Project Specification

A. Names of all team members:

- Narendra Nutakki
- Shylaja Gunda

B. Title of the project:

Design of a ***32-bit unsigned multiplier modulo 2^{32}*** and for ***squaring mod 2^{32}.***

C. Hardware and Software Unit Initial Specification:

- **Functional requirements:**
  - *Implementation of:*
    $C = A \bullet B \bmod 2^{32}$
    $C = A^2 \bmod 2^{32}$
  - *Number and sizes of operands:*
    Three operands, two for multiplication and one for storing result.

    A = 32 bit vector.
    B = 32 bit vector.
    C = 32 bit vector due to modulo operation.
  - *Functional arguments for Software:*
    A = long int (32-bits);
    B = long int;
    C = long int;

- **Example of a real-life application:**

  Multiplication and squaring techniques are used in modern block ciphers, such as MARS developed by IBM and RC6 developed at MIT, which are the leading candidates to the new Advanced Encryption Standard (AES). More information about RC6 cipher can be found at: http://www.rsasecurity.com/rsalabs/rc6/
  The documentation of MARS can be found at http://www.research.ibm.com/security/mars.html

The specifications of RC6and MARS are taken as optimization factors for the design.

- **Optimization criteria:**
  - *For hardware:*
    - Minimum Latency
  - *For Software:*
    - Minimum Execution time
    - Minimum number of clock cycles.

- **CAD tools:**
  - *For Hardware:*

    Mentor Graphics, Xilinx and Aldec tools available in ECE lab.
    - Aldec Active-HDL, v. 4.1
    - Xilinx Foundation Series, v. 3.1i
  - *For Software:*
    - Microsoft Visual Studio 6.0
    - Microsoft Windows XP.

    Also planning to implement the same program on Solaris workstation in UNIX environment.

- **Assumptions:**
  - *For Hardware:*
    - Elementary Components:
      AND, OR, XOR and Inverter gates.
    - Relations:
      All the two-input gates constitute one gate delay
  - *For Software:*
    - Language:
      C
    - Basic Library Functions:
      clock (), to determine the program run time.
      Shift operations
    - Exact Interface of the functions:

Unsigned long int multiply_32 (long int A, long int B);

Unsigned long int square_32 (long int A);

- **Test plan:**
  - *For Hardware:*
    - Design testing:
      A test bench will be written in VHDL and the code will be simulated using the test bench and the results will be verified for correctness.
    - Circuit area:
      Circuit area is determined by calculating number of input gates required for the design.
  - *For Software:*
    - Design testing:
      Various Inputs will be given to the function and the results will be checked for correctness.
    - function execution time:
      Using clock () function the time at the start and end of multiply function is determined and the difference is calculated.
    - function memory:
      The memory occupied by the function is determined by verifying the object file of the program.
- **List of references:**
  - *Intended Application:*

    The application is intended to design a 32-bit unsigned multiplier modulo 2^{32} which can be used in modern block ciphers used for encryption.
  - *Software algorithm:*

    procedure main ()
    begin

►declare two local character arrays to store the input

unsigned char X [4], Y [4];

► the input is stored in a file in hexadecimal notation and is read into the character arrays.

► stuff the input into two long int variables each of 32-bits length by calling stuff_input function.

stuff_input(X, Y);

► invoke the multiplication function which performs multiplication of two 32-bit unsigned values modulo 2^{32} and returns the result.

C = multiply_32 (A, B);

► print the result

►invoke squaring function to perform $\mathbf{A^2 \bmod 2^{32}}$

C = square_32 (A);

►print the result;

end proc;

procedure stuff_input(int X, int Y)
begin

► this procedure stuffs two character arrays into two 32-bit long int numbers

for i←1 to 4

►shift the output long int;

►store the 4-bits of the input into its corresponding position in the output long int.;

end;

procedure multiply_32 (long int A, long int B)
begin

► this function performs $\mathbf{A \bullet B \bmod 2^{32.}}$ Also it determines the time required to perform the operation.

```
                long int result;

                result = A * B;
                return result;
    end;


procedure square_32 (A)
begin
                ►this function performs A^2  mod 2^32

                long int result;

                result = A * A;
                return result;
end;
```

- *References:*

  - Computer Arithmetic: Algorithms and Hardware design by Behrooz Perhami
  - Computer Arithmetic Algorithms by Israel Koren.
  - Essential VHDL: RTL synthesis done right by Sundar Rajan
  - Papers submitted on “High-speed MARS hardware” by Akashi Satah, Nobuyuki Ooba, kohji Takano, Edward D’Avignon.