuestion is 2 1280 i. For 280 values of ho, RCa (1011K) generates Bob & Alice can communicate 20 menages before. the bey streams repeats twice. - (1)11,00). (1)11,20 depends on value of variage of brokens moonda post It has hist value, on merrages can be anexypted. En here 280 messages can be sent in mi if and two miles is inited its fire till and the . Then and process some med strong is need. did sel di eden est esmos in lungo - etiologe - (-) i= (i+1) miod 126 Experience of the F. 3.51 Lon (17) 4 PT 12.5 351 Lova (Eijerr C)ri This of the