# RC-6 CRYPTOSYSTEM IN VHDL

BY:-
Deepak Singh Samant

# OBJECTIVE:

TO IMPLEMENT A CRYPTOSYSTEM USING RIVEST CIPHER-6 (RC6) ALGORITHM IN VHDL(FPGA)

# What is CRYPTOLOGY?

CRYPTOGRAPHY is the art and science of achieving security by encoding message to make them non-readable .

CRYPTANALYSIS is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

CRYPTOGRAPHY

\+

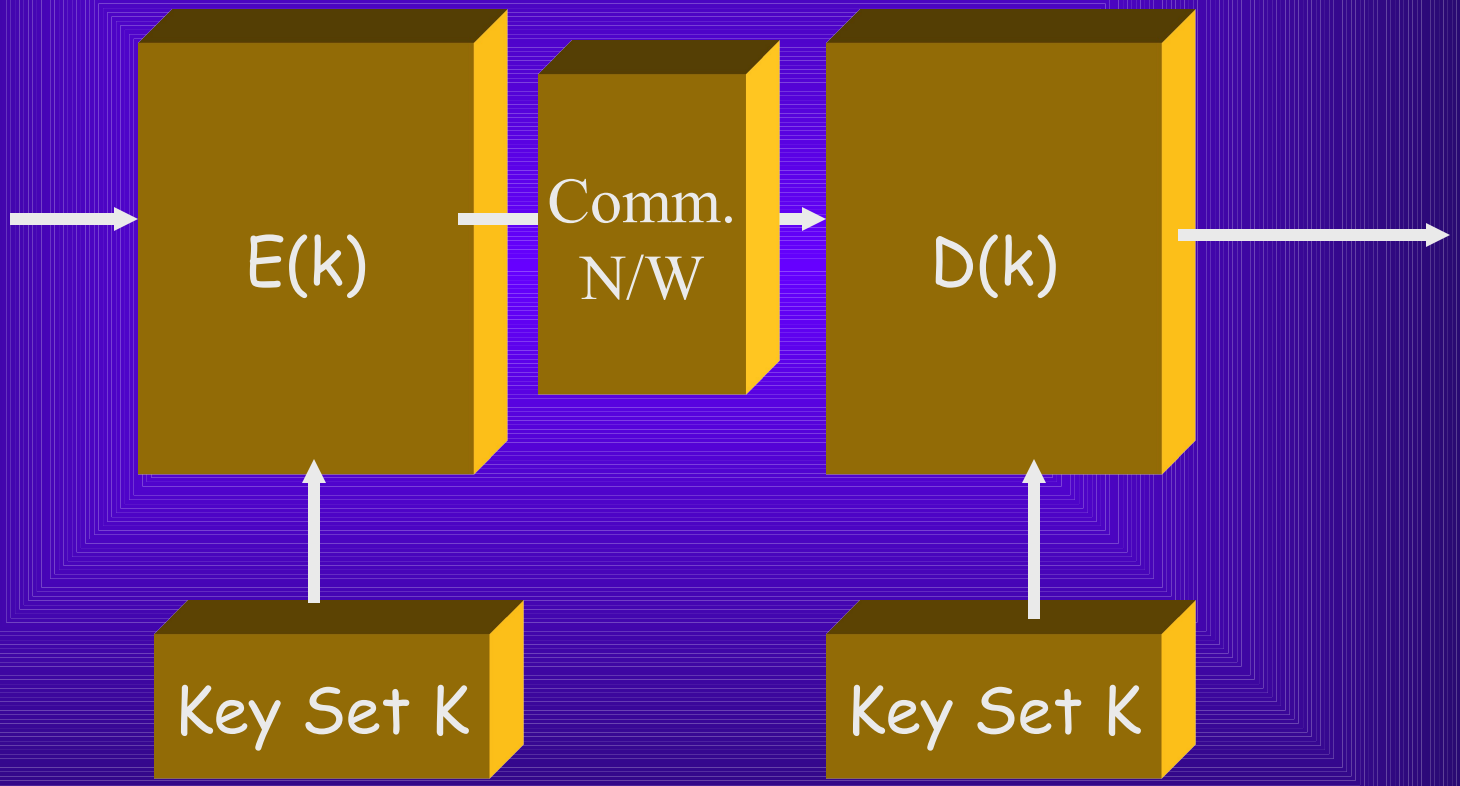
CRYPTANALYSIS

=

CRYPTOLOGY

# Cryptography

Overview:



# Types Of Attacks:

- General View:

1.Criminal Attack 2.Publicity Attack

3.Legal Attack

- Technical View:

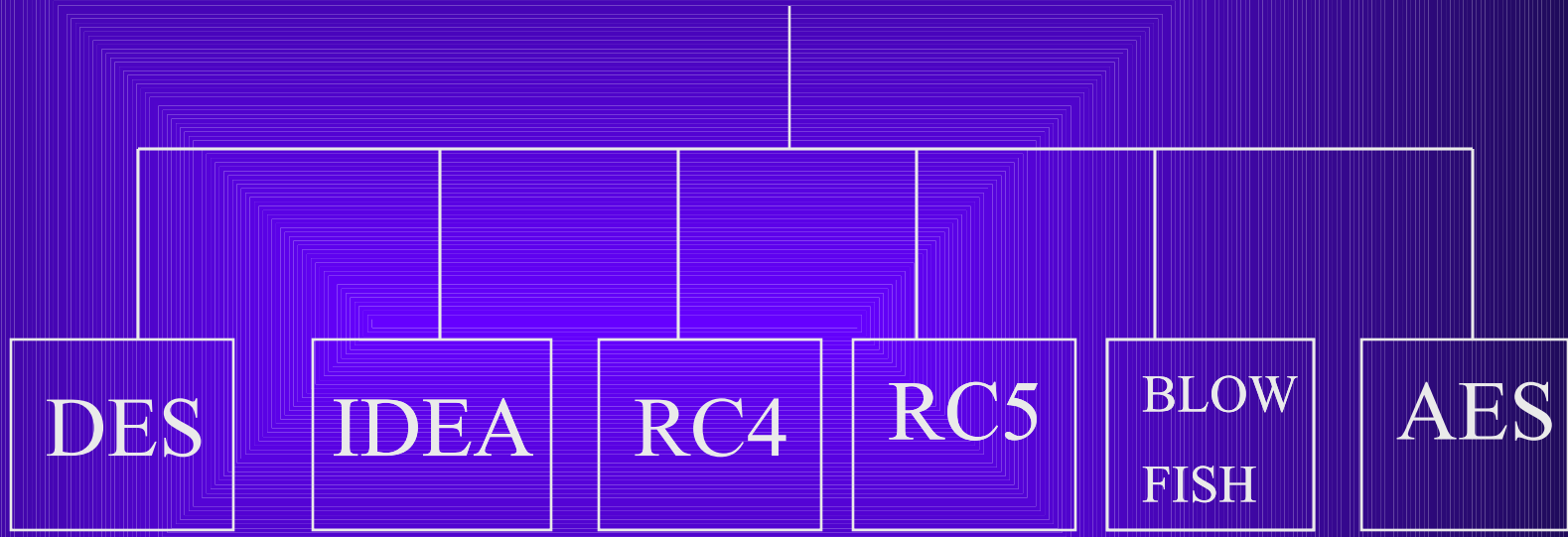
- Passive Attacks
  - Release of message
  - Traffic Attacks
- Active Attacks
  - Interruption
  - Modification
  - Fabrication

# Symmetric key cryptography

If same key is used for encryption and decryption,we call the mechanism as symmetric key cryptography.

It has the key distribution problem.

# Symmetric key cryptography Algorithm



# AES:

US government wanted to standardize a cryptographic algorithm,which was to be used universally by them.It was to be called as the Advanced Encryption Standard(AES).

Among various proposal submitted,only 5 were short listed:

1.Rijndael 3.Serpent 5.MARS

2.Twofish 4.RC6

# LITERATURE SURVEY

- **Comparison**:

**(1) MARS:**

- Its throughput in the studies was generally low. Therefore, its efficiency (throughput/area) was uniformly less than the other finalists.

(2) **RC6**

- throughput is generally average.
- RC6 seems to perform relatively better in pipelined implementations,
- non-feedback mode

**(3) Rijndael:**

- good performance in fully pipelined implementations.
- Efficiency is generally very good.

4) Serpent:

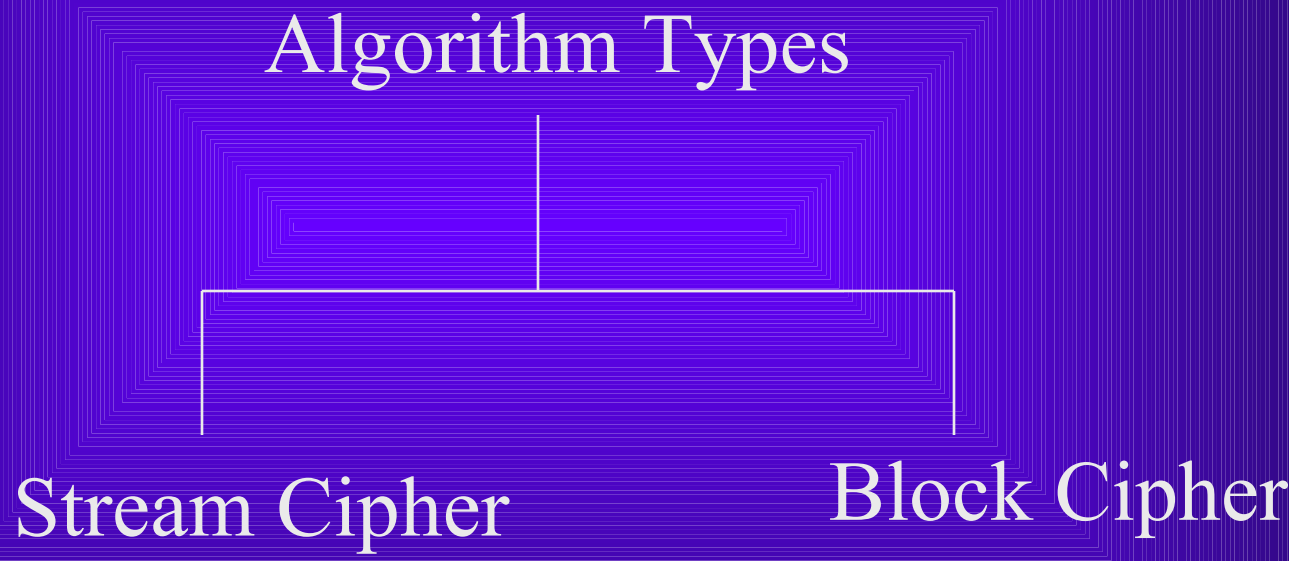
- feedback mode encryption.
- Efficiency is generally very good.

(5)Twofish:

- throughput and efficiency in the basic architecture, pipelined and unrolled implementations was generally average.

- The evaluation criteria were divided into three major categories:
  1) Security
  2) Cost, and
  3) Algorithm and Implementation Characteristics

# Symmetric Key Algorithm Types

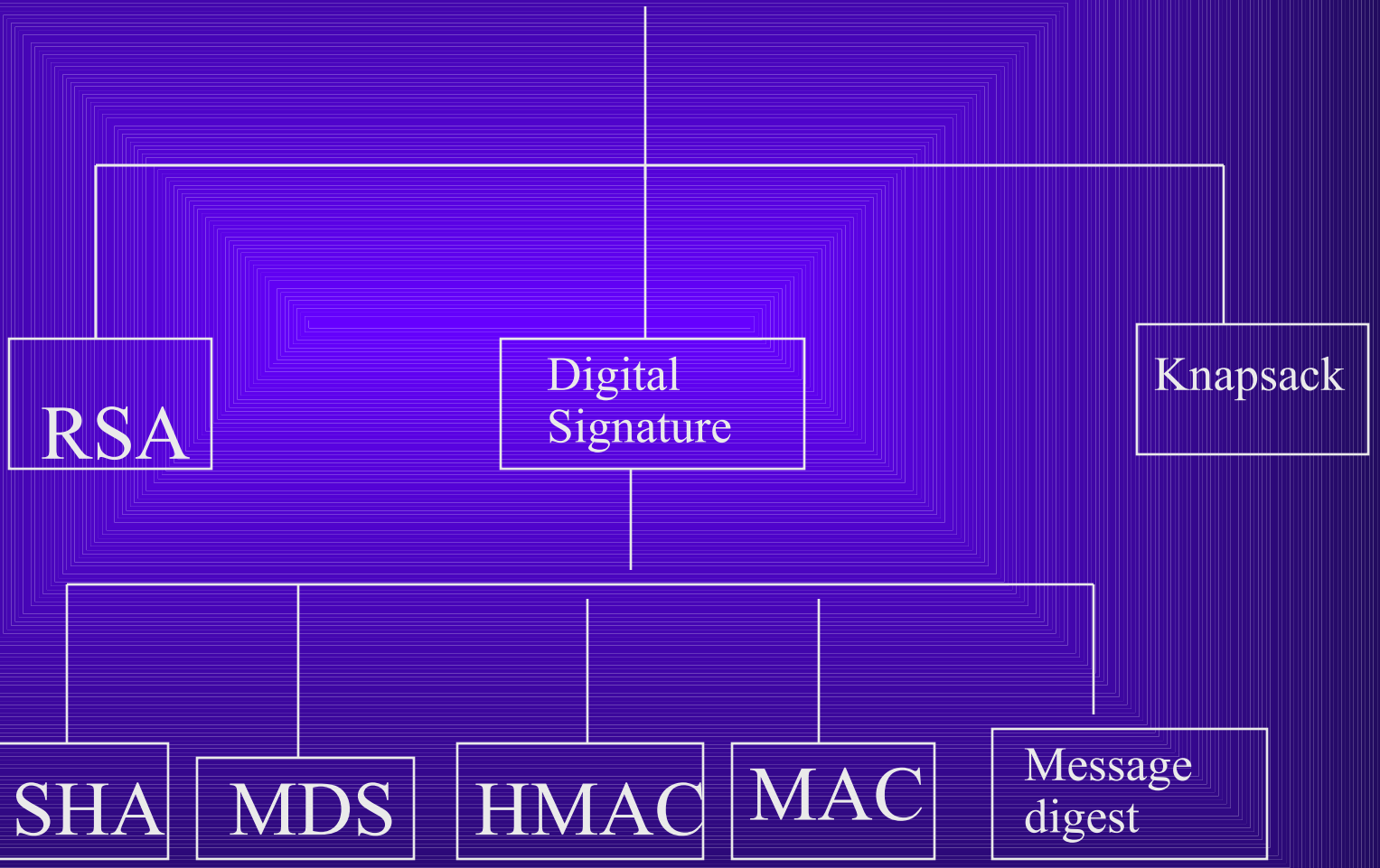


# Asymmetric key cryptography

If same key is used for encryption and decryption,we call the mechanism as symmetric key cryptography.

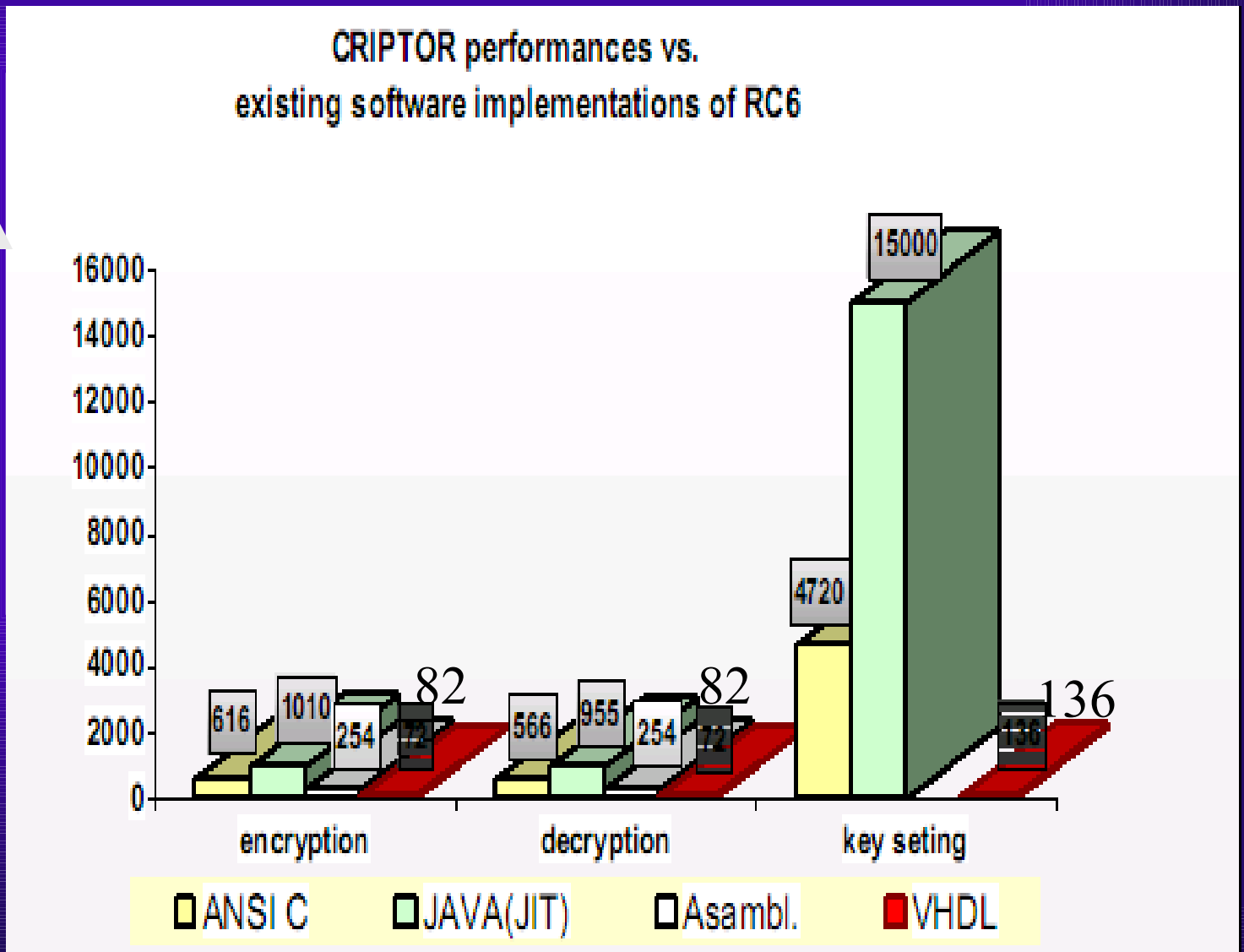
Here key pair is used one is Public key another one is Private key.

# Asymmetric key cryptography Algorithm



# Comparison B/W Software And VHDL

clock



# RC6 ALGORITHM

Why RC6?

- no key separation
- Small scale versions allowed experimentation
- Supports 32/64 bit processor
- High speed with minimal code memory
- Supports multi block processing
- Supports non-feedback mode operations
- Max potential for parallelism when multiple streams are processed

- RC6-w/r/b

  w=32/16, r=20, b=16/24/32

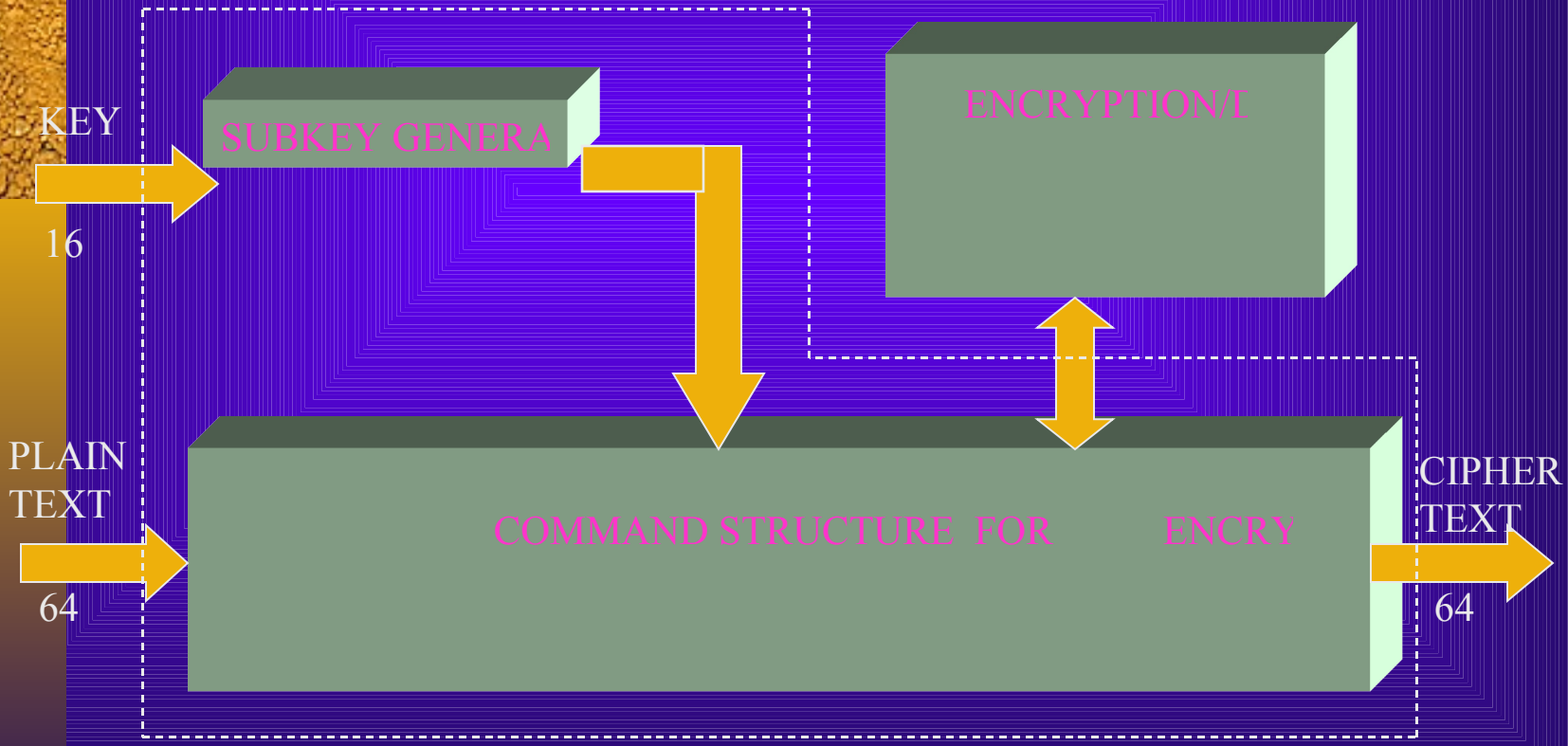
# RC6 Overview

- Advantages:
  1) Fast and flexible
  2) Based on RC5: secure
  3) Supports 32/64 bit processor
- Disadvantages:
  1) Integer multiplications on rotations
  2) Not Universally Practical

# Quick Overview

- We divide 64 bit plain text into four blocks of 16 bit and called it as A,B,C,D.
- Key length we used is also 16 bit.
- We used Spartan XC3s400pq208 chip for synthesis

# BLOCK DIAGRAM :



# Basic Operations:

RC6-w/r/b basic operations.

**1)a + b** :integer addition modulo 2w

**2)a - b** :integer subtraction modulo 2w

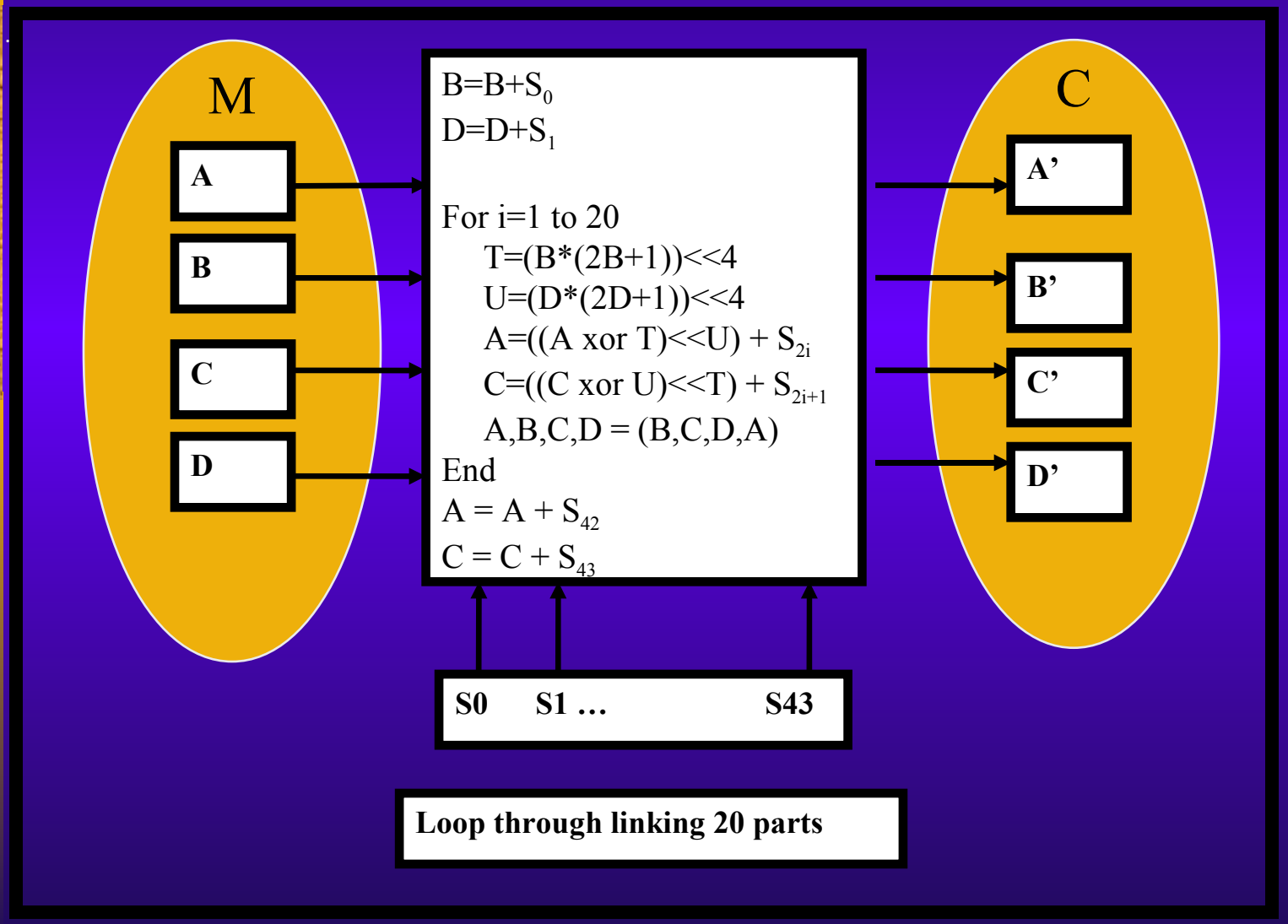
**3)a □ b** :bitwise exclusive-or of w-bit words

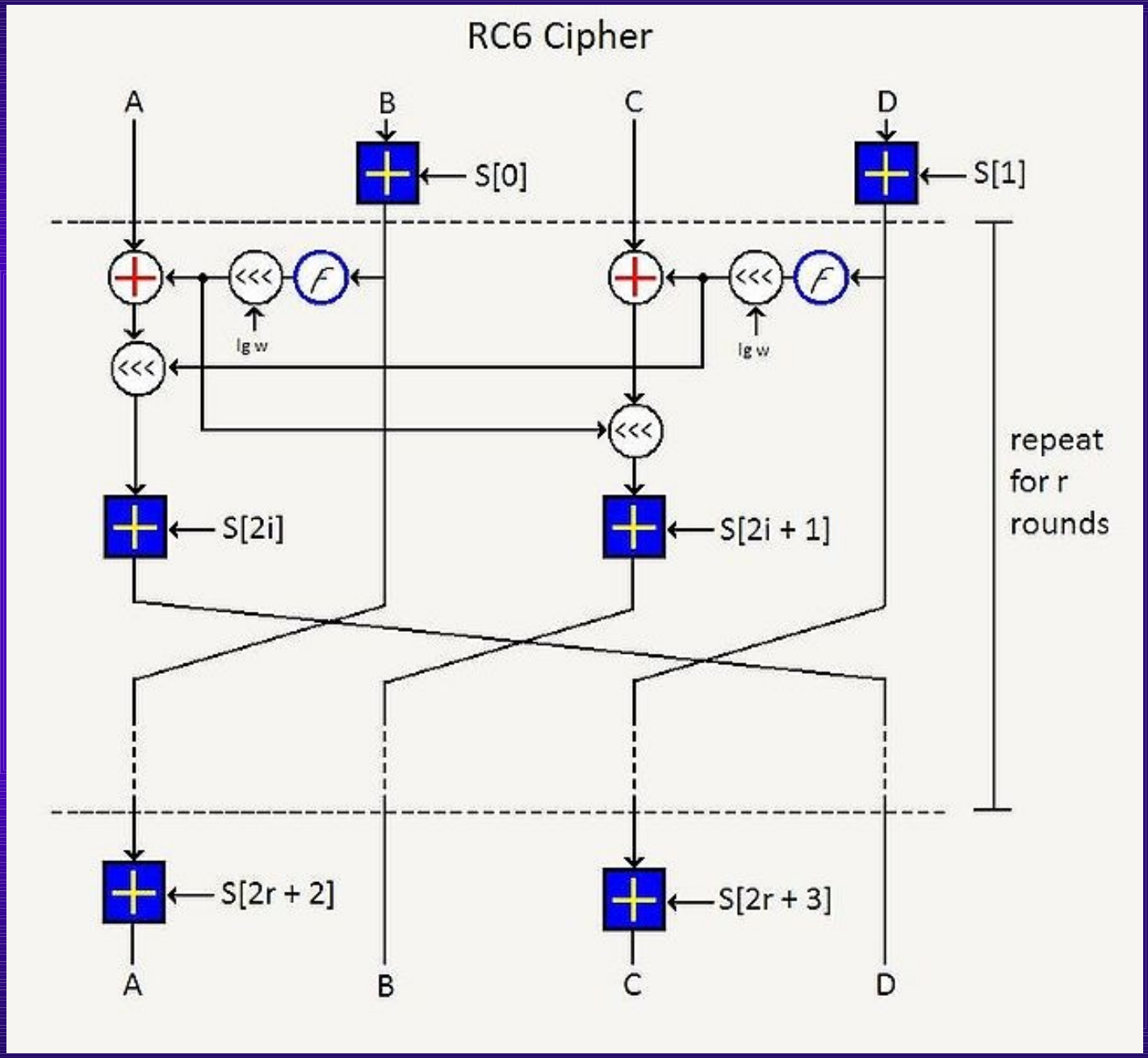
**4)a x b** :integer multiplication modulo 2w

**5)a <<< b** :rotate the w-bit word a to the left by the amount given by the least significant lgw bits of b

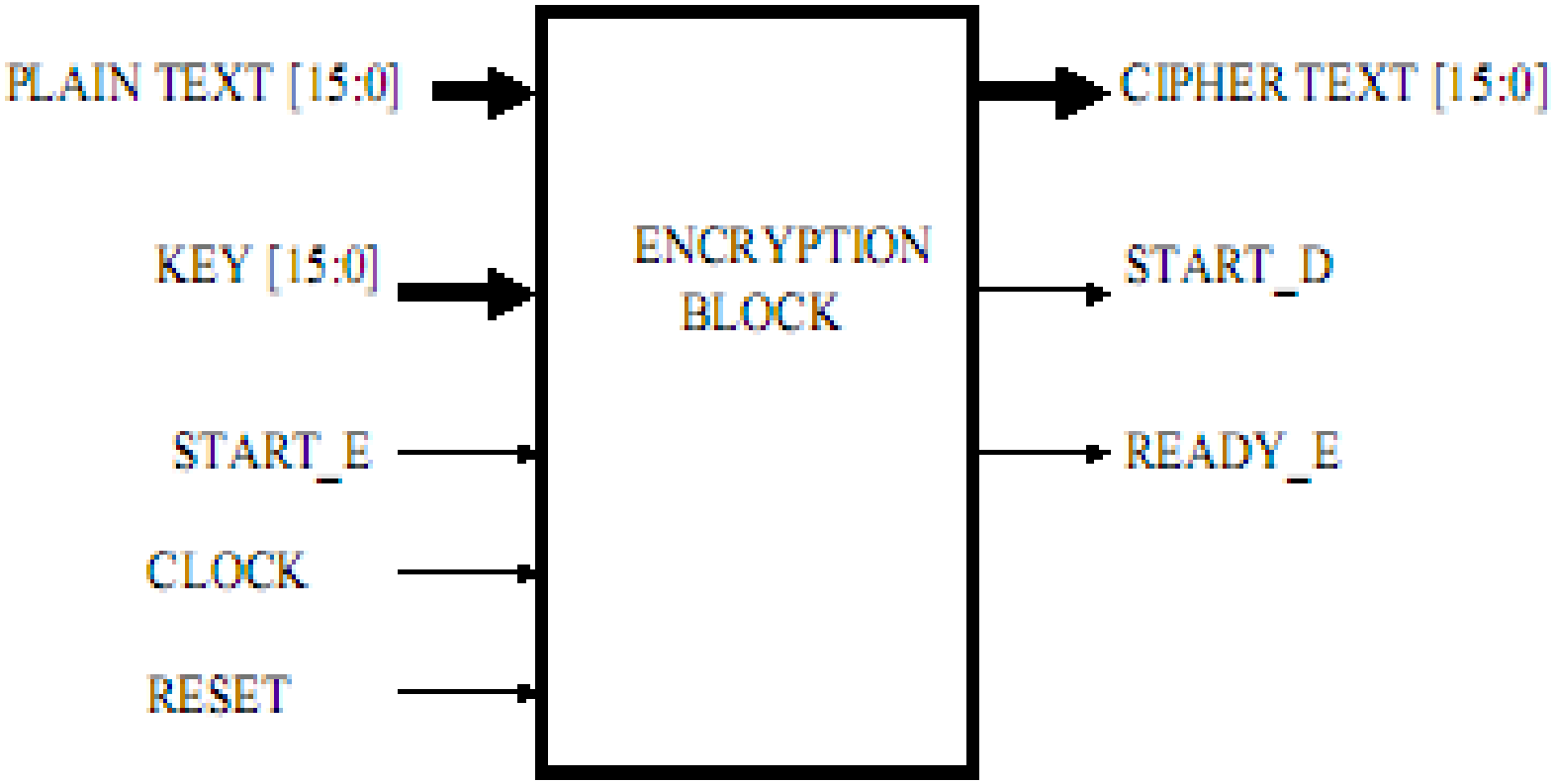
**6)a >>> b** **:**rotate the w-bit word a to the right by the amount given by the least significant lgw bits of b

# Encryption Block Diagram

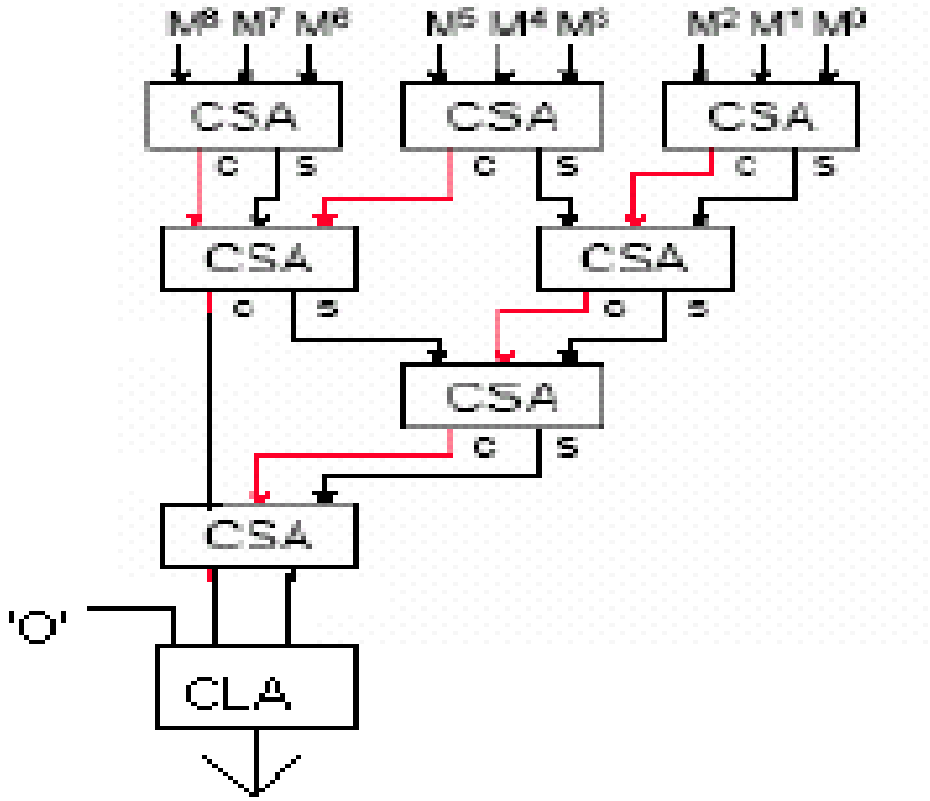


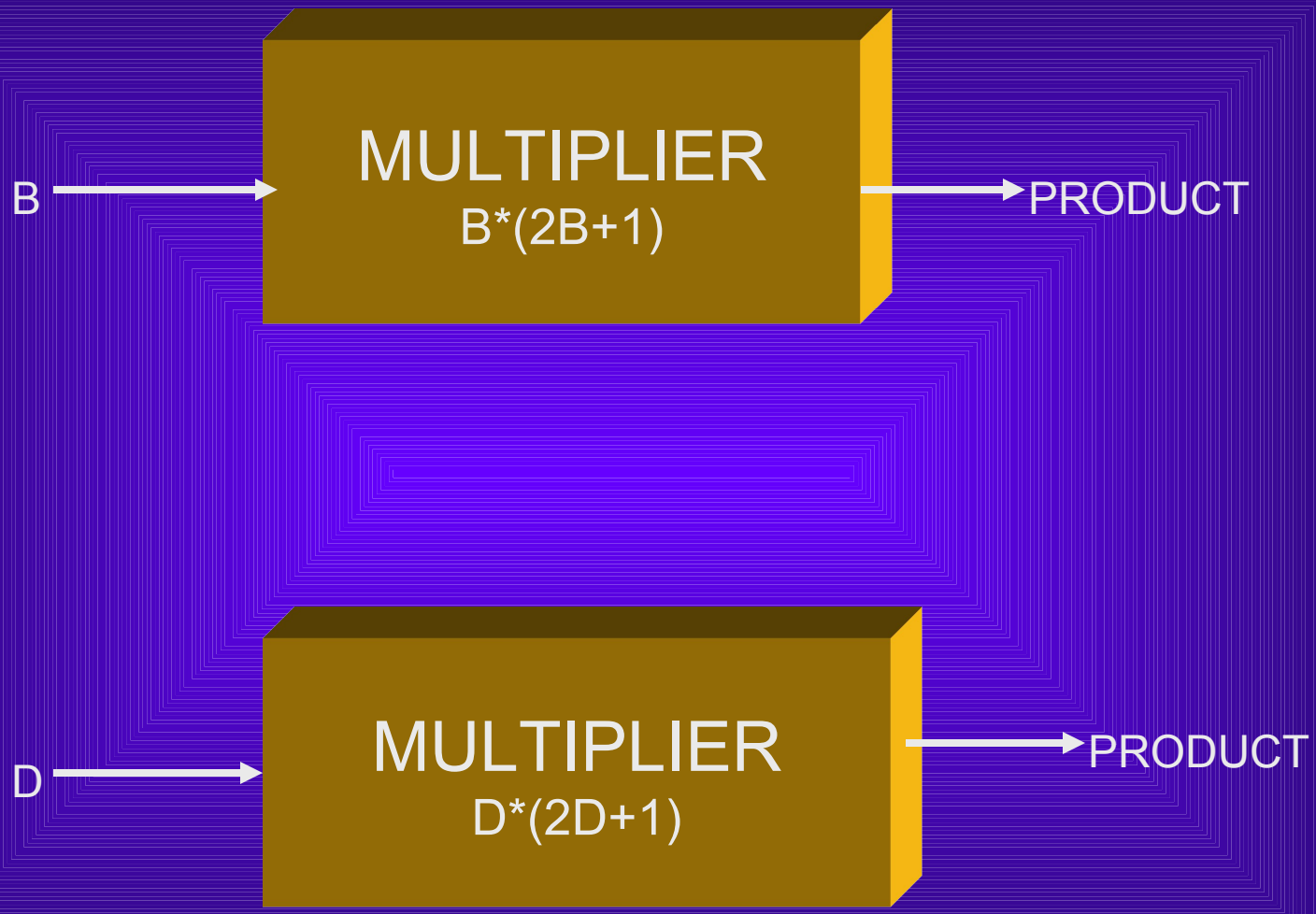

RC6 Cipher
A
B
C
D
S[0]
S[1]
lg w
lg w
S[2i]
S[2i + 1]
repeat
for r
rounds
S[2r + 2]
S[2r + 3]
A
B
C
D

# INPUT BLOCK

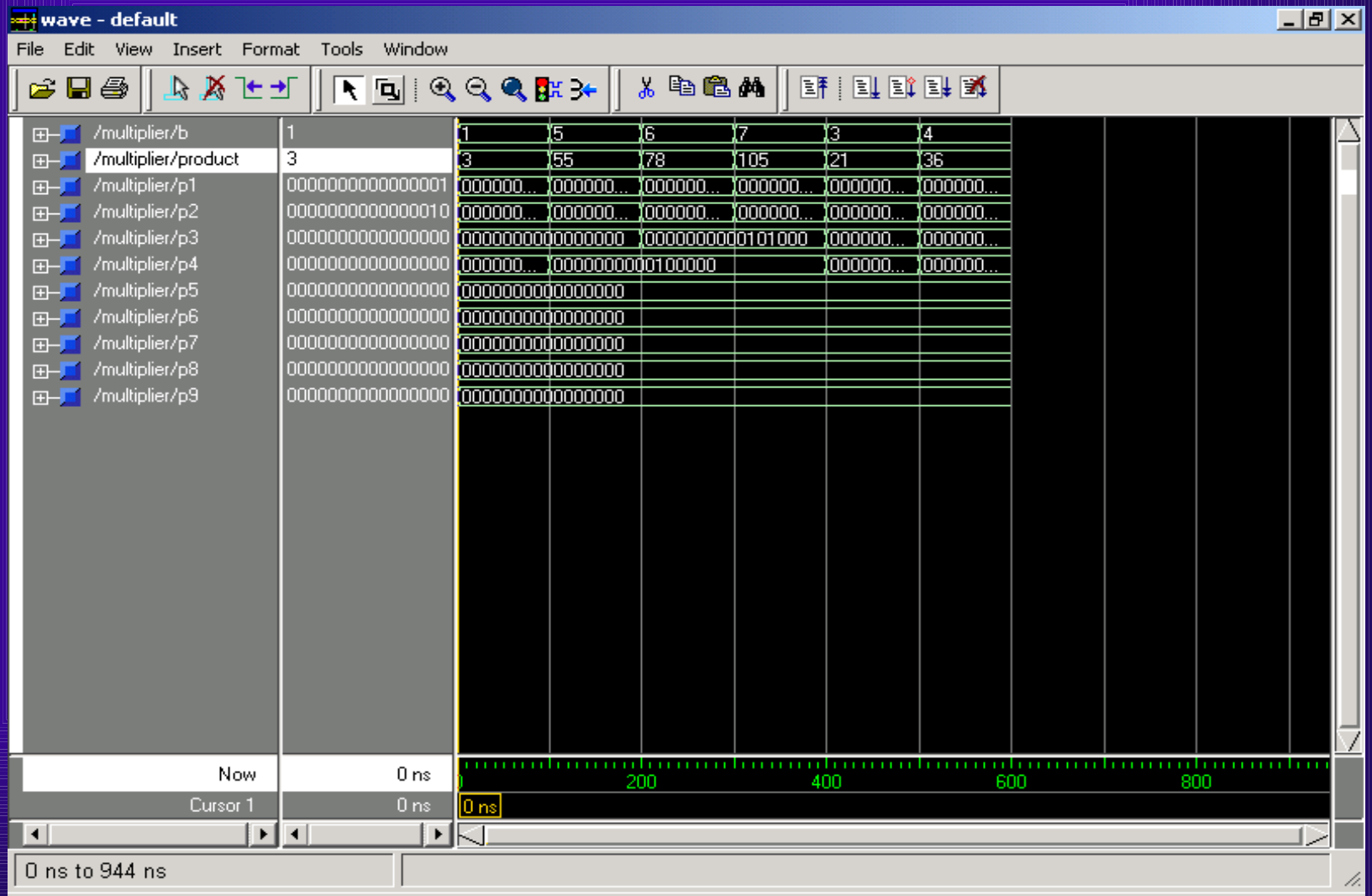

PLAIN TEXT [15:0]
KEY [15:0]
START_E
CLOCK
RESET
ENCRYPTION BLOCK
CIPHER TEXT [15:0]
START_D
READY_E

# Wallace tree

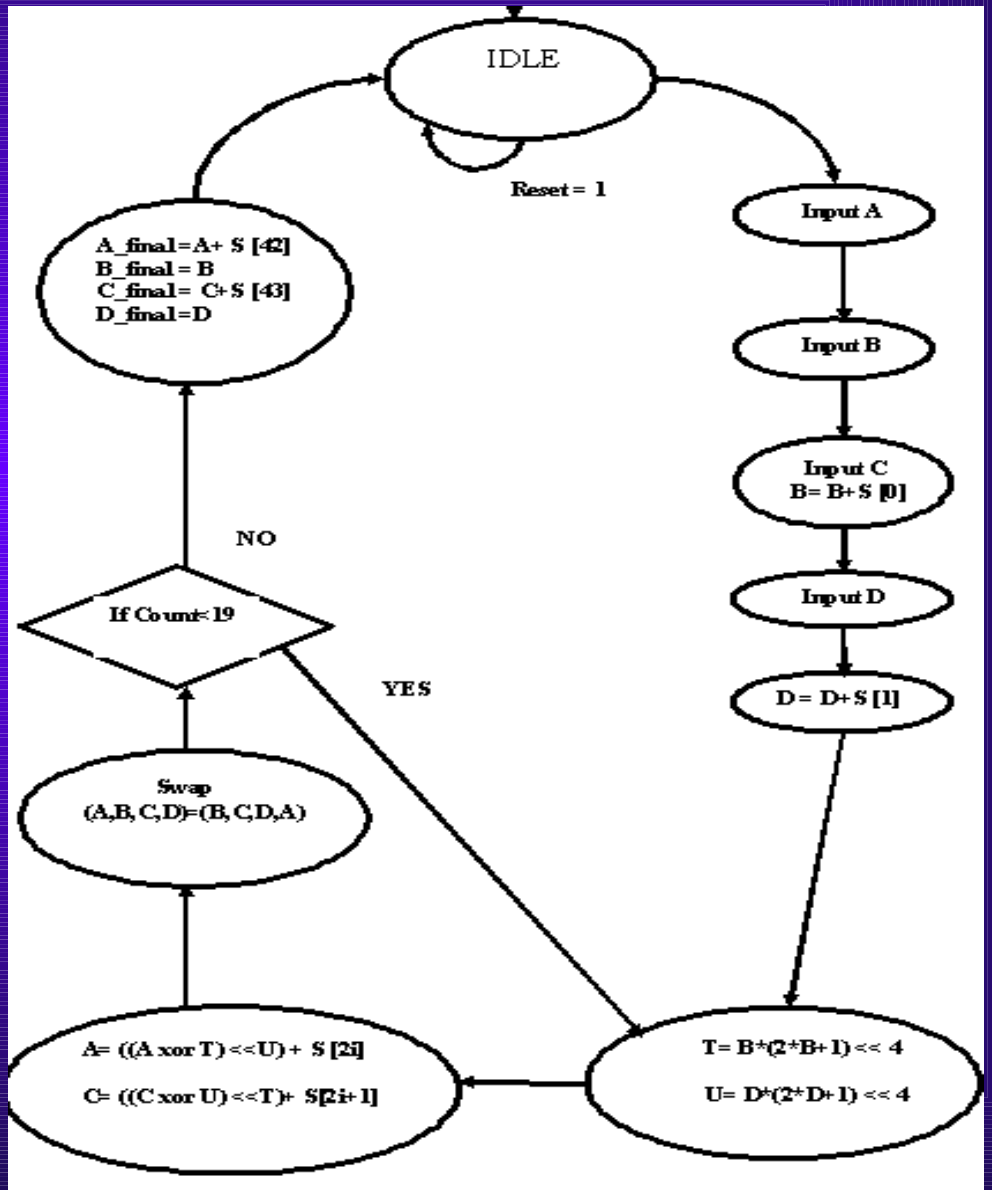



B
MULTIPLIER
B*(2B+1)
PRODUCT
D
MULTIPLIER
D*(2D+1)
PRODUCT

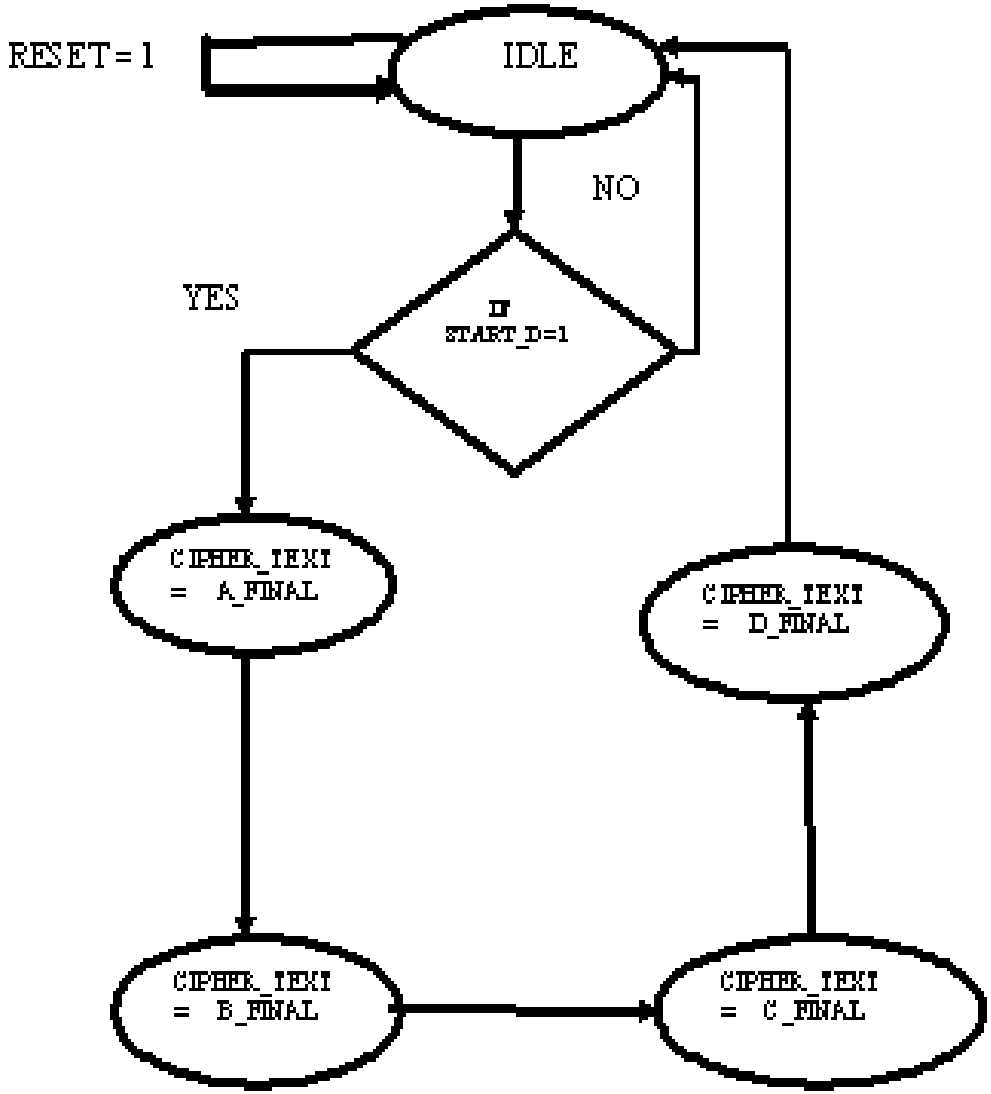
# MULTIPLIER SIMULATION



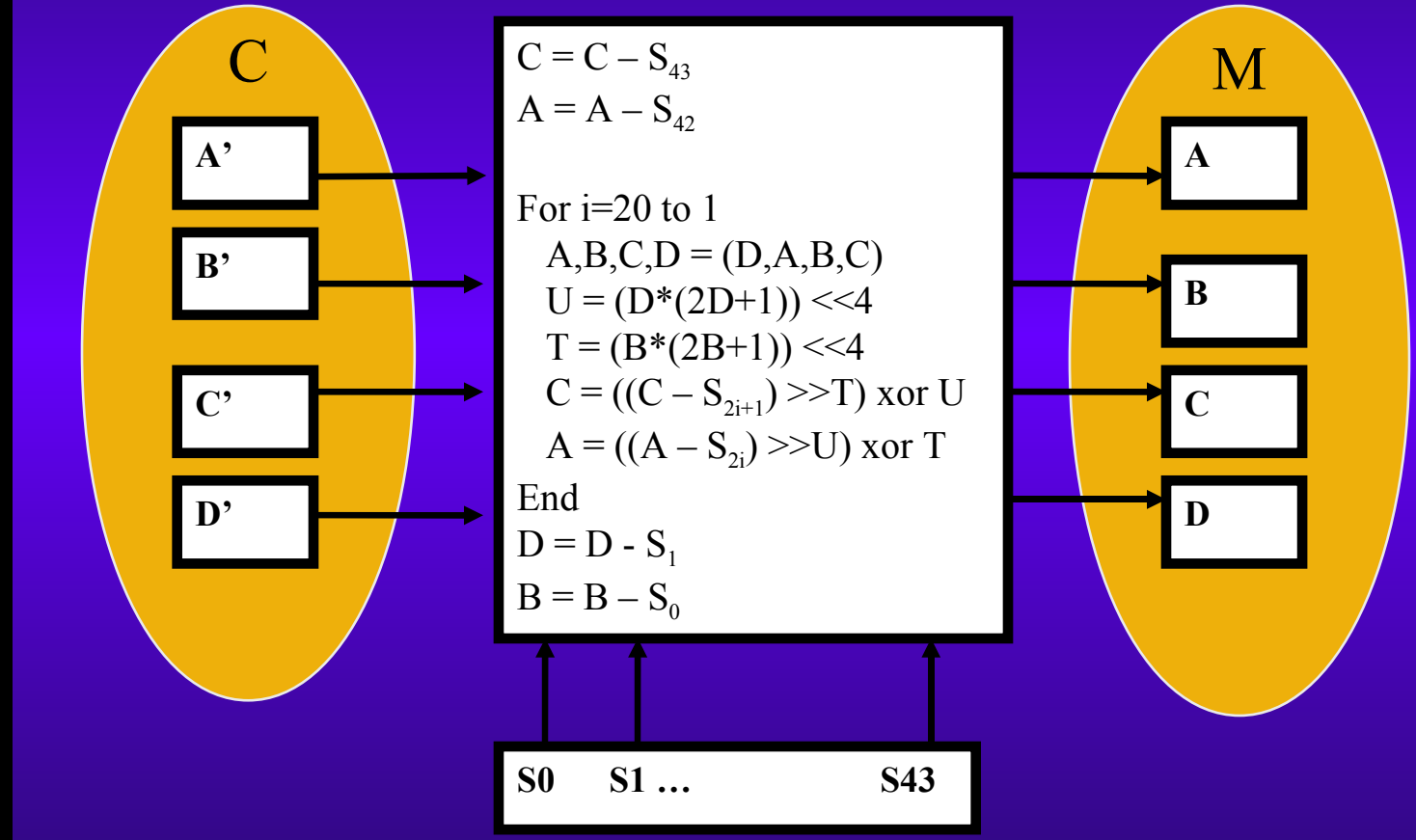
# STATE MACHINE For Encryption



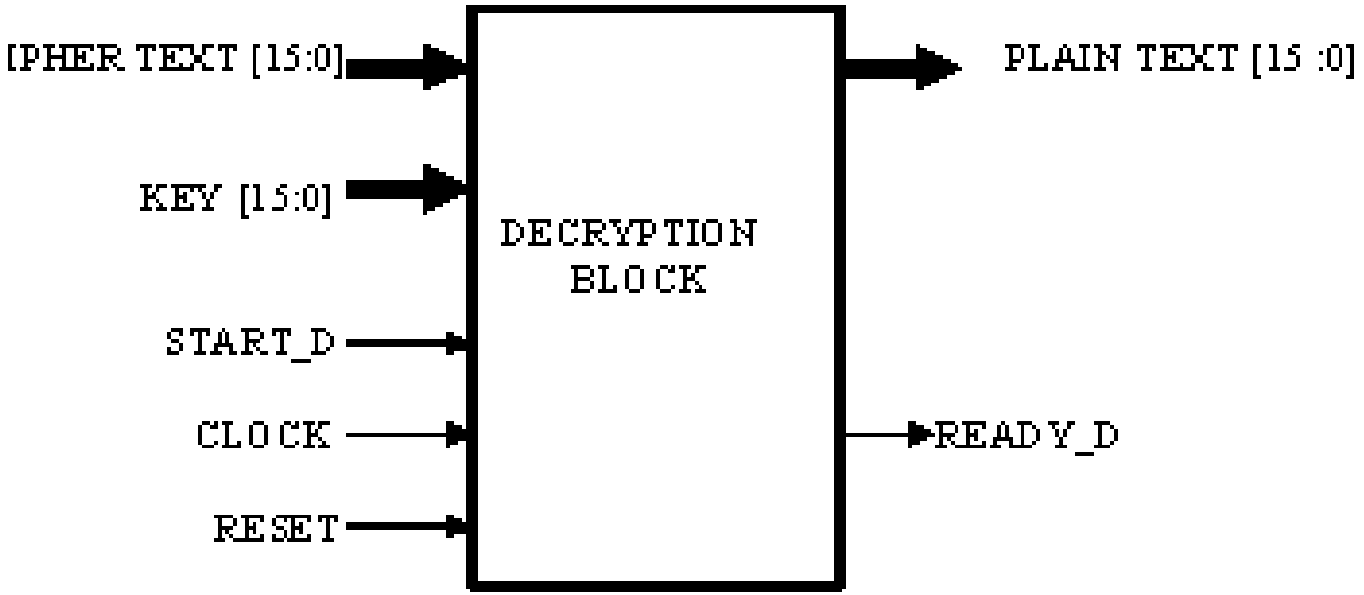
# STATE MACHINE For O/P Encryption



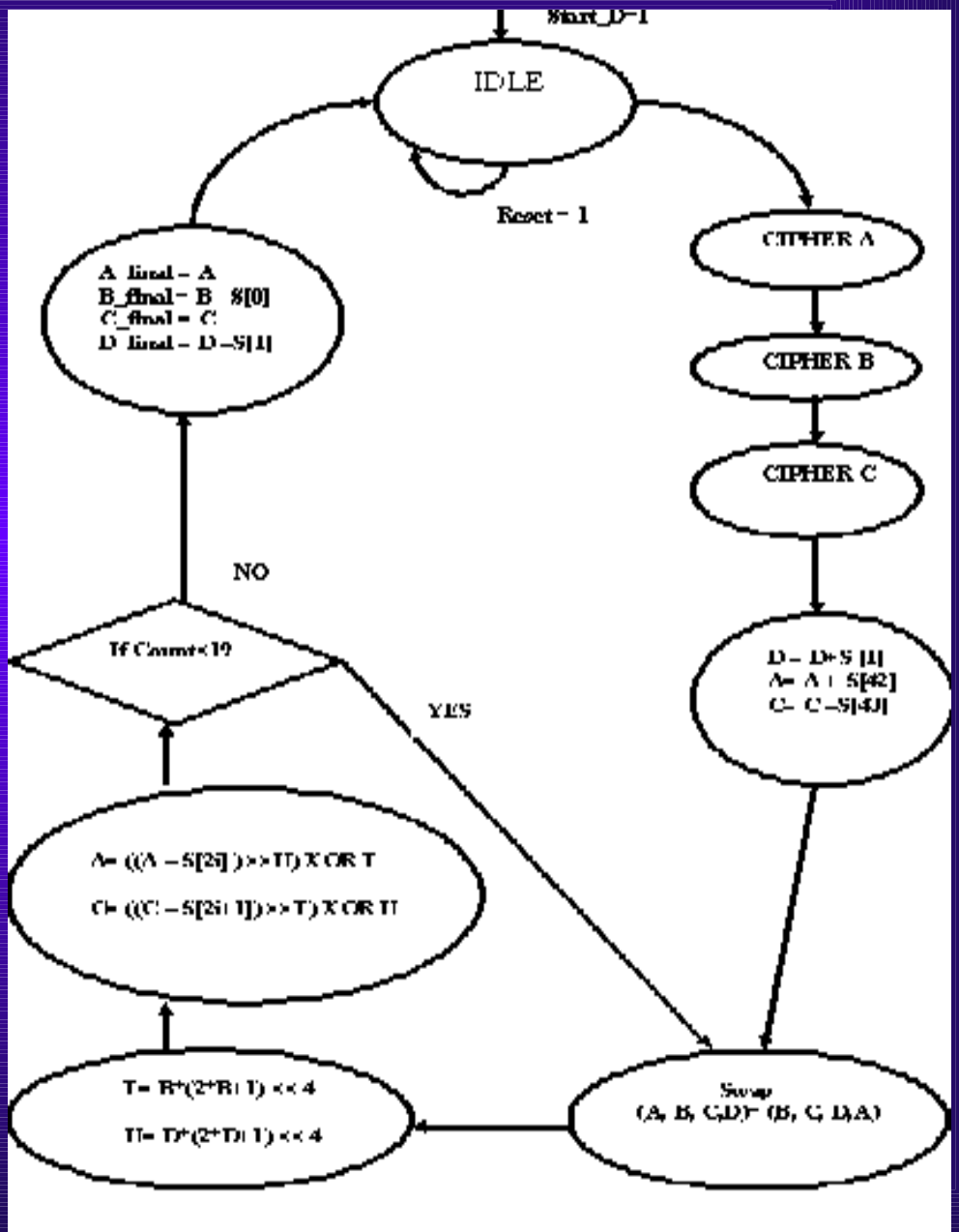
# Decryption Block Diagram



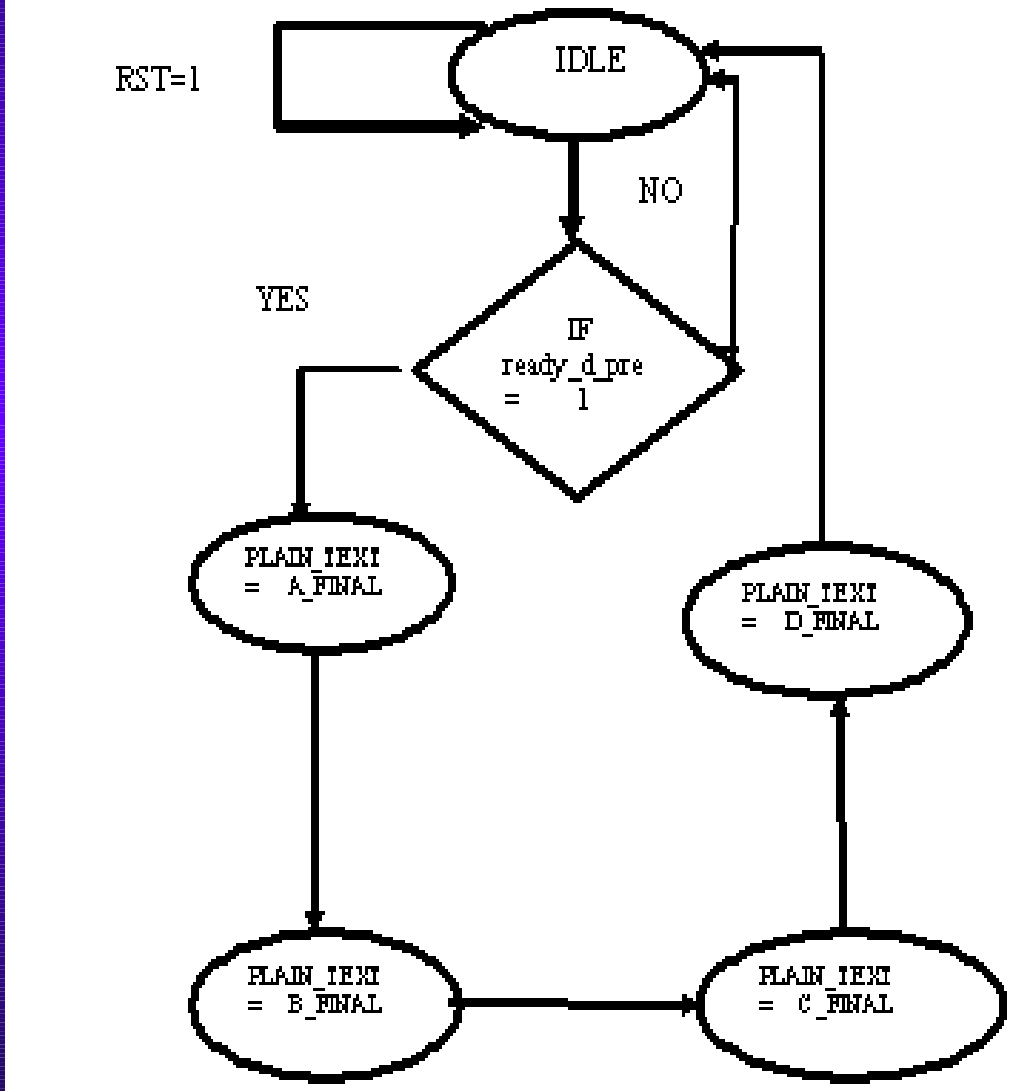
# OUTPUT BLOCK



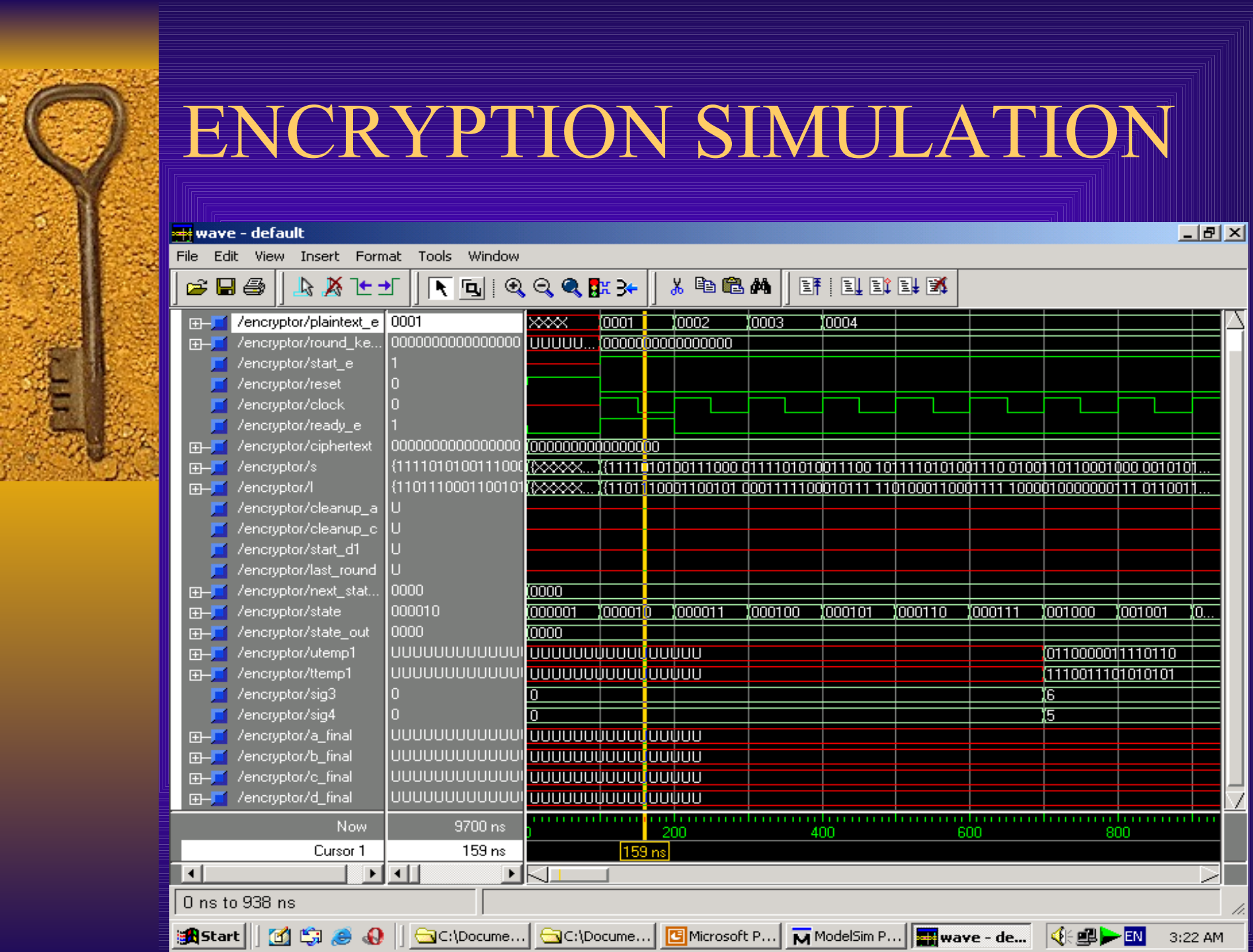
# STATE MACHINE For Decryption



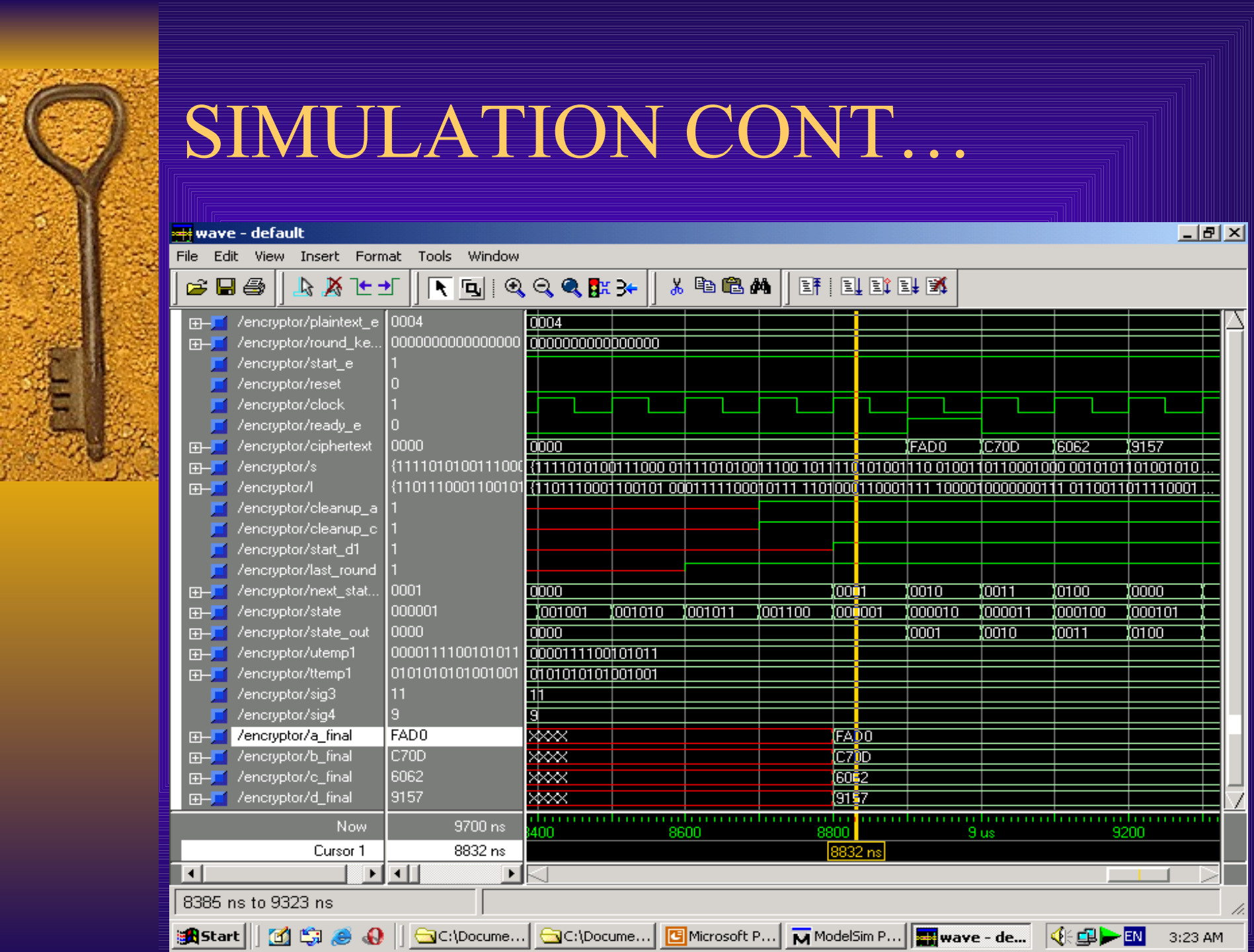
# STATE MACHINE FOR Decryption



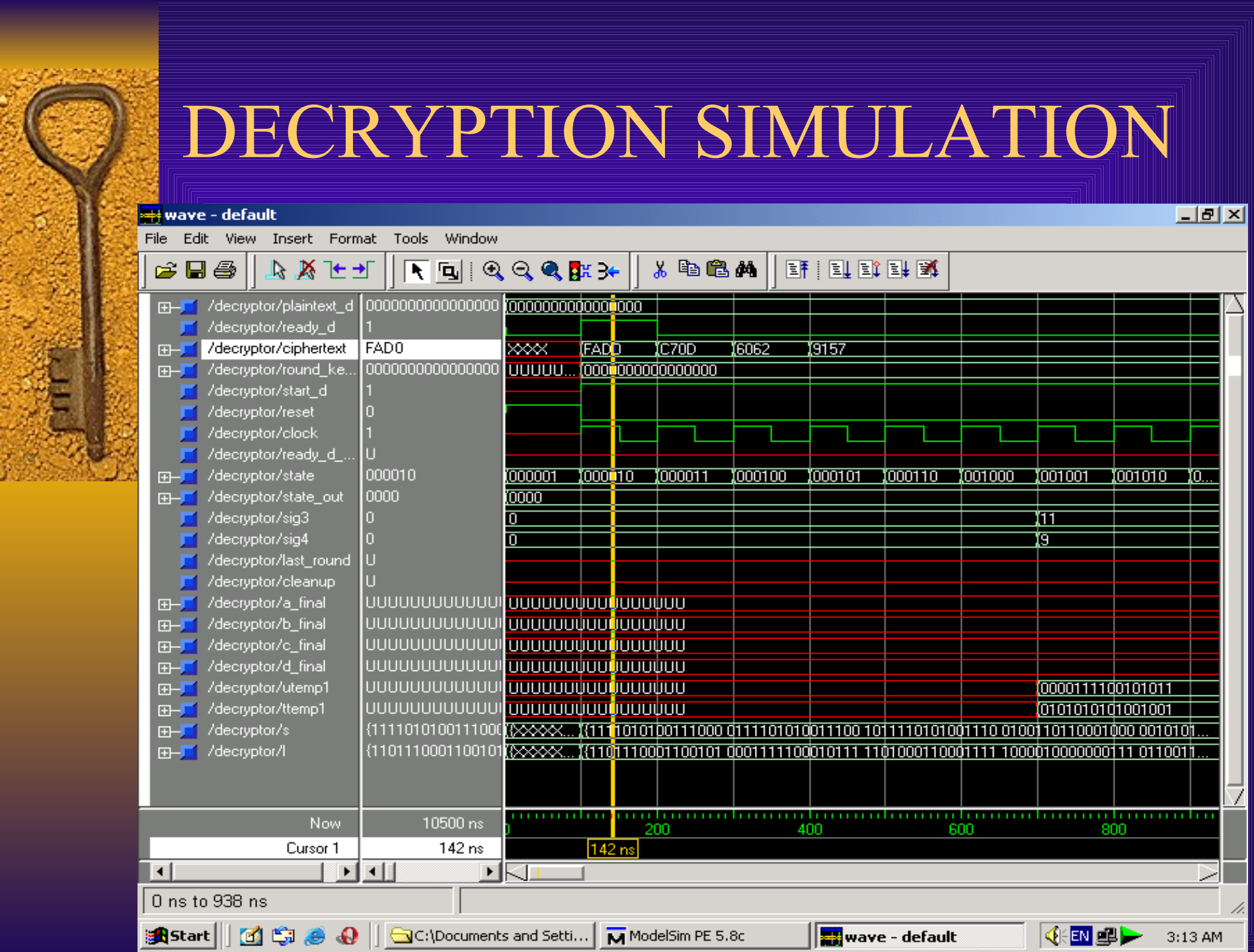
# ENCRYPTION SIMULATION



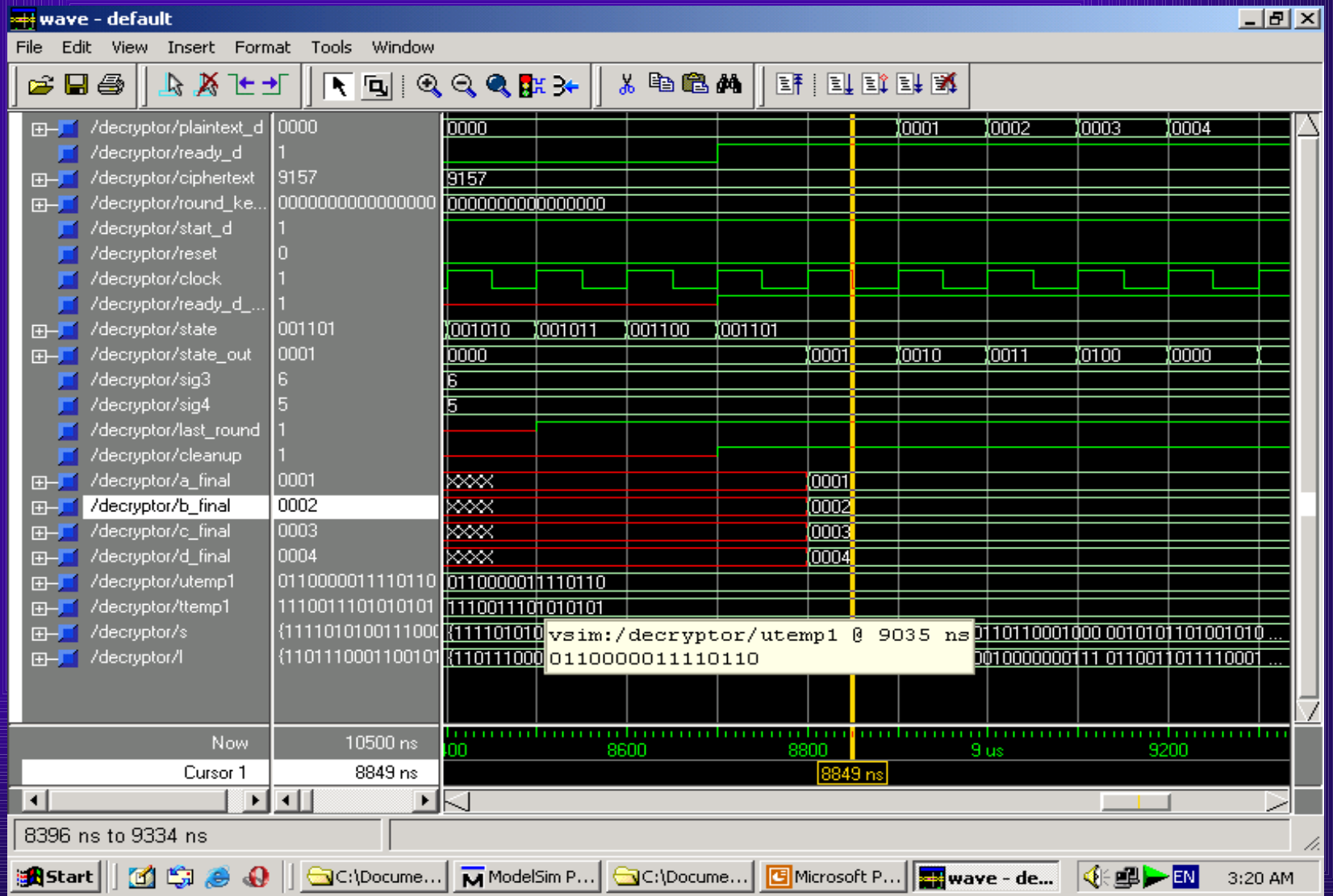
# SIMULATION CONT…



# DECRYPTION SIMULATION



# SIMULATION CONT..



# Synthesis

We used Spartan3 XC3s400pq208.

Large chip because of added keyset and amount of calculations.

# TECHNICAL SPECIFICATIONS:

- Software:- Xilinx Foundation Series 6.2i
- Hardware:- Spartan-3 Kit

| | |
|---|---|
| - Device : | XC3S400 |
| - System Gates: | 400k |
| - Equivalent Logic Cells: | 8,064 |
| - CLB Array (One CLB = Four Slices) | |
| -Rows: | 32 |
| -Columns: | 28 |
| -Total CLBs: | 896 |
| - Distributed RAM Bits (K=1024): | 56K |
| - Block RAM Bits (K=1024): | 288K |
| - Dedicated Multipliers: | 16 |
| - DCMs: | 4 |
| - Maximum User I/O: | 264 |

# Synthesis Report For Encryption

Selected Device : XC3s400pq208-5

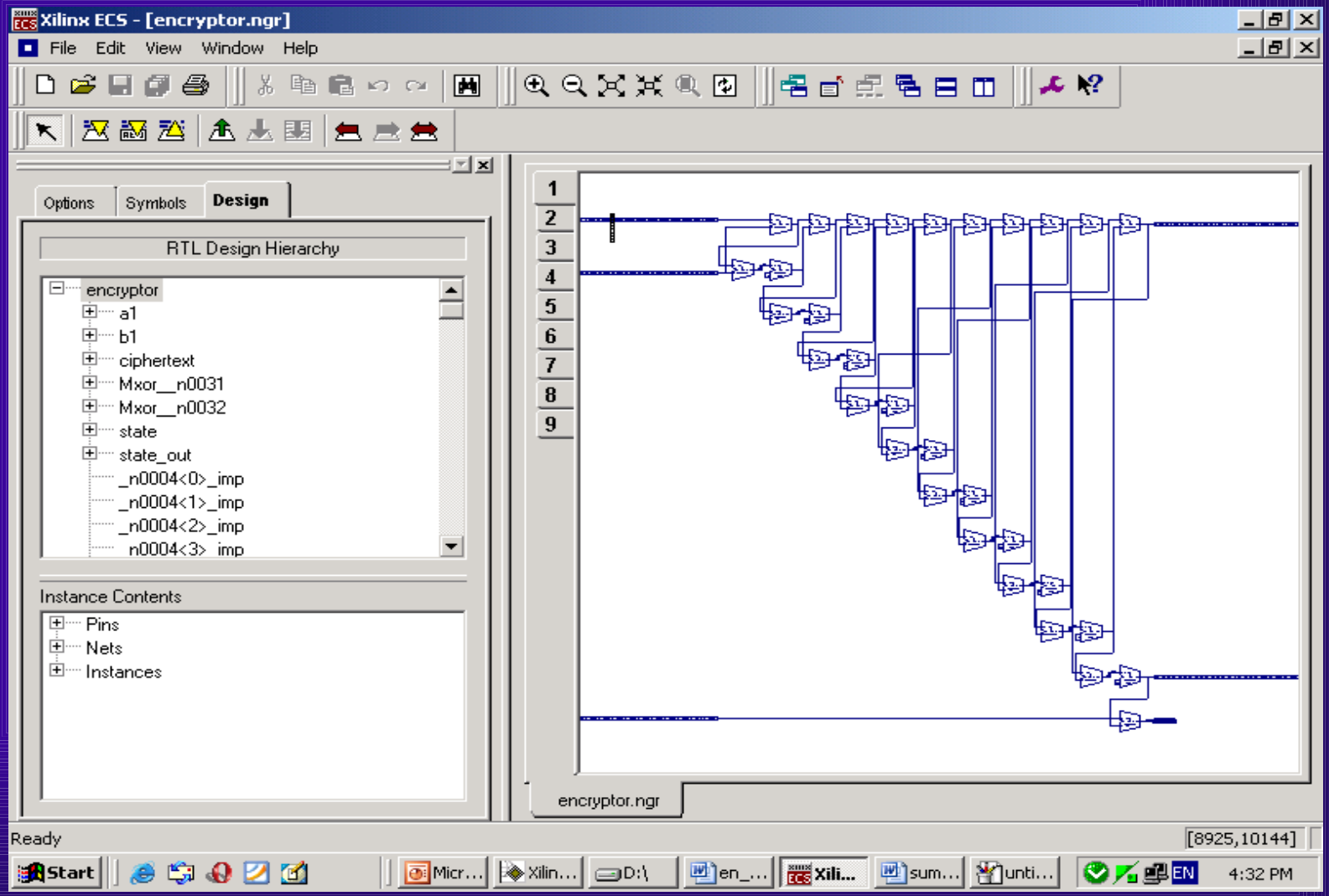
- Number of Slices: 1570 out of 3584 43%
- Number of Slice Flip Flops: 222 out of 7168 3%
- Number of 4 input LUTs: 2729 out of 7168 38%
- Number of bonded IOBs: 51 out of 141 36%
- Number of GCLKs: 1 out of 8 12%

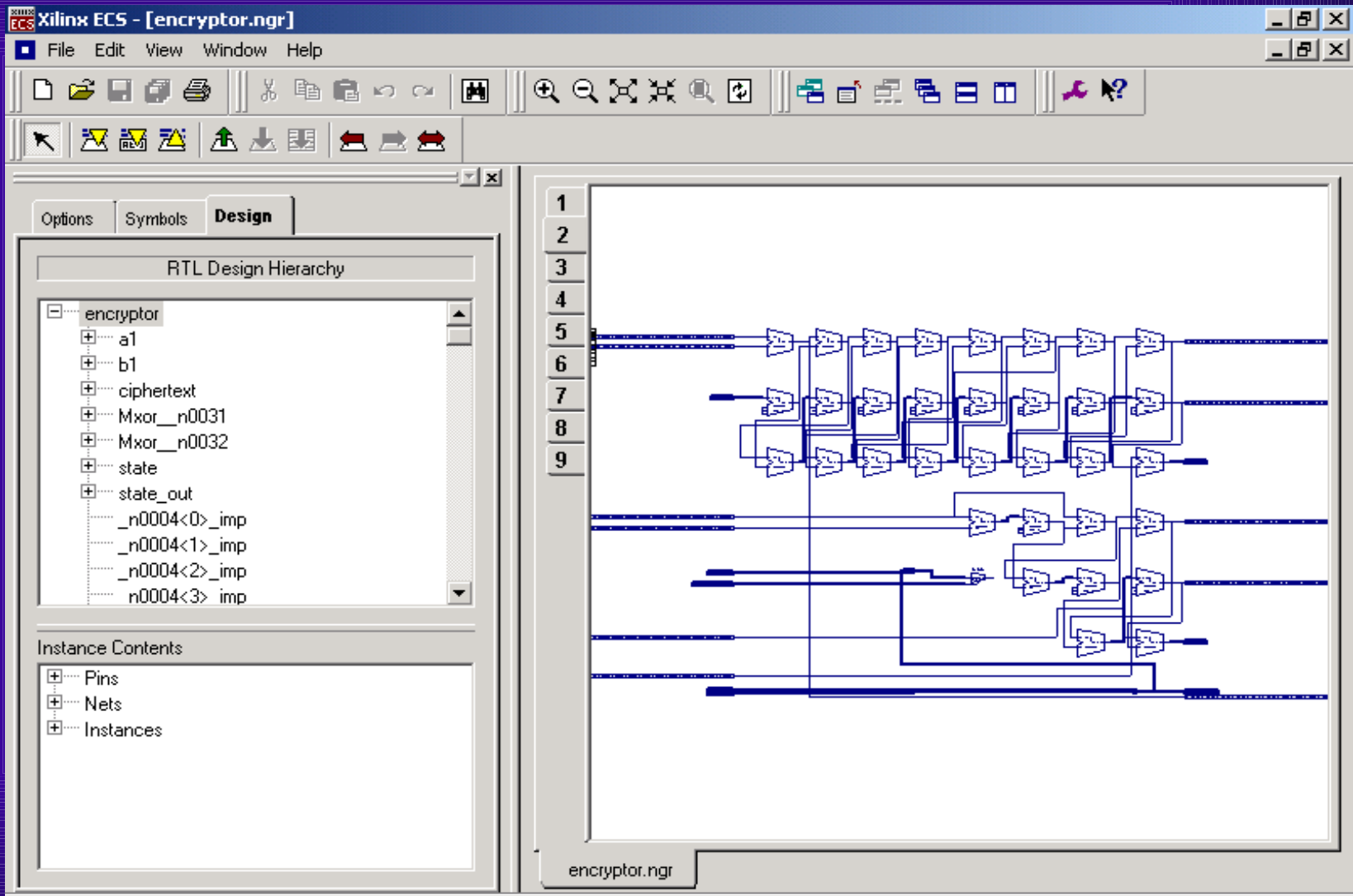
# Synthesis Report For Decryption

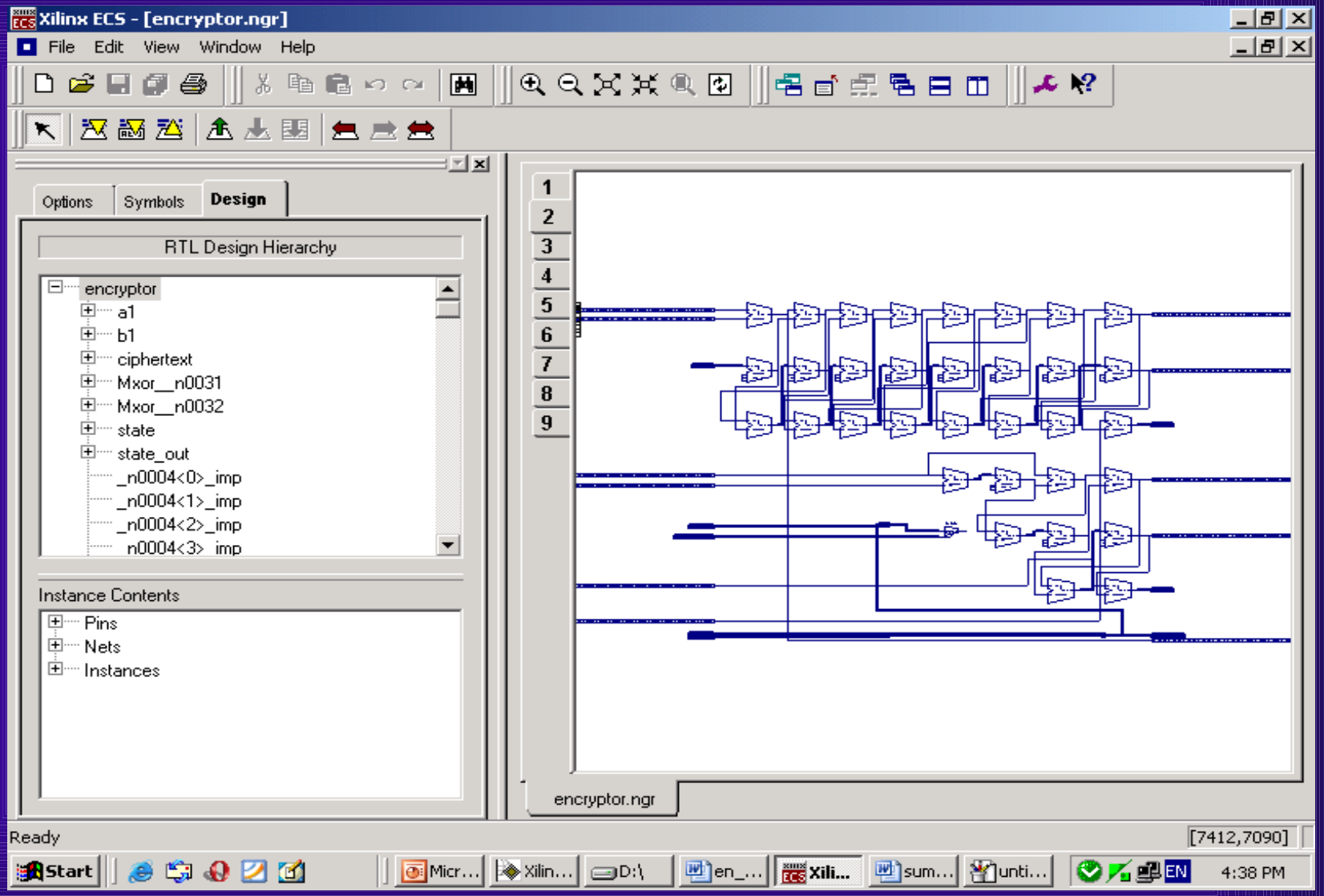
Selected Device : XC3s400pq208-5

- Number of Slices: 1533 out of 3584 42%
- Number of Slice Flip Flops: 219 out of 7168 3%
- Number of 4 input LUTs: 2672 out of 7168 37%
- Number of bonded IOBs: 51 out of 141 36%
- Number of GCLKs: 1 out of 8 12%

# The Circuit Overview




Xilinx ECS - [encryptor.ngr]
File Edit View Window Help
Options Symbols Design
RTL Design Hierarchy
encryptor
a1
b1
ciphertext
Mxor__n0031
Mxor__n0032
state
state_out
_n0004<0>_imp
_n0004<1>_imp
_n0004<2>_imp
_n0004<3>_imp
Instance Contents
Pins
Nets
Instances
1
2
3
4
5
6
7
8
9
encryptor.ngr
Ready
[8397,2918]
Start
4:33 PM


Xilinx ECS - [encryptor.ngr]
File Edit View Window Help
Options Symbols Design
RTL Design Hierarchy
encryptor
a1
b1
ciphertext
Mxor__n0031
Mxor__n0032
state
state_out
_n0004<0>_imp
_n0004<1>_imp
_n0004<2>_imp
_n0004<3>_imp
Instance Contents
Pins
Nets
Instances
1 2 3 4 5 6 7 8 9
encryptor.ngr
Ready
[7412,7090]
Start
4:38 PM

# Synthesis Summary

| | Encryption Chip | Decryption Chip |
|---|---|---|
| Area Used | 30.2% | 29.8% |
| Time Delay | 49.814ns | 50.968ns |
| Memory used | 99100 kilobytes | 98908 kilobytes |

# APPLICATION AREA:

- Internet E-Commerce
- Mobile telephone networks
- Bank automated teller machines
- Digital rights managements to restrict the use of copyrights material.
- Secret communication.

# FUTURE SCOPE:

- The length of the key can be made variable.
- The word size can be increased.
- Smart cards, Mobile, Digital Camera and ATM can adopt this scheme by far greater extent.

# CONCLUSIONS:

- RC6 is considered as a secured and elegant choice due to its simplicity, security, performance and efficiency.
- It appears that RC6 is best suited for implementation in the targeted Xilinx FPGA (Spartan-3).
- Our studies reveal that multiplication and addition are the major bottlenecks as far as speed of encryption in the RC6 cipher is concerned. Nevertheless, up to a great extent this shortcoming was tackled using pipelining in our design.
- Consequently, since RC6 works best in non-feedback mode, the highest Speed/Area ratio can be achieved in the same

# REFERENCES:


[1] Douglas L. Perry, “VHDL Programming by Example”, Tata McGraw-Hill Edition 2002, 1-266.

[2] Atul Kahate, “Cryptography and Network Security”, Tata McGraw-Hill Edition 2003,2,29,40,43,63,75,98,107.

[3] Ioan Mang, Greda Erica Mang, “Hardware Implementation with offline test capabilities of the RC6 block cipher” 0-7803-7625-0/02/$17.00© 2002 IEEE. British Crown Copyright.

[4] M. Riaz and H .M. Heys,”The FPGA Implementation of the RC6 and CAST-256 Encryption Algorithms”, Proceedings of the 1999 lEEE Canadian Conference on Electrical and Computer Engineering, Shaw Conference Center, Edmonton, Alberta, Canada May 9-12 1999

[5] S. Contini, R.L. Rivest, M.J.B. Robshaw and Y.L. Yin,” The Security of the RC6 Block Cipher”, Version 1.0, RSA laboratories, August 20, 1998.

# Thanks, and here's a random comic