

M.Tech Computer Science Information security.

Cryptography Basic.(CS6530)

Assignment-2.

Roll Number - CS21M515

Name - Ayub Shaikh.

Batch Year-2021

so values are getting repeated after 4 values it means it is having maximum pended is 4 which is 24-2 = 4 - max period.

5) What Should be value of a.

Assignment: - 2

Xn+1 = (a xn) mod 24

m. the modulus moo

X2 = (5 ×5) mod 16 = 9

x5 = (5 x1) mad 16 = 57

X1 = (5 x 5) mod 16 = 91

X8 = (5 x13) mod 16 = 1

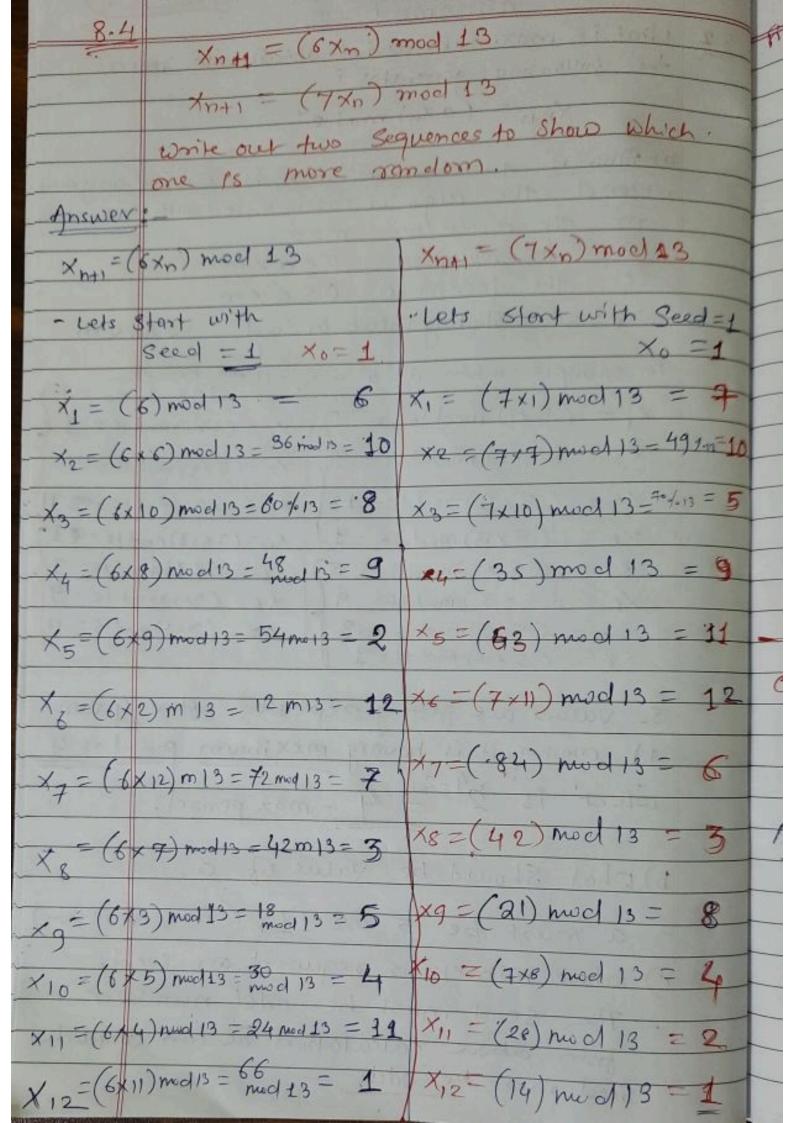
the following generals ?

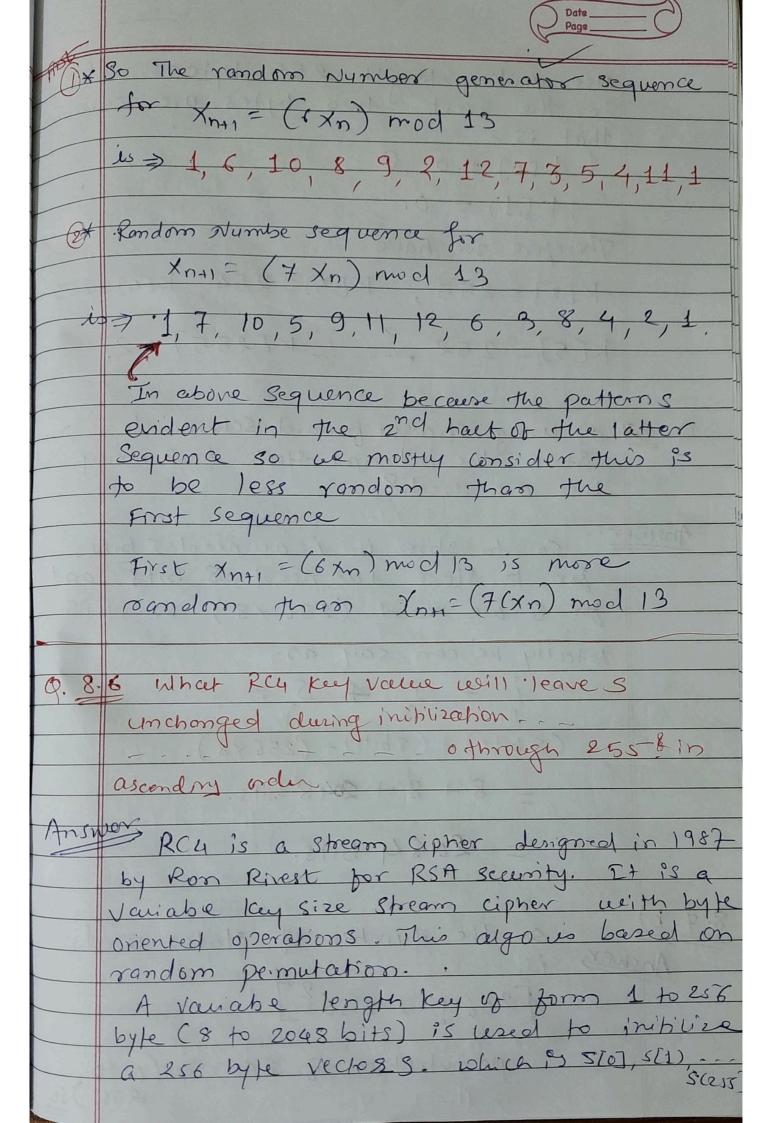
a must be 5 or 11. (from carwichon)

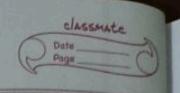
c) what resmetims required on seed.

. The seed must be odd number.

from above calculation we can conclude Seed most be odd.







use a key length 255 bites.
So the first two bites are zero
that is kto) = 0 &

k(d) = 0.

Therefore we have

KE2] = 255, KE3) = 254, KE43=253

K[5]= 252 K[255]=2.

(c. 87 a) wing straight forward scheme to Store the internal state how many bits are used.?

Answer: So to spire it i we need 8 bits, for to store i we need 8 bits and for 8 we need (256 x8) So it is

totally we can say as.

i + j 4 5

(8 bits) + (8 bits) + (256 x8)

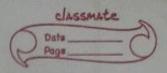
= 8 + 8 + 2048 bits.

= 2064 bits.

8.7 b) so the number of states used

[256! x 2562]

permuteupon of 256 'cos (0 to 255) 50



(0 to 255 so total 256).

[2561 x 2562]

× 21700

There fore 1700 bits are required

Q 8.8 a)

Answer: - 90 by telling the first 80 bits

Bob can obtain the militation vector V.

Known, so the message com be recovered and decrypted by computing

RC4 (VIIK) AC

(v, 11c,); (V211 C2) ... fransmitted we can that $V_i = V_j$ for distinct i, i, them adversary knows that the same key stream was used to encrypt both messages for example m_i & m_j . So in this case the messages are Vlunerable to by using the first 80 bits 0) VIIC we get the inipilization vector 30 them as he knows these them by using RC4 (VIIK) RC4

Adversary can compute the manage

Bithday paradox is type of cryptographic which is clan of Brete Force attack attack. The Success of this attack is depends on likelihood of collisions found bet random attack attempts.

Now here in this example since Key is fixed, the ky stream varies and we Know it is 80 bit vector which Setelted random. so it is 200 menages but there send by duice & bob so but

to consider only Alice menages send will be half or it so op it is ~ 240 so it could be approximately ~ 240

menages are sent we expect some V. (ketu) and same ky stream to be used more than once

8.8 of so in the lefe time of key the number of menage can be encrypted by K, So from above point c'ue can approximate suy \$ 200 \$ 200 menages.

so a key should be changed before 2 menages are sent

so that it won't used furce.

* Thank - you - sir x