Playfair Cipher

A PARALLELIZED APPROACH

Pranavodhayam P R
Sanford Jone

Github Link

Pipeline

1. Create 5x5 matrix
2. Fill matrix
3. Traverse through vocabulary
4. Form digraphs
5. Encrypt digraph
6. Concatenate
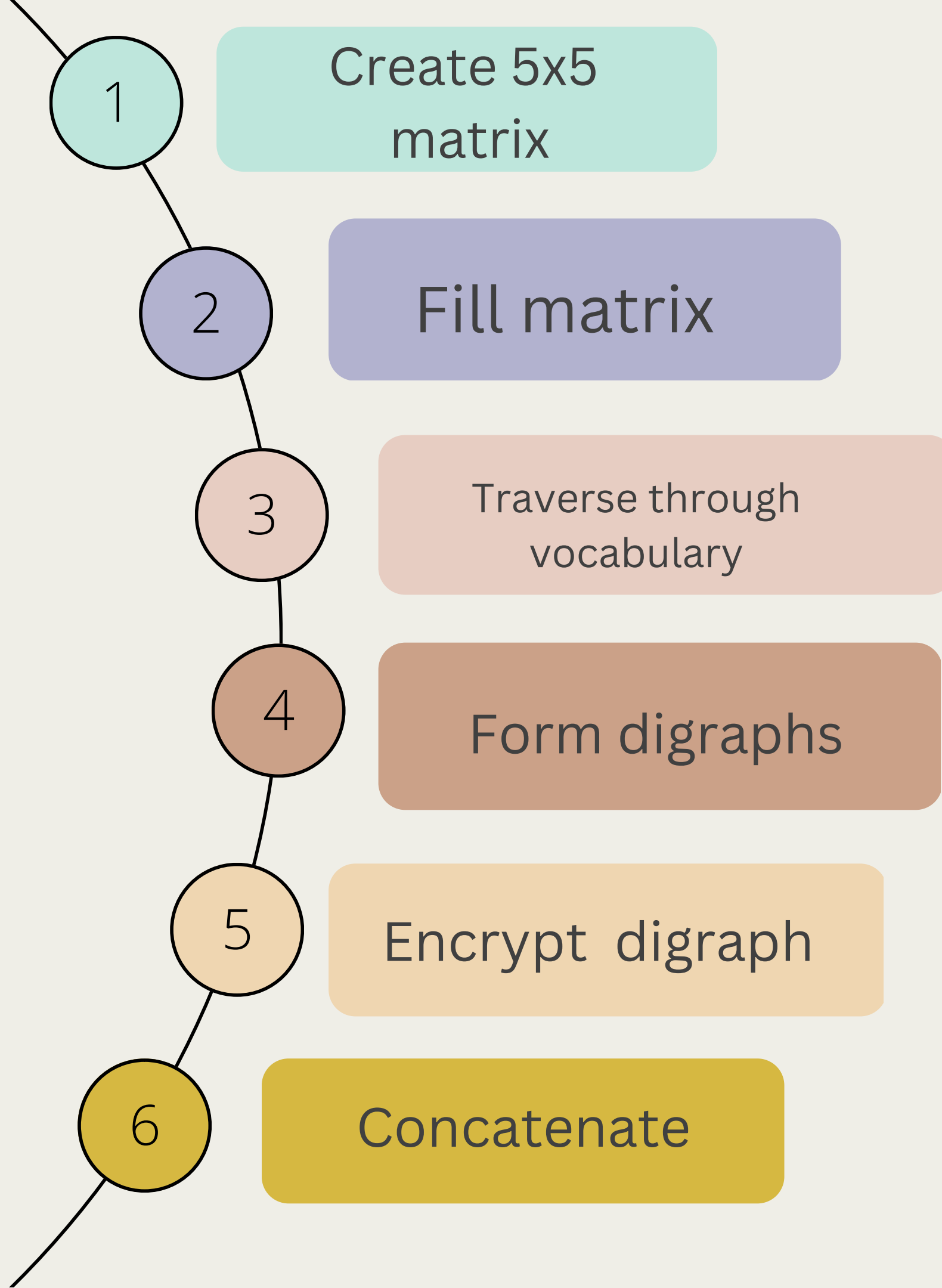
ASPECTS OF PARALLELISM

Parallelizing data

The vocabulary can be split into n parts that can be fed into n threads which will encrypt the words

Parallelizing the algorithm

In Playfair cypher , the words will be split into pairs after which they will be encrypted based on the three rules. Here , the pairs can be batched and fed into threads which will perform substitution

Performance metrics

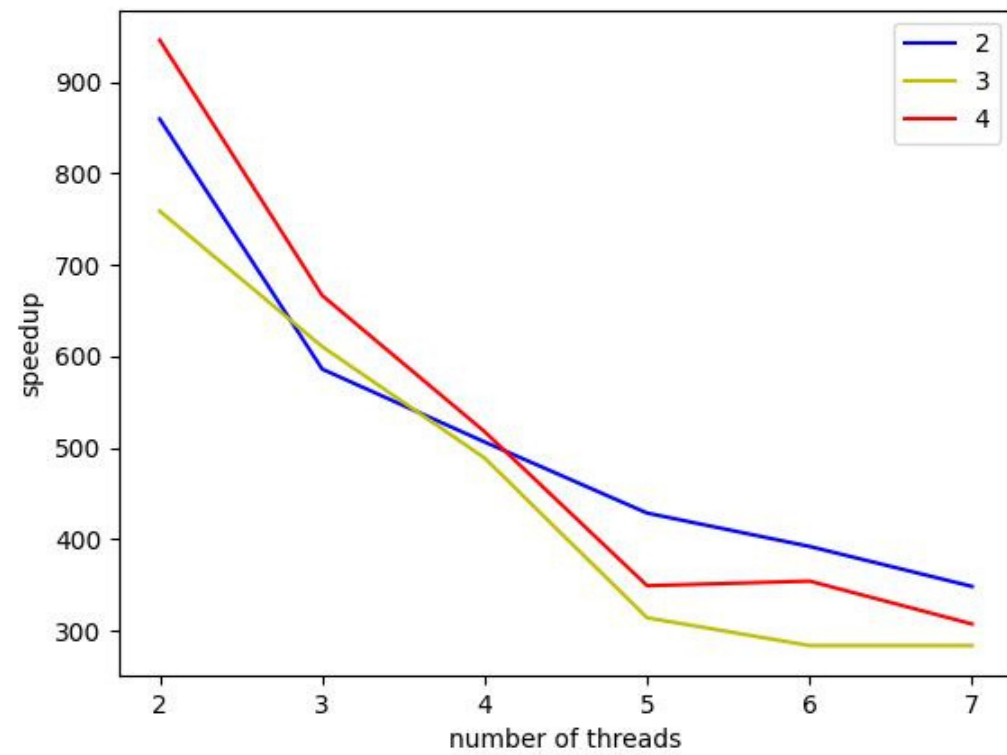| N	parallel-efficiency
90k	21600%
180k	637500%
370k	135000%

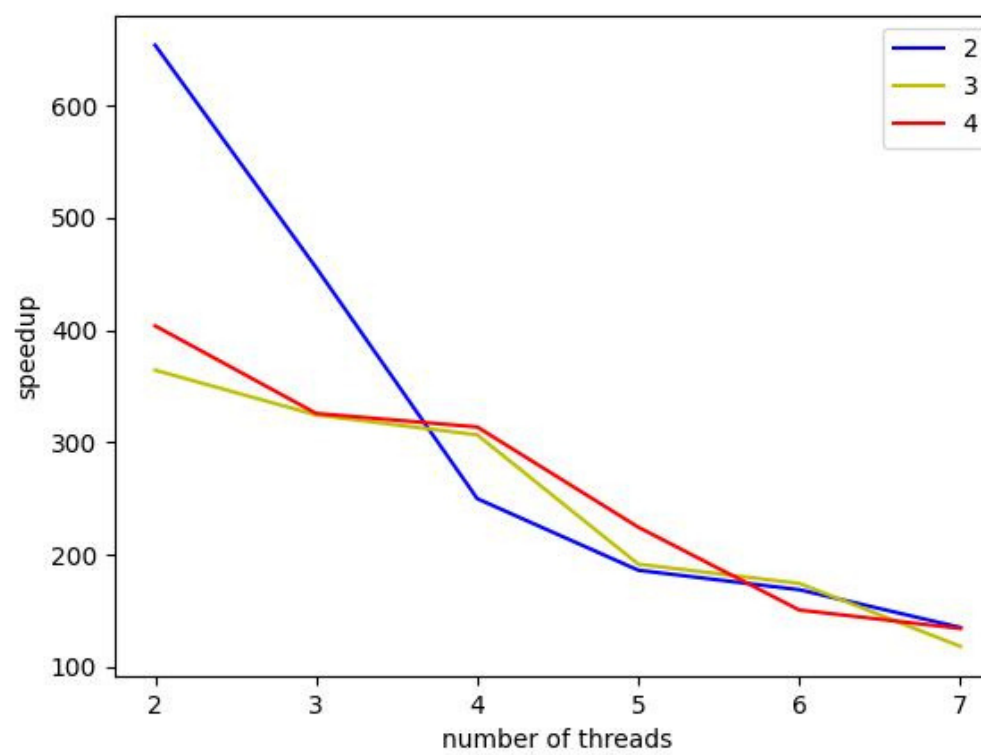| N	speed-up
90k	432x
180k	1275
370k	2700

GRAPH 1

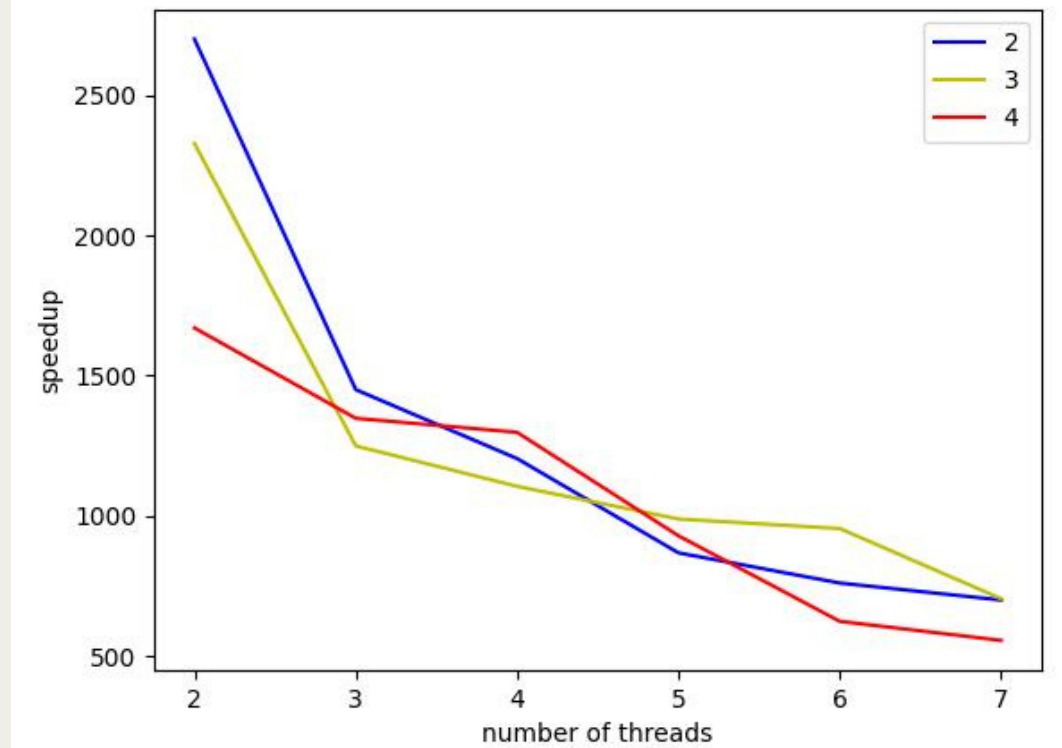For different values of N, Plot speed up with respect to the number of processing elements

90k

180k

370k

GRAPH 2

For different numbers of processing elements,
Plot speedup with respect to N