



NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA, SURATHKAL

P.O SRINIVASNAGAR, MANGALORE-575025

Placements 2009-10

PARUL CHAURASIA

B.TECH

Branch : COMPUTER SCIENCE

Gender : FEMALE

Reg. No. : 06CO43

Date Of Birth : OCTOBER-4-1986

Email- Id : stylishparul@gmail.com

Phone : 0755-2775475

Mobile : 9945614004

C.G.P.A. : 7.36

PRESENT ADDRESS	PERMANENT ADDRESS
ROOM NO. 13 III BLOCK, GIRLS HOSTEL NITK SURATHKAL KARNATAKA 575 025	3/3, PHASE II JHARNESHWAR COMPLEX JAWAHAR CHAUK, BHOPAL MADHYA PRADESH 462 003

B.TECH DETAILS

SEMESTER	YEAR	S.G.P.A	C.G.P.A
SEMESTER 1	DEC 2006	8.14	8.14
SEMESTER 2	MAY 2007	7.92	8.04
SEMESTER 3	DEC 2007	7.74	7.95
SEMESTER 4	MAY 2008	4.76	7.25
SEMESTER 5	DEC 2008	6.28	7.05
SEMESTER 6	MAY 2009	7.06	7.39
SEMESTER 7	DEC 2009	7.11	7.36

PRE DEGREE, 10+2th, 10th DETAILS

DISCIPLINE	INSTITUTION	UNIVERSITY /BOARD	YEAR	% MARKS
Xth	ST. MARY	M.P. STATE BOARD	2002	85.8%
XIIth	ST. MARY	M.P. STATE BOARD	2004	86%

SUPPLEMENTARY INFORMATION

EXTRA CURRICULAR ACTIVITIES

1. I am an executive member of Indian Society for Technical Education NITK.
2. I am an executive member and treasurer of Management Forum NITK.
3. I am an executive member of SPIC MACAY Mangalore Chapter, NSS NITK, DDFC NITK.
4. I was the Year Representative of 2nd year girls in CRRESCENDO-07.
5. I am a voracious reader and like Sydney Sheldon, Arthur Conan Doyle, J.K.Rowling.

ABOUT MYSELF

I am a good learner and a very enthusiastic person. I am very friendly and get along well with people. I am very hard working, confident, adaptable and ambitious person with good communication skills. I take my work very seriously. I love adventure and excitement.

CO-CURRICULAR ACTIVITIES

1. Summer project under Prof.Tim Poston NIAS, IISc campus May-June 2009.
To develop an OGRE graphics 3D tool application to display virtual objects using interactive shape and feel with the help of 3D Boolean operations
2. Training at BSNL Bhopal May-June 2008.
Study and analysis of Global Systems for Mobile Communications
3. Elliptic Curve Cryptographic Security in Transmission Control Protocol.
Building security functions into the TCP protocol using Elliptic Curve Cryptography, making TCP secured thus making Application Layer free from security issues and providing process to process security.
4. Other Curriculum Mini Projects.
 - i. Software Engineering Project titled "Design and Implementation of Data Dependent AES(Symmetric Private Key Block Cryptography Algorithm)" under Mahendra Pratap Singh - Lecturer Computer Science Department, NITK (6th Semester project).
 - ii. Compiler Project titled "Implementation of Recursive Descent Parser with Elimination of Left Recursion and Left Factoring" under B R Chandaverkar Lecturer, Computer Science Department, NITK(6th Semester project)
 - iii. Distributed DOS Attack Tool with IP-Spoofing Capabilities
Tool to perform Distributed Denial of Service attack with forged IP (IP Spoofing). This tool helps the researchers and developers to design, implement and to test solutions against Denial of Service attacks
5. Research Publication
 - i. International Conference on Cryptography, Coding and Information Security ICCIS 2010 March 29-31, 2010 (Rio de Janeiro, Brazil)
Accepted Paper titled "Elliptic Curve Cryptographic Security in Transmission Control Protocol" yet to be presented in the conference. This paper proposes adding security features into Transmission Control Protocol by superimposing security features into existing TCP with Elliptic Curve Cryptography.

CO-CURRICULAR ACTIVITIES

- ii. International Conference of Information Security and Internet Engineering
WCE - ICISIE 2010 June 30 - July 2 2010 (London, U.K)
Accepted Paper titled "Fast Generation of Pseudo-Random Cryptographic Keys using Variable Speed String Rotations" yet to be presented in the conference.
This paper describes new way to generate user friendly and user defined keys and also with fast generation of cryptographic keys needed during back end applications.(Same is accepted in ICCEE-09 Dubai, ICECS-09 Dubai, and IJCSNS Journal)
- iii. 12th International Conference on Information Technology
ICIT - 2010 December 21-24, 2009 (Bhubaneshwar, India)
Published a paper titled "Merging of RC5 with AES - Incorporating more Flexibility and Security in AES" ISBN: 978-0-07-068014-2 (Page 70-75). This paper proposes a modified Advanced Encryption Standards (AES) algorithm thus deals with designing Data Dependent AES which has RC5 characteristics of data rotations depending on data itself.(Same was accepted in ICCEE-09 Dubai, ICECS-09 Dubai, and TRACE-09 India)
- iv. IEEE-International Advanced Computing Conference
IACC - 2009 March 6-7, 2009 (Pondicherry, India)
Published a paper titled "Integration of TCP/IP module into BIOS to Boot Remote Operating System". ISBN: 978-981-08-2465-5 (Paper Id: IEEE-APPL 1228).
This paper is about building TCP/IP protocol stack at BIOS level thus using it to boot remote operating system.(Same was accepted in WCE-2009 London UK, ICC-2009 Fullerton California, IMECS 2009 Hong Kong, WORLDCOMP 2009 Nevada USA)

REFERENCE 1 :

Dr. S.S.Kamath
Asst. Professor
MACS Dept.
NITK Surathkal

REFERENCE 2 :

Dr. T.G.Basavaraju
Asst. Professor
Computer Dept.
NITK Surathkal