

DIGIT-ALL

Dept. of Computer Science and Engineering,
Gandhi Institute For Technology Bhubaneswar

June 2011

Vol. 1 Issue: 1



DIGIT-ALL

THE E-MAGAZINE, EXPLORES THE TECHNICAL SKILLS OF STUDENTS & FACULTIES. THE MAGAZINE HAS ARTICLES ON LATEST TECHNOLOGIES, CARTOONS, QUIZZES AND MANY MORE FUN FACTS.

EDITORS:

Prof. Sitanath Biswas (Faculty)

Ms. Rajnee Kumari (Student)

Mr. Chintanu Palai (Student)

Vision of the Institute:

To suffice for educational demand of the globe, by achieving excellence through a systematic edifice of performance and service revolving around intellectual, personal and professional growth by encouraging innovation and research built upon tradition of unparalleled quality.

Mission of the Institute:

- ◆ To advance knowledge in major paradigms of technology and to create a distinctive culture of research and innovation among the budding engineers with collaboration of faculties, technocrats, funding agencies and experts from other premier institutes for generating a pool of professionals.
- ◆ To generate a pool of eco-preneurs with the ability to address the industry and social issues of highest standard with inherent concern for environment.
- ◆ To meet the expectations of our society by equipping our students to stride forth as resourceful citizens and conscious of the immense responsibilities to make the world a better place to live in.
- ◆ To create at least one center of excellence within upcoming two academic years in one of the specialized engineering domain.

From HOD's desk:



Dear Readers,

Greetings from Department of Computer Science & Engineering!

As a department of Computer Science & Engineering, We have always strived to provide a well rounded curriculum and training to our students and prepare them to meet the challenges they face ahead in their professional life after they graduate from here. Various student driven initiatives, apart from regular academic curriculum, ensures that student at GIFT get an overall development of their overall personality. DIGIT-ALL is one such initiative.

As a half yearly magazine of GIFT, it helps the students to interact and share their ideas with the industry leaders and their peers studying in the college.

It brings me immense pleasure to bring the first issue of the DIGIT-ALL to you.

I thank everyone for their valuable contributions to the magazine and hope to receive similar enthusiasm through your precious insight in the fourth coming issues of DIGIT-ALL.

Thanks & Regards,

Prof. Satya R. Mohapatra

H.O.D, CSE

Gandhi Institute For Technology, Bhubaneswar

From the Editor's Desk



Dear Readers,

Congratulations to one and all who were by one or the other way involved in this effort and to all the contributors and readers for making DIGIT-ALL a grand success.

It's a grand feeling when a thought endured in the mind, comes into life in the form we had dreamed of. DIGIT-ALL is one such work which had its root in the minds of many. This e-magazine is like a short snapshot of the different research works carried out by the members of the Computer Science Department, the achievements of the students and of the other areas of interest of the students and other members. DIGIT-ALL can be defined as an approach to pause and appreciate our contributions towards the world of Computers from which we have been blessed with the knowledge we have gained.

My love affair with DIGIT-ALL continues and the first issue is now in your hands. I hope you like it. This is just the beginning. Furthermore I would love to receive suggestions for any sort of changes in our magazine.



Thanks and Regards

Prof. Sitanath Biswas

Dept. of CSE, G.I.F.T

CONTENTS

ARTICLES

-  **INKBLOTS**
IMPROVE SECURITY
OF ONLINE
PASSWORDS
-  **THE ONION**
ROUTER (TOR)

CARTOONS

TECHNICAL QUIZ

POETRY

HAPPENINGS

ARTICLES

⊕ INKBLOTS IMPROVE SECURITY OF ONLINE PASSWORDS

By: Prof. Manmath N. Das
Faculty, Dept. of CSE

This new type of password, dubbed a GOTCHA (Generating panOptic Turing Tests to Tell Computers and Humans Apart), would be suitable for protecting high-value accounts, such as bank accounts, medical records and other sensitive information.

To create a GOTCHA, a user chooses a password and a computer then generates several random, multi-colored inkblots. The user describes each inkblot with a text phrase. These phrases are then stored in a random order along with the password. When the user returns to the site and signs in with the password, the inkblots are displayed again along with the list of descriptive phrases; the user then matches each phrase with the appropriate inkblot.

"These are puzzles that are easy for a human to solve, but hard for a computer to solve, even if it has the random bits used to generate the puzzle," said Jeremiah Blocki, a Ph.D. student in computer science who developed GOTCHAs along with Manuel Blum, professor of computer science, and Anupam Datta, associate professor of computer science and electrical and computer engineering.

These puzzles would prove significant when security breaches of websites result in the loss of millions of user passwords -- a common occurrence that has plagued such companies as LinkedIn, Sony and Gawker. These passwords are stored as cryptographic hash functions, in which passwords of any length are converted into strings of bits of uniform length. A thief can't readily decipher these hashes, but can mount what's called an automated offline dictionary attack. Computers today can evaluate as many as 250 million possible hash values every second.

Given the continued popularity of easy passwords, such as "123456" or "password," it's not always difficult to crack these hashes. But even hard passwords are vulnerable to the latest brute force methods.

In the case of a GOTCHA, however, a computer program alone wouldn't be enough to break into an account.

"To crack the user's password offline, the adversary must simultaneously guess the user's password and the answer to the corresponding puzzle," Datta said. "A computer can't do that alone. And if the computer must constantly interact with a human to solve the puzzle, it no longer can bring its brute force to bear to crack hashes." The researchers described GOTCHAs at the Association for Computing Machinery's Workshop on Artificial Intelligence and Security in Berlin, Germany, Nov. 4.

Because the user's descriptive phrases for inkblots are stored, users don't have to memorize their descriptions, but have to be able to pick them out from a list. To see if people could do this reliably, there searchers performed a user study with 70 people hired through Mechanical Turk. First, each user was asked to describe 10 inkblots with creative titles, such as "evil clown" or "lady with poofy dress." Ten days later, they were asked to match those titles with the inkblots. Of the 58 participants who participated in the second round of testing, one-third correctly matched all of the inkblots and more than two-thirds got half right.

Blocki said the design of the user study, including financial incentives that were too low, might account for the less-than-stellar performance. But he said there also are ways to make descriptions more memorable. One way would be to use more elaborate stories, such as "a happy guy on the ground protecting himself from ticklers."

The researchers also have invited fellow security researchers to apply artificial intelligence techniques to try to attack the GOTCHA password scheme.

Great Quotes:

"A few years ago a friend said that I use to hunt and fish and build houses and things but now my whole life revolved around my computer I replied "But my computer revolves around the world".

— Stanley Victor Paskavich,

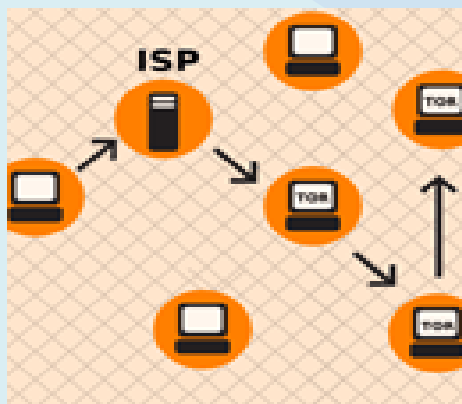
✦ THE ONION ROUTER (TOR)

By: Ms. Madhulika Pandey
Student, Dept. of CSE

An "onion router" is an Internet application that takes requests for web-pages and passes them onto other onion routers, until one of them finally decides to fetch the page and pass it back through the layers of the onion until it reaches you. The traffic to the onion-routers is encrypted, which means that other people can't see what you're asking for, and the layers of the onion don't know who they're working for.

Onion routing is immensely useful for protecting a users privacy and sending confidential information over the Internet without it being compromised. TOR can also provide anonymity to websites and other servers. Servers configured to receive inbound connections through TOR are called hidden services.

Rather than revealing a server's IP address (and thus its network location), a hidden service is accessed through its onion address. The Tor network understands these addresses and can route data to and from hidden services, even those hosted behind firewalls or network address translators (NAT), while preserving the anonymity of both parties. Tor is necessary to access hidden services.



A Figure representing the model of an ISP

Hidden services have been deployed on the Tor network beginning in 2004. Other than the database that stores the hidden-service descriptors, Tor is decentralized by design; there is no direct readable list of all hidden services, though a number of hidden services catalog publicly known onion addresses.

The TOR browser is available for Windows, Mac and Linux operating systems.

Great Quotes:

“Now, 75 years [after To Kill a Mockingbird], in an abundant society where people have laptops, cell phones, iPods, and minds like empty rooms, I still plod along with books. [Open Letter, O Magazine, July 2006]”

– **Harper Lee**

“That the state of knowledge in any country will exert a directive influence on the general system of instruction adopted in it, is a principle too obvious to require investigation.”

– **Charles Babbage**

“UNIX is basically a simple operating system, but you have to be a genius to understand the simplicity.”

– **Dennis Ritchie**

SOME INTERESTING FACTS

By: Mr. Abhisek Kumar
Student, Dept. of CSE



- ◆ The first domain name ever registered was Symbolics.com.
- ◆ U.S. President Bill Clinton's inauguration in January 1997 was the first to be webcast.
- ◆ Doug Engelbart had made the first computer mouse in 1964, and it was made out of wood.
- ◆ Every minute, 10 hours of videos are uploaded on You tube.
- ◆ While it took the radio 38 years, and the television a short 13 years, it took the World Wide Web only 4 years to reach 50 million users.
- ◆ 'Stewardesses' is the longest word which can be typed with only the left hand.
- ◆ If you were to remove all of the empty space from the atoms that make up every human on earth, the entire world population could fit into an apple.
- ◆ Google uses an estimated 15 billion kWh of electricity per year, more than most countries. However, Google generates a lot of their own power with their solar panels.

Proverbios

If the automobile had followed the same development cycle as the computer, a Rolls-Royce would today cost \$100, get a million miles per gallon, and explode once a year, killing everyone inside.

-- Robert X. Cringely

CARTOONS

By: Ms. Nivedita Dey
Student, Dept. of CSE

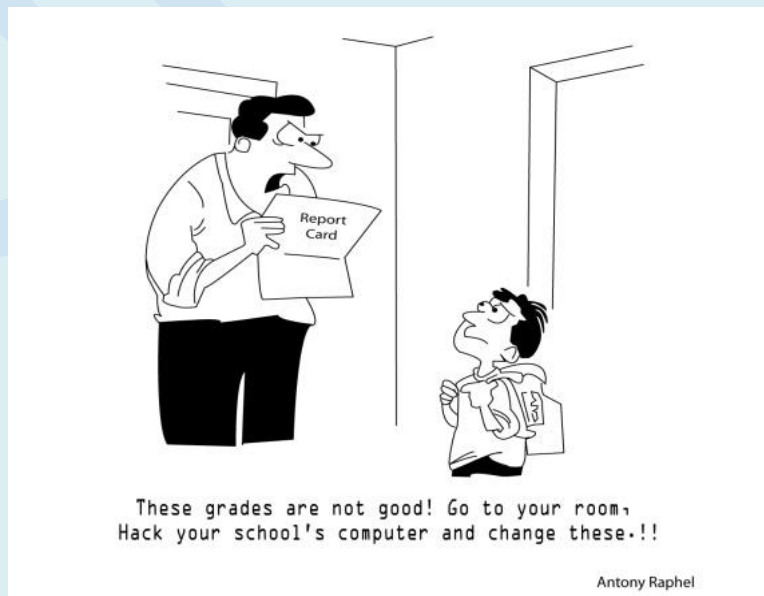
First time for Everything .. !!



Computers are useless. They can only give you answers.

Pablo Picasso

Networksecurity at threat....!!



Computers are like Old Testament gods; lots of rules and no mercy.

Joseph Campbell

TECHNICAL QUIZ

BY: Ms. Diptimayee Rana
Student, Dept. of MCA

- ❖ *A technique used by codes to convert an analog signal into a digital bit stream is known as*
- A. Pulse code modulation
B. Pulse stretcher
C. Query processing
D. Queue management
E. None of the above
- ❖ *An optical input device that interprets pencil marks on paper media is*
- A. O.M.R
B. Punch card reader
C. Optical scanners
D. Magnetic tape
E. None of the above
- ❖ *Most important advantage of an IC is its*
- A. Easy replacement in case of circuit failure
B. Extremely high reliability
C. Reduced cost
D. Low power consumption
E. None of the above
- ❖ *Data division is the third division of a _____ program.*
- A. COBOL
B. BASIC
C. PASCAL
D. FORTH
E. None of the above
- ❖ *Which language was devised by Dr. Seymour Cray?*
- A. APL
B. COBOL
C. LOGO
D. FORTRAN
E. None of the above
- ❖ *A program that converts computer data into some code system other than the normal one is known as*
- A. Encoder
B. Simulation
C. Emulator
D. Coding

- ❖ *A device designed to read information encoded into a small plastic card is*
- A. Magnetic tape
B. Badge reader
C. Tape puncher
D. Card puncher
E. None of the above
- ❖ *A hybrid computer uses a _____ to convert digital signals from a computer into analog signals.*
- A. Modulator
B. Demodulator
C. Modem
D. Decoder
E. None of the above
- ❖ *A group of magnetic tapes, videos or terminals usually under the control of one master is*
- A. Cylinder
B. Cluster
C. Surface
D. Track
E. None of the above
- ❖ *Any device that performs signal conversion is*
- A. Modulator
B. Modem
C. Keyboard
D. Plotter
- ❖ *Codes consisting of light and dark marks which may be optically read is known as*
- A. Mnemonics
B. Bar code
C. Decoder
D. All of the above
- ❖ *A type of channel used to connect a central processor and peripherals which uses multiplying is known as*
- A. Modem
B. Network
C. Multiplexer
D. All of the above
E. None of the above

Answers
1. A
2. A
3. B
4. A
5. C
6. A
7. B
8. C
9. B
10. A
11. B
12. C

POETRY:

By: Mr. Rahul Singh Dekh
Student, Dept. of CSE

She.

*I am she
The woman of power
The eternal mother.
The creator of Life
The essence of purity,
Unlike any other.
The Divine within
The mortal sin
The flame of passion
The cloak of compassion
When all world falls apart
The only spirit who stands tall
Was made from a man's rib
To protect his heart, from his crib
Love is my only weapon
For it conquers nations
I give it free, I give it all
The Vibrant light
For, I am She.*

HAPPENINGS

1. Infosys campus connect program on 19th Jan , 2011,
2. 27th Mar, 2011, Campus Drive by Real Infoware & DynPro India.
3. 29th - 30th April, 2011, Campus Drive by TECHNOMAX IT SOLUTION and AAS Technologies.

THE END