PROJECT TITLE: PARALLEL HILL CIPHER ALGORITHM

by-
Vijay Shrinivas Senthilnathan(21011101143)-AI&DS-B
Mathu(21011101076)-AI&DS-B

- **Overview:**

1. Matrix Operations: Parallelize matrix multiplication, a core step in the Hill cipher, using parallel algorithms or GPU acceleration for increased efficiency.
2. Block-level Parallelism: Process multiple blocks of plaintext concurrently, dividing the workload for parallel execution.
3. Pipelining: Implement a pipeline structure to overlap different stages of the encryption process, improving overall throughput.
4. GPU Acceleration: Leverage Graphics Processing Units (GPUs) for their parallel processing capabilities, especially beneficial for large matrix operations.
5. SIMD Instructions: Exploit Single Instruction, Multiple Data (SIMD) instructions in modern processors for simultaneous processing of multiple data elements.

- **Application:**

- Large-scale Data Encryption: Efficiently encrypt large datasets, applicable in secure communications, database encryption, and scenarios with substantial data volumes.
- Real-time Encryption: Achieve real-time or near-real-time encryption for streaming data, crucial in applications requiring low-latency encryption, such as secure communication in real-time systems.
- Resource-Intensive Environments: Distribute computational load across multiple nodes or processors in resource-intensive environments like cloud computing or distributed systems.
- Hybrid Approaches: Combine parallel processing with other optimization techniques, such as efficient matrix inversion algorithms, to create hybrid algorithms for enhanced performance.

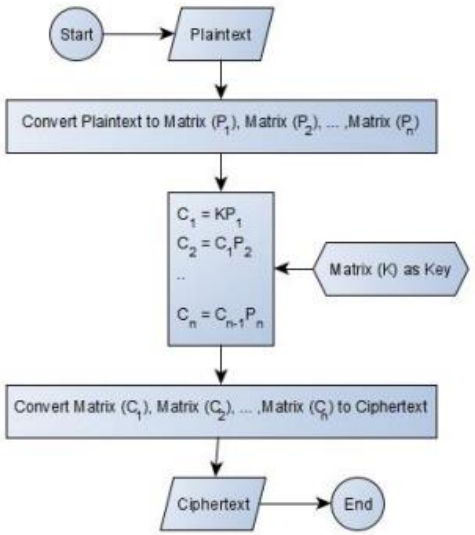


Figure 5 Encryption Process on Hill Cipher Chain.

- **Matrix Multiplication:**

1. The main computational task in the Hill cipher is the matrix multiplication of the key matrix with the plaintext matrix.
2. Techniques such as parallel matrix multiplication algorithms (e.g., Strassen's algorithm) can be employed to speed up the matrix multiplication process.

- **Block Processing:**

1. Hill cipher processes the plaintext in blocks, and each block is treated independently.
2. Different blocks of the plaintext can be processed concurrently on multiple processors or threads, which is a form of parallelization. However, the order of processing blocks is important, as the result of one block affects the subsequent blocks due to the matrix multiplication.

- **GPU Acceleration:**

1. Graphics Processing Units (GPUs) are well-suited for parallel computation.
2. The matrix multiplication step can be offloaded to a GPU, taking advantage of its parallel processing capabilities. GPU acceleration is especially effective for large matrix operations.

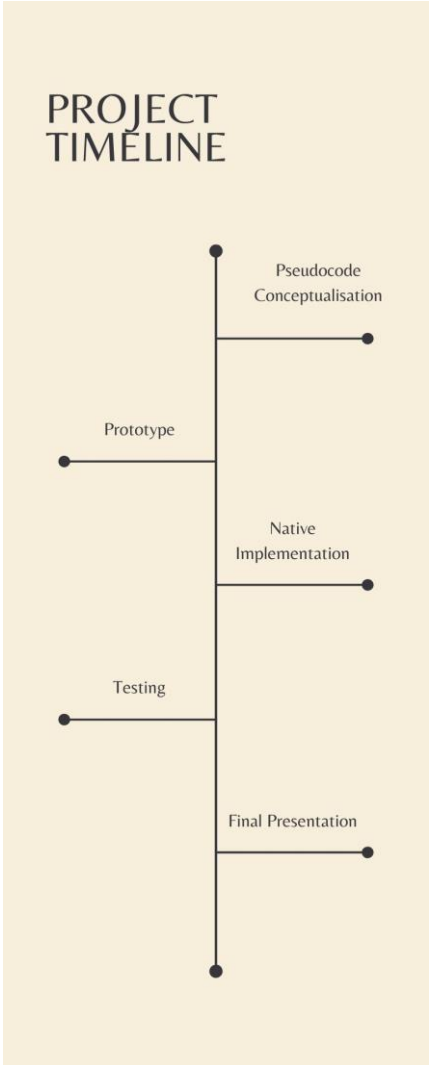
- **SIMD Instructions:**

1. Single Instruction, Multiple Data (SIMD) instructions in modern processors can be exploited for parallel processing.
2. SIMD allows multiple data elements to be processed simultaneously with a single instruction.
3. Implementations can be optimized to take advantage of SIMD instructions for operations within the matrix multiplication.

- **Pipelining:**

1. Breaking down the encryption process into stages and pipelining them can improve overall throughput.
2. Pipelining involves overlapping the execution of different stages, allowing the next stage to start before the previous one completes.

PROJECT TIMELINE



REFERENCES

- **Parallel algorithm for Hill Cipher on MapReduce(IEEE Ref Paper)-By Xinyu Wang & Zhaoe Min :**

Link of Reference :

https://ieeexplore.ieee.org/abstract/document/6972384

- **Parallel Hill Cipher Encryption Algorithm(Ref Paper)-By Mais Haj Qasem & Mohammad Qatawneh:**

Link of Reference:
https://www.researchgate.net/publication/323220951_Parallel_Hill_Cipher_Encryption_Algorithm

- **Primary Key Encryption Using Hill Cipher Chain(Pdf)-By Muhamat Abdul Rohim, Kiswara Agung Santoso & Alfian Futuhul Hadi:**

Link of Reference:

https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.atlantis-press.com%2Farticle%2F125970031.pdf&psig=AOvVaw0NRF2Rh9jjVOHJp95NpIFE&ust=1706523307589000&source=images&cd=vfe&opi=89978449&ved=0CBUQjhxqFwoTCLC_1vTs_4MDFQAAAAAdAAAAABAD

GITHUB REPOSITORY LINK

https://github.com/ssvijayy/High-Performance-Computing.git