Project 3 - Implement the Paillier Homomorphic Public Key Encryption Scheme and the Secure Dot Product

1 Tasks to be Performed

- Implement the Paillier key generation function that takes a positive integer k as an input and outputs the public key (N, g) and the private key (λ, μ) such that N is a k-bit integer.
- Implement the Paillier encryption and decryption functions
- Implement the homomorphic encryption based secure dot product protocol

2 Expected Outcomes

When the main program is executed, here is the expected output:

1. Enter the name of the file that contains p, q and g:
2. Enter the output file name to store λ and μ:
3. Enter the name of the file that contains $\vec{u}$:
4. Enter the output file name to store $E(\vec{u})$:
5. Enter the name of the file that contains $\vec{v}$:
6. Enter the output file name to store $E(\vec{v})$:
7. Enter the output file name to store $E(\vec{u} \bullet \vec{v})$ and $\vec{u} \bullet \vec{v}$:

3 Programming Language and Library Requirements

This project needs to be implemented in C and uses the GMP library (The GNU Multiple Precision Arithmetic Library, http://gmplib.org/) to manipulate big numbers.

4 Deliverables

- README: describe the purpose of your files and provide instructions on how to compile and execute your program.
- Well-documented source code.

5 Submission Instruction

Please submit your implementation using Canvas. For technical questions related to the project, please contact Nitish M. Uplavikar (nmu455@mst.edu) directly. His office is Computer Science Building # 312.