DIGIT-ALL

Dept. of Computer Science and Engineering.

Gandhi Institute For Technology Bhubaneswar

oct 2018

Vol:8 Issue:2

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. SMRUTI RANJAN SWAIN

MS. SOUMYA RANJAN SAHOO

MR. SRUTISWARUPA

DIGIT-ALL

Vol:8
Issue:2

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,

Dr. Sujit Kumar Panda

H.O.D, CSE

Gandhi Institute For Technology, Bhubaneswar

DIGIT-ALL

Vol:8
Issue:2

CONTENTS

ARTICLES PAGE NO.

- Inkblots Improve Security Of Online Passwords 05
- The Onion Router (Tor) 06
- A Vulnerable Network Undersea Internet Cable Attacks 08
- Cyber Attack Prevention for the Home User 11
- Internet Freedom Rhetoric Versus Reality 14

CARTOONS 20

TECHNICAL QUIZ 21

POETRY 23

ARTICLES

INKBLOTS IMPROVE SECURITY OF ONLINE PASSWORDS

Ms.Swapna Das (CSE-1601298063)
Mr.Soumya Suraj Das (ECE-1701298008)

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,

DIGIT-ALL

Vol:8
Issue:2

THE ONION ROUTER (TOR)

Mr.Samaresh Mohapatra (CSE-1601298059)

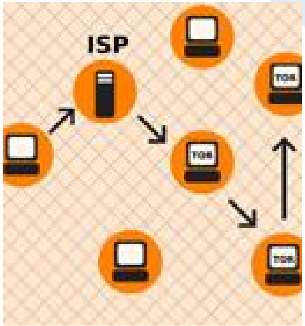
Mr.Swagatam Nanda (ECE-1701298362)

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.



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

A Vulnerable Network Undersea Internet Cable Attacks

Mr.Utkal Keshari Das(CSE-1701298143)
Mr.Subham Ranjan (ECE-1701298337)

Multiple undersea internet cables were mysteriously severed and subsequently gained significant attention in the beginning of 2008. The attacks on those cables highlighted the enormous amount of internet traffic that uses the undersea cable system, which carries many times more traffic than the satellite system does.

The focus on the undersea internet and its growth and protection have become much more of a main stage topic since February 2008. The events occurred over a series of days and were carried out predominantly in Middle Eastern waters. Many countries had their internet services dramatically reduced as a result of the attacks.

From late January to early February, as many as nine undersea internet cables were severed. Dr. Richard Sauder wrote an interesting review of the information provided by various reporting agencies on these events.

- Quoting the New York Times, Dr. Sauder stated, "During the height of the disruption, some 70 percent of the Egyptian Internet was down" (2008).
- Here, Dr. Sauder quotes CNN when discussing the first two cables that were severed, "[The two cables] account for as much as three-quarters of the international communications between Europe and the Middle East" (2008).

- An English Daily in the UAE, the Khaleej Times, offered this statistic, “An estimated 1.7 million Internet users in the UAE have been affected by the recent undersea cable damage, an expert said yesterday, quoting recent figures published by TeleGeography, an international research Web site.” The Times also mentioned a key point to this paper, “Almost 90 per cent of Internet traffic is routed through undersea cables and only 10 per cent is done through the satellite” (2008).

These points outline the importance of undersea cable technology and its protection. How we manage security issues revolving around the maintenance and use of these giant cables will play a major role in the continuity and future use of the net.

Various reporting agencies discussed the following list of undersea internet cables that were compromised during that short timeframe in early 2008: A cable off of Marseille, France; two off of Alexandria, Egypt; one off of Dubai, in the Persian Gulf; one off of Bandar Abbas, Iran in the Persian Gulf; one between Qatar and the UAE, in the Persian Gulf; one in the Suez Canal, Egypt; and a cable near Penang, Malaysia.

Additionally, an initially unreported cable cut on 23 January 2008 affected the following undersea internet cables: the SeaMeWe-4 (South East Asia-Middle East-Western Europe-4) near Penang, Malaysia; the FLAG Europe-Asia near Alexandria; FLAG cable near the Dubai coast; FALCON undersea internet cable near Bandar Abbas in Iran; and SeaMeWe-4, also near Alexandria (Kaleej, 2008).

The impact of these cables being severed is summed up nicely by Computer Weekly: “As the undersea cables carry about 95% of the world’s telephone and internet traffic, any widespread internet downtime can have devastating economic implications" (2008). With dozens of new cables to be laid in the next few years, as reported by PC Pro in July of 2008, any disruption in the cables will have massive impact on internet users.

Conversely, one could argue that with more cables being laid, some redundancy will occur so that the increased number of undersea cables will ensure greater continuity in times of cable breakdown. In any event, protecting these cables has become more of a hot topic after theses attacks. The idea that submarines may carry men close enough to the cables to cut or otherwise damage them brings other goals to mind. A possibility exists that during the downtime of the cables, monitoring devices may be attached to gain some amount of unrestricted access to the transmissions running through the cable. Competing governments have a direct pecuniary interest in the construction, laying, and maintenance of these cables. Control of or influence on these cables by any one entity could dramatically impact internet availability for a given population as well as information access by various governments.

The undersea cable network still carries most internet traffic and is still growing. The issue is not in building the cables, but in protecting them. Many traditional agreements between nations regarding information transfer and jurisdiction will come under fire as this unbridled communication network grows and its security becomes more and more of an international concern.

Cyber Attack Prevention for the Home User

Mr.Satyapriya Bhol(CSE-1701298170)
Mr.Nirmal Behera (ECE-1701298291)

As the sophistication of cyber criminals continues to increase, their methods and targets have also evolved. Instead of building the large Internet worms that have become so familiar, these criminals are now spending more time concentrating on wealth gathering crimes, including fraud and data theft. An online article from CyberMedia India Online Ltd., suggests that because home users often have the poorest security measures in place, they have become the most widely targeted group. CyberMedia states that 86% of all attacks are aimed at home users (2006). As attacks on home users increase, new techniques are surfacing, including the use of malicious code to attack web browsers and desktop applications.

The following is a short review of some techniques that are easily employed and can help stem the tide of these criminal cyber attacks:

Although home users may not feel like they are connected to a network, any activity on the Internet can be considered "networked activity." Therefore, protection measures employed by networks may also benefit the home user. Routers and firewalls can help control access to a home computer, but more specific steps may be utilized.

Consider the difference between network intrusion prevention and network detection systems. Prevention systems "automatically detect and block malicious network and application traffic, while allowing legitimate traffic to continue through to its destination" (Top Layer, 2008). A detection system may detect suspicious activity, but where is the protection from fast acting attacks? A prevention system must identify and stop malicious attacks before they do damage and have a chance to infect a system. As the Top Layer article indicates, "[The prevention system] must operate with switch-like latency at all times" (2008). Technology from the nineties will no longer suffice to protect users from attack by today's modern cyber-criminal.

The prevention system must not only block malicious code, but it must also never block legitimate traffic even while being attacked. It must also be scalable and should protect, to some degree, against newer, more advanced types of security threats.

Along with intrusion prevention, another useful tool for the home user is to become familiar with some of the tricks and techniques that hackers use to break into systems. Some of these tricks include scanning systems for weak spots, like an operating system that has not been upgraded or recently patched, or the use of malware to record important information from the computer (e.g., passwords or financial information). There are many tools that the hacker employs to gain unauthorized access to systems across the Internet. Remember that a system may not always be attacked to steal information; it may also be attacked to be used as a storage site for illegal content (such as pirated movie downloads) or a system could be recruited into an online 'bot army.'

To increase security of the home computer, the home user can take a few relatively simple steps. One of the first steps in computer hacking prevention is to make sure that all of your software is up-to-date. Many users have suffered attacks from malicious code that has already been identified and protected against. A new patch will come out for a given piece of software that protects against a recent virus, but if the home user does not download the patch, then that user is susceptible to viruses or malicious code.

Different applications on the market will scan and remove malicious code that has found its way onto a hard drive. Running various virus software applications yields benefits as well. Different software will detect different malware (Hackingalert, 2008). The whole problem with cyber-security presently is that since the cyber-criminal is constantly upgrading his knowledge and methods, most intrusion prevention software applications only deal with the methods previously used.

The home user may benefit by subscribing to any one of a variety of newsletters that stay abreast of the hacker world. One such free newsletter is offered by Hackingalert.com.

Overall, the user must take a large role in understanding the issues regarding cyber security and implementing their solutions.

Internet Freedom Rhetoric Versus Reality

Mr.Rahul Patra (CSE-1701298104)
Mr.Bikash Kumar Panda (ECE-1701298249)

In the last few years the Internet has borne witness to and facilitated a great deal of social and societal change. From Hilary Clinton's positive 2010 address; 'Remarks on Internet Freedom', to the Tunisian and Egyptian revolutions that showcased the power of social media, the internet, its use and power, has been at the forefront of recent news.1 However, equal to, if not overtaking the positive and enabling factors of the Internet in recent years are the many controversies surrounding it. While undoubtedly carrying the potential to do great good, the Internet has been plagued with numerous impediments, setbacks and controls that greatly damage its offered freedoms. ACTA, SOPA, PIPA, Tempora, Prism, DMCA and adult content opt in, are all examples of recent controversies surrounding freedom on the Internet.2 What is particularly surprising is that all of these restrictions to freedom stem from the very states that laud Internet freedom so highly.

The US and UK being so publicly supportive of Internet Freedom in rhetoric, yet so thoroughly undermining it in action represents a key impediment to global Internet Freedom. If the leading global states are unwilling to forward Internet Freedom in any more than word, how can others be expected to in deed? The current system of Internet governance in general presents a relatively hostile environment within which to foster Internet Freedom. The power of large corporations and companies is immense and the influence they have is equal to their power. Both of these factors further impede the proliferation of Internet Freedom in a way that is currently being decided in the courts of the United States. It is not the undemocratic states that appear to pose the largest threat to Internet Freedom, but the very states that should be protecting it.

This piece will begin by presenting a distinction of the different aspects of Internet Freedom and a brief outline of its current global standing. It will then explain the damage caused by the disparity between freedom rhetoric and reality, after this it will move to explain the current systems of governance and the hostile environment this creates for global Internet freedom. Finally, this work will offer a small and by no means conclusive list of possibilities that would ease the transition to wider freedoms before drawing together the conclusions into a brief summary.

Internet Freedom is an amalgam of two distinct aspects. The initial aspect is the actual physicality of connection; being able to access infrastructure such as computers, phone lines or mobile devices. With the rapid pace of technological advancement, the dropping costs linked to Moore's Law and programs like the Mark Zuckerberg fronted internet.org, access rates to infrastructure are increasing rapidly.3 There are numerous other programs that aim to reduce the digital divide and new Internet users are joining the web each day. Therefore, this piece will concentrate primarily on the second aspect of Internet Freedom; unfettered access to online content.

Recently declared a human right under the 2012 United Nations Human Rights Council resolution ‘The Promotion, Protection and Enjoyment of Human Rights on the Internet' (HRC 2012, Resolution A/HRC/20/L.13), online interactions are now afforded protection equal to offline, real world interaction.4 The HRC 2012 resolution links to The Universal Declaration of Human Rights Article 19, specifically the protection of free speech as an attempt to further Internet Freedom through uncensored discourse and content regardless of frontiers.5 Although now considered a human right, the HRC 2012 resolution has appeared relatively impotent since its adoption and there are still extensive levels of censorship online. There are numerous reasons for online censorship but one of utmost pertinence is that it is almost impossible to form a global consensus on content and access that will attract global support.

As with any contentious subject there will be differing norms and views. The Internet is no exception. Different States have different societal norms and these are reflected in Internet content and acceptable online subjects. Simply put, not everyone wants to have free and unfettered access to the Internet. The ideals of Internet Freedom are prevalent mainly in Western states. Many states view much Internet content as offensive and adversely influential, one just has to consider the 'Innocence of Muslims' riots of 2012.6 Of course in any state there will be a continuum between those that wish to access all material and make their own decisions and those that wish to be shielded from certain content. The logical outcome of this would be to make the Internet completely free and have consumers set their own individual parameters of censorship, however as shall be expounded, this is not a realistic proposition and generally leads to a level of censorship that will vary from region to region, state to state.

The United States, a country that prides itself in its history of liberty and freedom, certainly has a strong public rhetoric regarding Internet Freedom. Indeed, Hillary Clinton has presented several public speeches that provide a litany of the ways that the Internet can enhance a state's economy, religious freedom and democracy. However just months after her 2010 address, 'Remarks on

Internet Freedom' it was discovered that the US had launched a concerted and highly advanced cyber attack against Iran.7 The hypocrisy of lauding the democratizing factors of a free Internet while simultaneously using it as an advanced attack mechanism was not a one off. In 2013 the Edward Snowden leaks highlighted the NSA PRISM program, a classified system forcing US ISPs and phone providers to supply a huge amount of metadata to US security agencies for analysis, and allowing the NSA direct access to company servers.8 Given Hillary Clinton's position as Secretary of State (who also serves on the National Security Council) at the time both events were underway it seems likely that Clinton was aware of the actions.

This kind of hypocrisy is incredibly damaging to any of the legitimate claims or attempts at supporting Internet Freedom. Even more recently in October 2015, the Cybersecurity Information Sharing Act (CISA) bill was passed.9 CISA allows technology companies to share information on cyber threats with US authorities and other companies in order to enhance group security, however the bill is vague enough to allow for large scale personal data sharing without a warrant.10 President Obama signed the bill into law, which was attached to the federal funding 'omnibus' bill, on the same day that the rest of America was preoccupied with the release of the newest Star Wars film. If leading states such as the US do not fully support Internet Freedom, or discuss it in an open and honest manner then there seems little hope for a global movement.

Internet Freedom is a continuum line of liberty and security, the more freedom, generally the less security and vice versa. As has been briefly shown the Internet is a powerful tool indeed at a state level for surveillance and other means. One expects a degree of control and surveillance in nondemocratic states such as China and Cuba and these abuses of freedom are well documented.11 The propensity to abuse Internet freedoms by democratic states however provides a much bigger impediment to Internet Freedom as a whole. If the states that support Internet Freedom are not willing to adhere to their own rhetoric the hypocrisy is an instantaneous barrier to spreading the freedoms they claim to support through foreign policy.

Presumably it will also raise questions as to why the US and UK would support Internet Freedom and its proliferation when they are perfecting means of using it as a surveillance tool. The Internet offers such attractive surveillance opportunities to security services that unfettered, unrestricted and anonymous Internet access does not seem a realistic global goal. Just like Western democratic states, states that are not governed by a system of democracy are acutely aware of the power that the Internet has to facilitate subversion of state control.12 The Arab spring uprising is a prime example of the dangers that the Internet can impose on a government. Between these two it seems unlikely that either type of state will gain dramatically from advancing Internet Freedom.

SOME INTERESTING FACTS

Mr.Aditya Raj (CSE-1601298447)

- 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

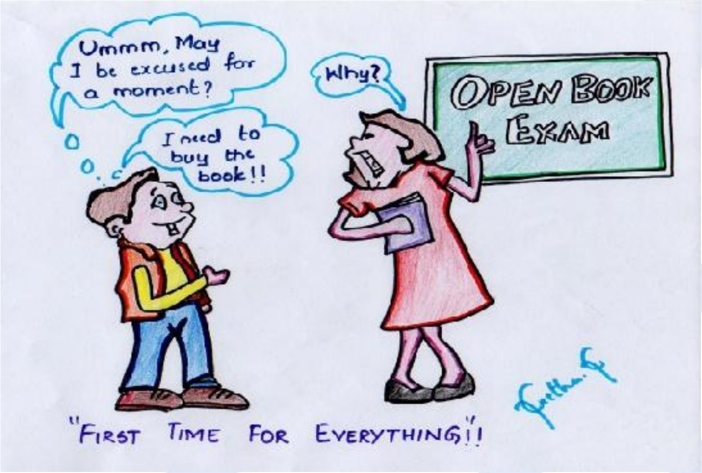
If the automobile had followed the same development cycle as the computer, a Rolls-Royce would today cost $100, get a million miles per gallon, and explode once a year, killing everyone inside.

-- Robert X. Cringely

CARTOONS

Mr.Kishore Das (CSE-1601298053)

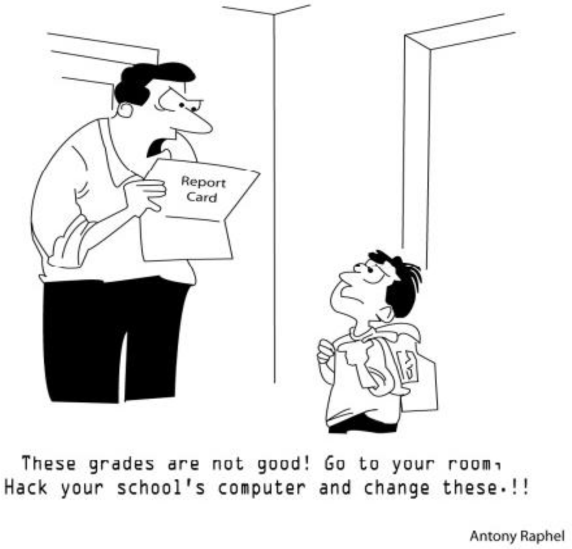
First time for Everything .. !!


Ummm, May I be excused for a moment?
I need to buy the book!!
Why?
OPEN BOOK EXAM
"FIRST TIME FOR EVERYTHING!!"

Computers are useless. They can only give you answers.

Pablo Picasso

Networksecurity at threat….!!


Report Card
These grades are not good! Go to your room, Hack your school's computer and change these.!!
Antony Raphel

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

Joseph Campbell

TECHNICAL QUIZ

Ms.Anamika Pradhan (CSE-1601298038)

- *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:

Mr.Babul Patra (1601298532)

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.