|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test** | **Conditions** | **Procedures** | **Expected Results** | **Actual Results** |
| Multiply Functionality | Msm file loads into emulator without errors  R3=x54,  R4= x53,  R5= x54 | R3 adds r5 to itself the specified number of times (r4) | R3= x1b90 | R3= x1b90 |
| Mod Functionality | Msm file loads into emulator without errors  R3=x1b90,  R4= 0,  R5= x54  Constant value 119 | R3 adds -119 until it becomes negative at which point it adds 119 once | R3= x23 | R3=x23 |
| Encryption Equation | Msm file loads into emulator without errors  R3=x54,  R4= x53,  R5= x54,  R6= x53  R7= 4 | Break the mod function down with product rule of mods as explained in the explanation of algorithm document. Multiply R3 by itself R7 times and modulate after each multiplication to keep R3 reasonably sized  m' =me mod n | R3= x54 | R3= x54 |
| Decryption Equation | Msm file loads into emulator without errors, String encrypted correctly  R3=x54,  R4= x53,  R5= x54,  R6= x53  R7= 76 | Do the same as encryption mathematically except with a different exponent  m = m'd mod n | R3= x54 | R3= x54 |
| Memory write | Msm files loaded and program completed | The program wrote to the specified locations | X1000= Encrypted= “TS8/….etc”  X2000= decrypted= “This is a (FAIRLY…” | X1000= Encrypted= “TS8/….etc”  X2000= decrypted= “This is a (FAIRLY…” |
| Modelsim functionality | Fully Compiled Code on Quartus and Modelsim-Altera,  Program has run to the point of the final hlt command, ModelSim has the regs 0-7 displayed | The program runs in modelsim | R0= x0000  R1= x2002  R2=x0054  R3=x0053  R4=x0038  R5=x0054  R6=x0068  R7=x0069 | R0= x0000  R1= x2002  R2=x0054  R3=x0053  R4=x0038  R5=x0054  R6=x0068  R7=x0069 |
| DE2 Functionality (Reset) | Program Loaded onto DE2, run=’0’,  Key0 pressed | Registers are reset to x0000 | R0= x0000  R1= x0000  R2= x0000  R3= x0000  R4= x0000  R5= x0000  R6= x0000  R7= x0000 | R0= x0000  R1= x0000  R2= x0000  R3= x0000  R4= x0000  R5= x0000  R6= x0000  R7= x0000 |
| DE2 Functionality (Run) | Program Loaded onto DE2, run=’1’ (SW17 up),  Key0 not pressed | Program runs on DE2 | Run light lights up | Run light lights up |
| DE2 Functionality (Overall) | Program Loaded onto DE2, SW17 in the up position for t>0s | Program runs correctly and the switches corresponding to each register are switched up (to ‘1’) | R0= x0000  R1= x2002  R2=x0054  R3=x0053  R4=x0038  R5=x0054  R6=x0068  R7=x0069 | R0= x0000  R1= x2002  R2=x0054  R3=x0053  R4=x0038  R5=x0054  R6=x0068  R7=x0069 |