MAY' 18

26 Day 146-219 Wk-21
SATURDAY

05/2018
Monday 7 14 21 28
Tuesday 1 8 15 22 29
Wednesday 2 9 16 23 30
Thursday 3 10 17 24 31
Friday 4 11 18 25
Saturday 5 12 19 26
Sunday 6 13 20 27

HWSEC Graded ΔTut - 1

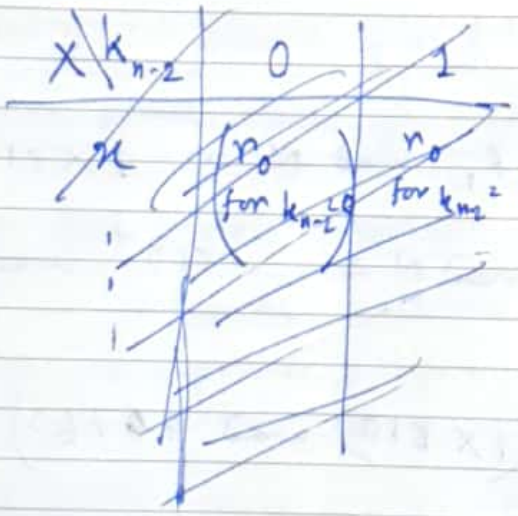
10.3.22

SUNANDAN ADHIKARY
21CS91R14

Hypothesis table

→ We know $k_{n-1} = 1$

then $k_{n-2} = 0$ or 1



→ We know the real power trace at $i = n-2$ th iteration

↳ A column in Real trace table

→ Now we correlate each 2 columns in Hypo trace with $(n-2)$ th column of Real trace [it is likely to be the highest one]

→ 0 for $i = n-1$ in algo

$R_0 = (R_0 \times R_1) \bmod N$

$R_1 = (R_1)^2 \bmod N$

→ for $i = n-2$ in algo

if $k_{n-2} == 0$

$R_1 = (R_0 \times R_1) \bmod N$

$R_0 = (R_0)^2 \bmod N$

if $k_{n-2} == 1$

$R_0 = (R_0 \times R_1) \bmod N$

$R_1 = (R_1)^2 \bmod N$

$R = R_0$

Hypotrace $[i, k_{n-2}] = HW(R)$

notes
Phone
email
website

the formula for correlation :

$$\sum_{i=1}^{10} Hypotrace[i-1, k_{n-2}] - mean(Hypotrace[i-1])$$
$$\times \sum_{i=1}^{10} Realtrace[i-1, k_{n-2}] - mean(Realtrace(i-1))$$

$$\sum_{i=1}^{10} (Hypotrace[i-1, k_{n-2}] - mean(Hypotrace[i-1, k_{n-2}])$$
$$\times \sum_{i=1}^{10} (Realtrace[i-1, k_{n-2}] - mean(Realtrace(i-1, k_{n-2}))$$

= Correlation matrix [k_{n-2}]

The Highest data in correlation matrix will give k_{n-2}