Society for Promotion of Excellence in Electronics Discipline

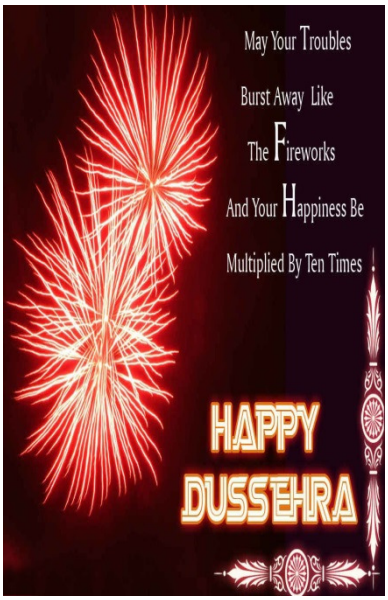
SPEED e-Newsletter
Volume 4, Issue 4
October 2016

SPEED e- NEWSLETTER

Main Article

"QKD": A 'Quantum' leap in Cryptography

Recently China launched the world's first **Quantum Communications Satellite** into orbit from the Gobi Desert. This signaled the dawn of a potentially game-changing communications technology: **Quantum Key Distribution**. If the experiment is successful, it could lead to considerably more secure global communications. Many news outlets described the technology as "**hack-proof**" technology. Quantum crypto-systems achieve this by exploiting the quirky properties of subatomic particles. This article attempts to introduce the science behind.



INSIDE THIS ISSUE

Main Article	1-4
SPEED Activity	5-6
College News	7-9
Puzzle	10
Answer Key	12

(Volume 4 issue 3)

Information security has been very important since ancient times. It is of increasing importance in the current technological age using broadcast, network communications, Internet, e-mail, cell phones which may transmit sensitive information related to finances, politics, business and private confidential matters. **Cryptography** is transmitting information with access restricted to the intended recipient even if the message is intercepted by others. Cryptography has been developed to keep secrets. A famous historical example is **"Caesar's Cipher"**, which was named after Julius Caesar. In this method, a message is encrypted using a shifted alphabet; i.e., each letter in the text is replaced by another letter some fixed number of positions down the alphabet. Caesar's Cipher was easy to break, and was rarely used for serious encryption applications.

1. Classical cryptography:

The fundamental objective of cryptography is to enable two people (Alice and Bob) to communicate over an insecure channel in such a way that an opponent (Eve) cannot understand what is being said. Alice encrypts the plaintext, using a predetermined key, and sends the resulting Cipher text to Bob over the public channel. Upon receiving the cipher text – Eve can't determine what the plaintext was, but Bob knows the encryption key, can decrypt the cipher text and get the plaintext. Breaking the system is hard due to large numbers of possible keys. The fundamental difficulty here is key distribution to parties who want to exchange messages.

1.1 RSA Public-key Protocol

The **Public Key Cryptography** emerged in 1970s. RSA algorithm (named after its inventors, Ron **R**ivest, Adi **S**hamir, and Leonard **A**dle-man) is the most popular public key encryption protocol at the moment. It is widely used in the Internet now days. Each user has two mutually inverse keys, the encryption key is published; the decryption key is kept secret. Anybody can send a message to Bob but only Bob can read it. Its security largely relies on the presumed complexity of factoring large numbers. It is widely assumed that breaking an RSA-encrypted message with current conventional computers will take an extremely long time. But the threats like Shor's algorithm and advancements in computer hardware may not be able to provide forward security for certain applications that require long-term information confidentiality.

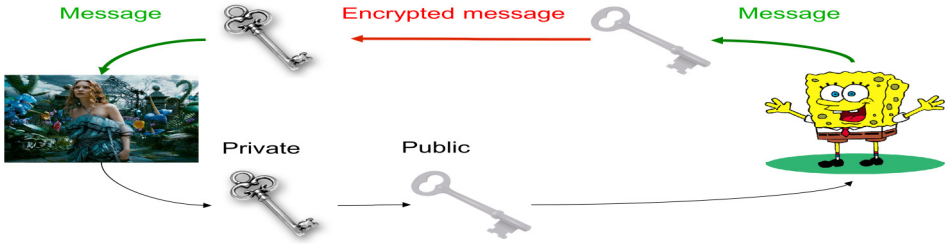


Fig. 1

1.2 One-time Pad Protocol

One-time pad (OTP) algorithm may be a good alternative to RSA algorithm to keep secrets. In binary OTP, two users are assumed to share a long random bit string as a key, which is as long as the message. This key is not known to anyone else. At Alice's (a sender) side, a cipher text is generated by performing XOR operation between the key and the message. A receiver, Bob, can reconstruct the message by performing XOR operation between the key and cipher text.

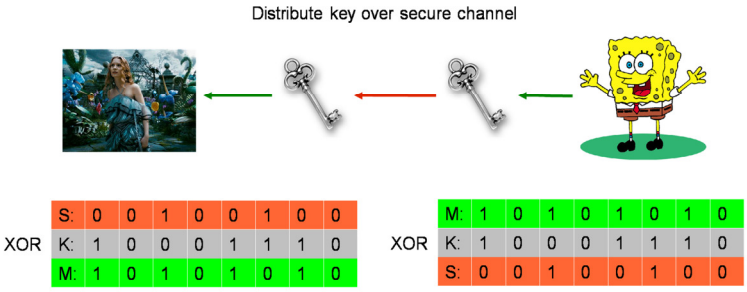


Figure 2: Secrete key cryptography

But still issues like - long key, key only valid for one transmission, secure key distribution cannot be addressed.

1.3 Key Distribution Problem

It is very challenging to distribute the key to the other party with perfect secrecy. This challenge is described as the key distribution problem. To distribute a secret key without leaking any information to eavesdroppers is classically non-solvable problem because classical information is duplicable. Therefore, when the key is transmitted through some channel, an eavesdropper can always make a copy of such classical information.

1.4 A Quantum Solution

This key distribution problem can be solved quantum mechanically. The key bits can be encoded on quantum states of some microscopic particles, like photons. These encoded particles are then sent to Bob. Eve can intercept such particles in the channel. However, Eve cannot make perfect duplicates of the information encoded on the particles due to the quantum no-cloning theorem. Moreover, any attempt to duplicate the quantum states will introduce bit errors. Alice and Bob can quantify the maximal information that might have been learned by Eve from quantum bit error rate (QBER) and channel transmittance. (Cont….)

(….Cont) Quantum cryptography was proposed first by **Stephen Wiesner**, Columbia University in New York, in the early 1970s, he introduced the concept of quantum conjugate coding. He showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded. A decade later, building upon this work, researchers proposed a method for secure communication based on “conjugate observables". In 1990, a different approach to quantum key distribution based on peculiar quantum correlations known as quantum entanglement was developed.

2. Basics of Quantum Computing:

2.1 Elements of the Quantum Theory

Light waves are propagated as discrete quanta called photons. They are mass less and have energy, momentum and angular momentum called spin. Spin carries the polarization. If on its way we put a polarization filter a photon may pass through it or may not. We can use a detector to check if a photon has passed through a filter.

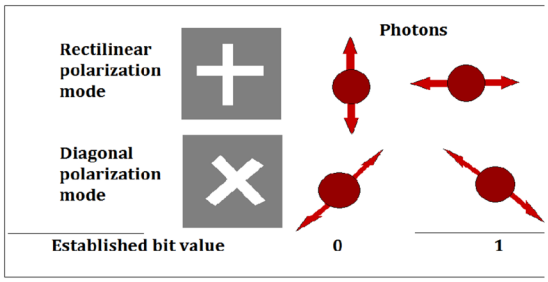


Figure3: The QUBIT

2.2 Binary information

Each photon carries one ‘QUBIT’ of information Polarization can be used to represent “0” or “1”.In quantum computation this is called QUBIT. To determine photon’s polarization the recipient must measure the polarization by, for example, passing it through a filter.

2.3 Heisenberg Uncertainty Principle

Certain pairs of physical properties are related in such a way that measuring one property prevents the observer from knowing the value of the other. When measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurements. If a photon passes through a vertical filter it will have the vertical orientation regardless of its initial direction of

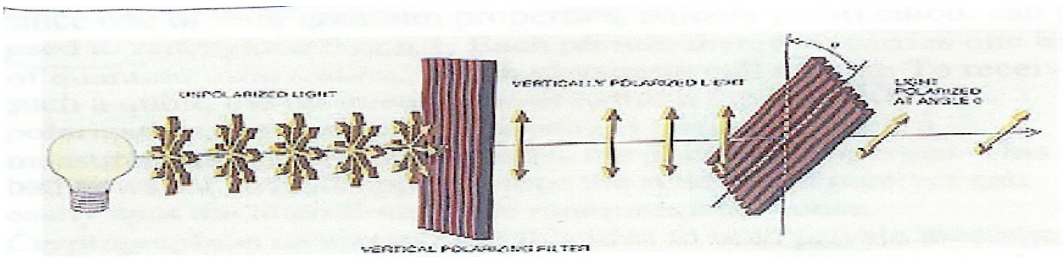


Figure 4: The Polarizer

2.4 Photon Polarization The probability of a photon appearing after the second filter depends on the angle θ and becomes 0 at θ = 90 degrees. The first filter randomizes the measurements of the second filter.

2.5 Polarization by a filter

A pair of orthogonal filters such as vertical/horizontal is called a basis. A pair of bases is conjugate if the measurement in the first basis completely randomizes the measurements in the second basis.

2.6 Sender-receiver of photons

Suppose Alice uses 0-deg/90-deg polarizer sending photons to Bob. But she does not reveal it. Bob can determine photons by using filter aligned to the same basis. But if he uses 45deg/135 deg polarizer to measure the photon he will not be able to determine any information about the initial polarization of the photon. Then the result of his measurement will be completely random.

2.7 Eavesdropper Eve

If Eve uses the filter aligned with Alice's she can recover the original polarization of the photon. If she uses the misaligned filter she will receive no information about the photon .Also she will influence the original photon and be unable to retransmit it with the original polarization. Bob will be able to deduce Eve's presence.

3. Quantum Cryptography:

3.1 The BB84 Protocol:

QKD solved the key distribution problem. Once key is securely received it can be used to encrypt messages transmitted by conventional channels. Unconditionally secure key distribution method proposed by: Charles Bennett and Gilles Brassard in 1984.This method called **BB84 protocol** works as below:

1. Quantum communication phase

-Alice sends Bob a sequence of photons, each independently chosen from one of the four polarizations -

-For each photon, Bob randomly chooses one of the two measurement bases (rectilinear and diagonal) to perform a measurement.

-Bob records his measurement bases and results. Bob publicly acknowledges his receipt of signals.

2. Public discussion phase

-Alice broadcasts her bases of measurements. Bob broadcasts his bases of measurements.

-Alice and Bob discard all events where they use different bases for a signal. The remaining bits are defined as "sifted bits".

To test for **tampering,** Alice randomly chooses a fraction, of all remaining events as test events. For those test events, she publicly broadcasts their positions and polarizations.

-Bob broadcasts the polarizations of the test events.

-Alice and Bob compute the error rate of the test events (i.e., the fraction of data for which their values disagree). If the computed error rate is larger than some prescribed threshold value, say 11%, they abort. Otherwise, they proceed to the next step.

-Alice and Bob each convert the polarization data of all remaining data into a binary string called a raw key (by, for example, mapping a vertical or 45-degrees photon to "0" and a horizontal or 135-degrees photon to "1". They can perform classical post-processing such as error correction and privacy amplification to generate final key.

Bob needs to be authenticated. Otherwise, Eve can easily launch a man-in-the-middle attack by disguising herself as Alice to Bob and as Bob to Alice. Fortunately, authentication of an m-bit classical message requires only a logarithmic in m bit authentication key. Therefore, QKD provides an efficient way to expand a short initial authentication key into a long key.

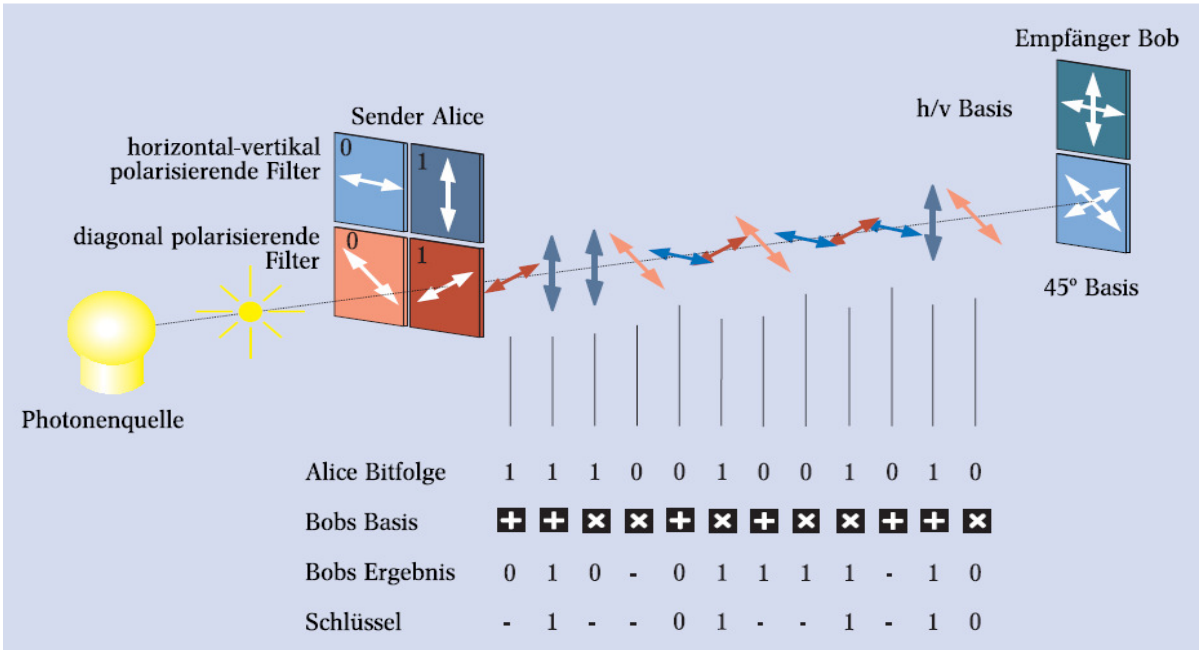
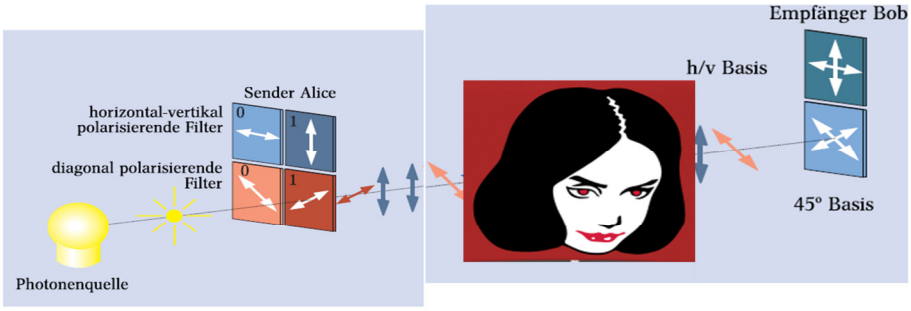


Figure 5: The Quantum Key Distribution Working



Copy machine: $\Psi \otimes |b\rangle \otimes |0\rangle \rightarrow \Psi \otimes \Psi \otimes |f_\Psi\rangle$ e.g. $|\uparrow, b, 0\rangle \rightarrow |\uparrow, \uparrow, .$

$|\nearrow, b, 0\rangle = |\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle), b, 0\rangle$

$\rightarrow \frac{1}{\sqrt{2}}(|\uparrow, \uparrow, f_\uparrow\rangle + |\rightarrow, \rightarrow, f_\rightarrow\rangle) \neq |\nearrow, \nearrow, f_\nearrow\rangle$ **50%** decre in correlatic

Bobs Basis	+	+	×	×	+	×	+	×	×	+	+	×
Bobs Ergebnis	0	~~1~~	0	-	0	~~1~~	1	1	~~1~~	-	1	~~0~~
Schlüssel	-	~~1~~	-	-	0	~~1~~	-	-	~~1~~	-	1	~~0~~

Alice and Bob **recogni** attack from error rate!

Figure 6: Eve's copy machine

3.2 Hack proof technology:

Quantum cryptography means just the exchange of keys. Actual transmission of data is done through classical algorithms. Quantum cryptography enjoys forward security. Alice & Bob can find out when Eve tries to eavesdrop. An eavesdropper Eve does not have a transcript of all quantum signals sent by Alice to Bob. Further, Security is easy to prove while assuming perfect apparatus and a noise-free channel. Cryptography obtains its fundamental security from the fact that each QUBIT is carried by a single photon, and each photon will be altered as soon as it is read. Therefore, once a QKD process has been performed, the information is gone and it will be too late for Eve to go back to eavesdrop.

3.3 Overcoming limitations:

-The maximum transmission distance is mainly limited by channel loss. The quantum signals cannot be classically amplified due to quantum no-cloning theorem. Hence to extend the transmission distance in fiber, quantum repeaters are needed and in free space, ground-satellite QKD is the best option.

-The speed of a QKD system is determined by its slowest component. A typical **BB84 QKD system** has the following active optical components: a pulsed laser source, amplitude modulators, phase modulators, and SPDs (single photon detectors). Among these SPDs are the slowest. The major problem to implement a high-speed QKD system is to build High-speed SPDs.

3.4 Applications:

Quantum cryptography can be the best choice for applications that require long-term information security. Here is the list of some of the potential users:

Government agencies: This includes intelligence, diplomatic, and military agencies. Quantum cryptography can help keep the sensitive data secure during transmission.

Financial institutes: Financial information is very sensitive and needs long-time confidentiality. It can reduce the risk of leaking the client's information during communication.

Health care providers: Health care records are being digitized gradually. The distribution of a patient's health record need to be kept secured for the life span of the patient.

References:

(!) "Introduction to Quantum Cryptography " Dr. Janusz Kowalik IEEE talk Seattle,

(2) "Quantum Cryptography" Ranveer Raaj Joyseeree & Andreas Fognini

(3) "Quantum Cryptography in Real-life Applications:

By :
Sapana S. Rane
Head, Department of Electronics,
Mamasaheb Mohol College,
Pune-411038.
Email :spna_rane@ rediffmail.com

A new MoU of cooperation between Department of Electronic Science, SPPU and Korean Company – K-Water, for in setting up Tidal power and Floating Solar Energy Projects

Recently 0n 24th August 2016, the Savitribai Phule Pune University has entered into an MoU with a Korean Company – K-Water, which is pioneer in setting up Tidal power Projects and Floating Solar Projects. The Department of Electronic Science, SPPU would play a Lead Role in executing various projects in these domains in association with the Korean company.

BENNETT, COLEMAN & CO. LTD. | ESTABLISHED 1838 | TIMESOFINDIA.COM PUNE | MONDAY, AUGUST 29, 2016 | PAGES 26 | PRICE ₹4

THE TIMES OF INDIA

INCLUSIVE OF PUNE TIMES (AVAILABLE ONLY IN PUNE CITY, PCMC AREA & PUNE DISTRICT) | EPAPER.TIMESOFINDIA.COM

University scouts for places to tap tidal & solar power plants

SwatiShindeGole
@timesgroup.com

Pune: Savitribai Phule Pune University (SPPU) aims to identify sites for successful development of tidal and floating solar power projects in the country with the help of Korea Water Resources Corporation (K-water).

SPPU signed a memorandum of understanding (MoU) with K-water for development of tidal and floating power generation projects last week and a panel of experts visited Mumbai to look into the possibility of setting up the first ever tidal river energy plant in India at the Kasheli bridge area along Ulhas River in Thane.

The energy director and manager of K-water, Hong Jeong Jo and Bong-Keun Oh, and Dr Arvind Shaligram, head of department of the electronic science at SPPU visited the location on Tuesday to check the feasibility of the project. The MoU is likely to facilitate closer scientific and technical interactions and open new avenues for power generation projects.

K-water is a well-known government owned corporation of Korea the has built world's largest tidal power plant in Korea and also several floating solar power plants in their reservoirs.

A D Shaligram said, "The sea is known to exhibit periodic tides -- high tide and low tide behaviour -- which contain substantial amounts of high energy. This potential of the sea has so far not been tapped in India. In tidal power projects, the movement of sea water due to tides is converted into electricity. Floating solar power projects use water surface (those of reservoirs, like lakes and dams) covered with floating solar power generating panels, thereby offering several techno-commercial and ecological advantages."

TOI

SPPU signed a memorandum of understanding (MoU) with K-water for development of tidal and floating power generation projects

GOING GREEN

Through the MoU, the university will provide its technical expertise and consultation to various government and non-government agencies for the identification of sites and successful development of tidal and floating solar power projects in India. K-water will extend its knowledge and experience towards the ambitious project.

The MoU was signed by the registrar of the university, Narendra Kadu and the director of energy department of K-water, Hong Jeong Jo.

W N Gade, vice-chancellor of the university said, "This is going to be very fruitful collaboration to fulfil power requirement of the society at affordable costs. The University will provide all the possible support for successful design and development of the projects."

With inputs from Freny Fernandes

One Day workshop on "*Future Trends in CMOS VLSI*" co-organized by SPEED

CMOS VLSI have revolutionized the field of electronics by providing complex functionalities on densely packed electronic chips, those consume ultra low power and are becoming cheaper and more reliable with the time travel. Researchers across the globe are striving hard to bring up innovative technologies for novel applications.

Department of Electronic science, Savitribai Phule Pune University (SPPU) organized a One Day workshop on "Future Trends in CMOS VLSI", on 30th August 2016. This workshop was organized in association with Society for Promotion of Excellence in Electronics Discipline (SPEED) and ni logic Pvt. Ltd. Pune, IEEE India Council EDS chapter were Technical sponsors. The main goal of the **CMOS VLSI** workshop is rigorous technical discussion on recent advances and future directions in Digital CMOS VLSI design, and fostering Interdisciplinary collaborative research in this area.

Since its inception the **department of electronic science** has been working strongly with education initiatives and research in the domain of Microelectronics technology, which is backbone of CMOS VLSI. Industry standard high end design tools from Cadence, Mentor Graphics, MicroWind, Xilinx etc. are included in teaching and research programs. Professor A.D. Shaligram is presently chairman of IEEE India Council Electron Devices Society Chapter. Many Alumni of the department are well placed in companies like Intel, Seagate, Open Silicon etc.

The keynote speaker Dr. Etienne Sicard, a senior Professor of Electrical and Computer Engineering at the INSA group, at the University of Toulouse, France delivered excellent technical sessions

Dr. Sicard was felicitated during concluding session at the auspicious hands of Professor Wasudev Gade, Honorable Vice Chancellor of Savitribai Phule Pune University.

The workshop was attended by over 80 faculty members and students from different Science and Engineering colleges and the University.

NEWS and EVENTS at COLLEGES

Mauli Group of Institutions College of Engineering and Technology, Shegaon :

Mauli Group of Institutions College of Engineering and Technology, Shegaon has organized 1st National Conference on **"Innovative Trends in Science & Engineering "**in association with ISTE New Delhi, SPEED & IJRITCC Journal on 8th July 2016. The conference was inaugurated by Hon. **Prof. Pratapsinh K. Desai,** President, ISTE New Delhi in the Chairmanship of **Hon. Shri Dnyneshwardada P. Patil,** President, of MGI-COET, Shegaon; Hon. **Dr. Rajkamal** Former Vice Chancellor, Devi Ahilya University, Indore and Director of Medicaps Institutes of Technology and Management, Indore ; **Dr. A. D. Shaligram**, Chairman of Speed & Head Dept. of Electronics Science , SPPU ; **Dr. D. S. Dhote** Head Dept. of Electronics, Brijlal Biyani Science College, Amravati; **Dr. H. R. Deshmukh** Executive Council member of ISTE, Maharashtra were the guest of honors for the function. **Dr. C. M. Jadhao** (Chairman, NCITSE'16) addresses the delegates and the researchers to explore their knowledge and always be ready to learn new things. **Prof. Niraj N. Kasliwal** (Convener, NCITSE'16) was taken the opportunity to introduce the guest. Inauguration was followed by excellent Keynote addresses by Dr. Rajkamal and Dr. A. D. Shaligram. Keynote sessions were followed by five parallel technical sessions for different tracks. All the registered papers were included in the Proceedings of the conference. The main objective of this conference was to address and provide platform to discuss the emerging trends there by ability to share the knowledge in the recent advancements. The conference was also providing a perfect platform for academicians to upgrade their knowledge in Science Engineering and Technology domain.

"Let us work towards Excellence in Electronics for the betterment of society"

-Deepa Ramane

GET CONNECTED TO

SPEED

Share your talent in Electronics with others by submitting related information through your electronics teachers of college to SPEED on

Speednewsletters @gmail.com

Website

www.excellentspeed .org

Students' Zaroka : Winning Electronics Projects and Poster

MIT Arts Commerce and Science College, Alandi, Pune:

Department of Electronic Science under "**MITRONICS**" has organized an Intercollegiate Electronics Poster Competition for B.Sc (computer Science) and B.Sc. (Electronic Science) students on date 3rd September, 2016 at MIT Arts, Commerce & Science College Alandi (D), Pune. Inauguration of "**MITRONICS**" Group and **Intercollegiate Electronics Poster Competition** is done by Prof. Dr. B.B. Waphare, Principal, MIT ACSC, Alandi. In this competition total 70 students participated. Out of which approximately 30 students were from different colleges of Pune district like St. Miras College, D.Y. Patil ACS Colleges, A.T.S.S -CBSCA College, etc. Total 35 posters were presented in this Electronics Poster Competition.

The themes given for this posters Competition is **Digital India, Robotics and its Applications, Role of Sensors in Modern world** etc. The judgment of posters competition was done by Prof. B. B. Pawar and Prof. B.K. Shaikh. Result of this poster competition is given as follows:

1st Prize: Miss. Bhagyashri Soni & Miss. Shampata Jadhav from St. Miras College.

2nd Prize: Miss. Rushali Belapurkar & Miss. Namrata Jadhav from St.Miras College.

3rd Prize: Miss. Sneha Gursale & Miss. Sakshi Pawar from MIT ACSC, Alandi (D).

Announcing

"Dr. Vijay Gadkar"

Prize for Innovative Project

In ELECTRONIC PROJECT COMPETITION

(Details of competition will be announced shortly)

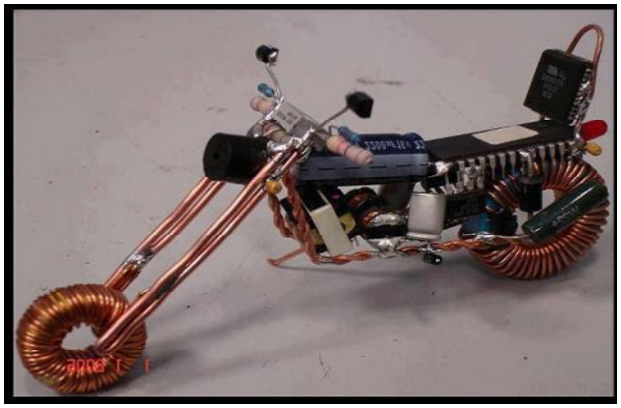
(Dear Students, start hard work and be the winner of prize !!)

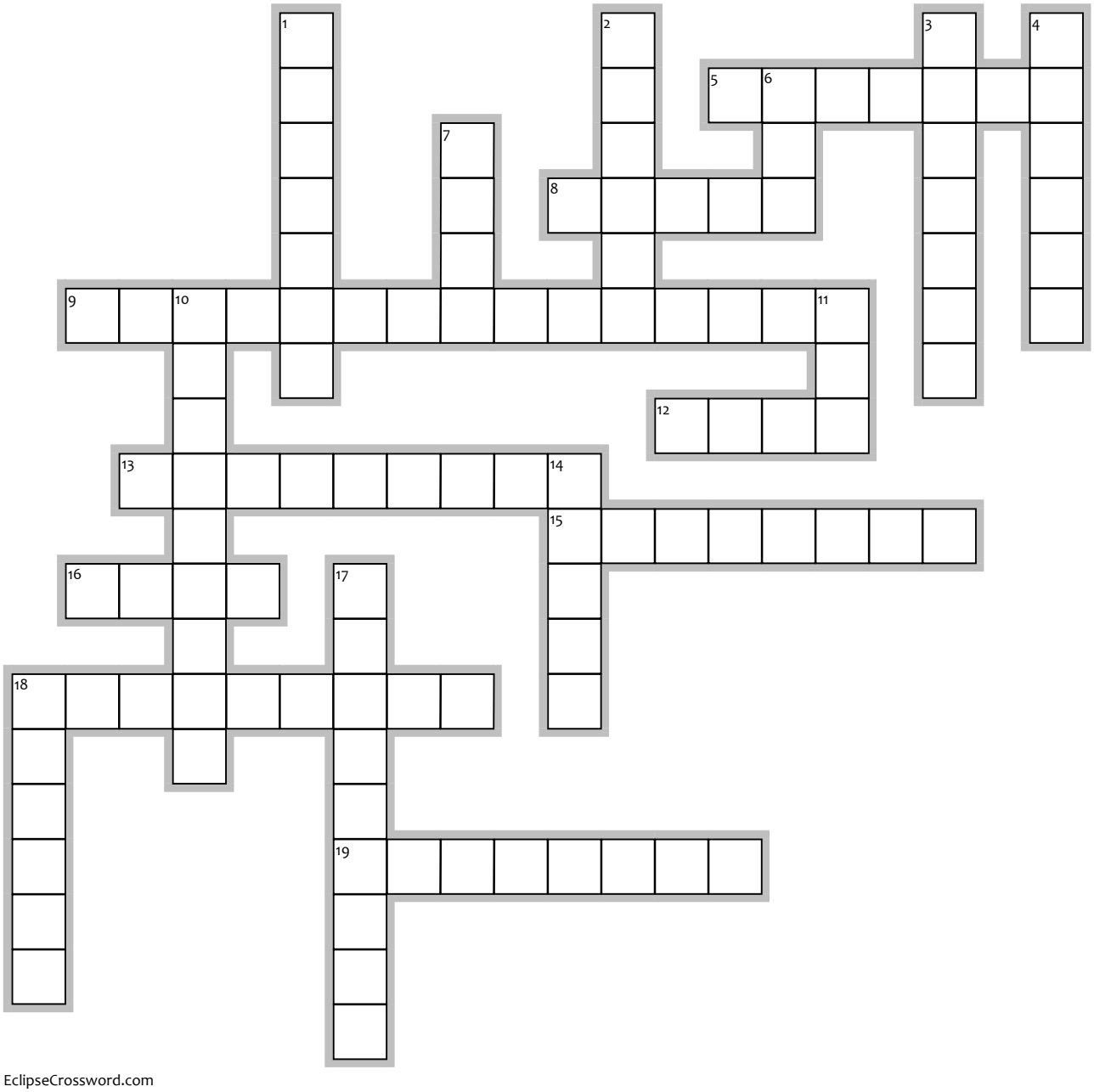
Students' Zaroka : Winning Electronics Projects and Poster

Activities at St Meera's College, Pune:

- As a part of social activity students of S.Y. B.Sc.(CS) along with their class teachers visited center H.O.P.E.(Human organization for pioneering in education) They donated daily needs to the children's.
- Dr. Sangeeta Kale HoD – Applied Physics, DIAT (Defense institute of advance technology) guided students on topic "Nanotechnology – It's amalgamation in science and engineering".

Want Ride on Electronic Bike ?





EclipseCrossword.com

ACROSS

5. "A JK Flip-flop is presently in the SET state and must remain SET on the next clock pulse. Then J must be X and K must be 1" - This statement is..... (7)
8. " A RS Flip-flop is presently in a SET state and must go to the RESET state on the next clock pulse. S must be 1 and R must be 0" - This statement is..... (5)
9. ..... tables define logical properties of a Flip-flop. (15)
12. The ..... state for the T Flip-flop is the same as the present state Q if T = 0 and complemented if T = 1 (4)
13. Characteristics Equation of the circuit are used to describe its ..... in algebraic form. (9)
15. Characteristics ..... of the circuit are used to describe its behavior in algebraic form. (8)
16. A RS Flip-flop is presently in a SET state and must go to the RESET state on the next clock pulse. S input must be ..... and R must be 1. (4)
18. For a ....., when the present state Q = 0 goes to the next state Q = 1, the required D input is D = 1. (9)
19. Characteristics tables define logical properties of a..... (8)

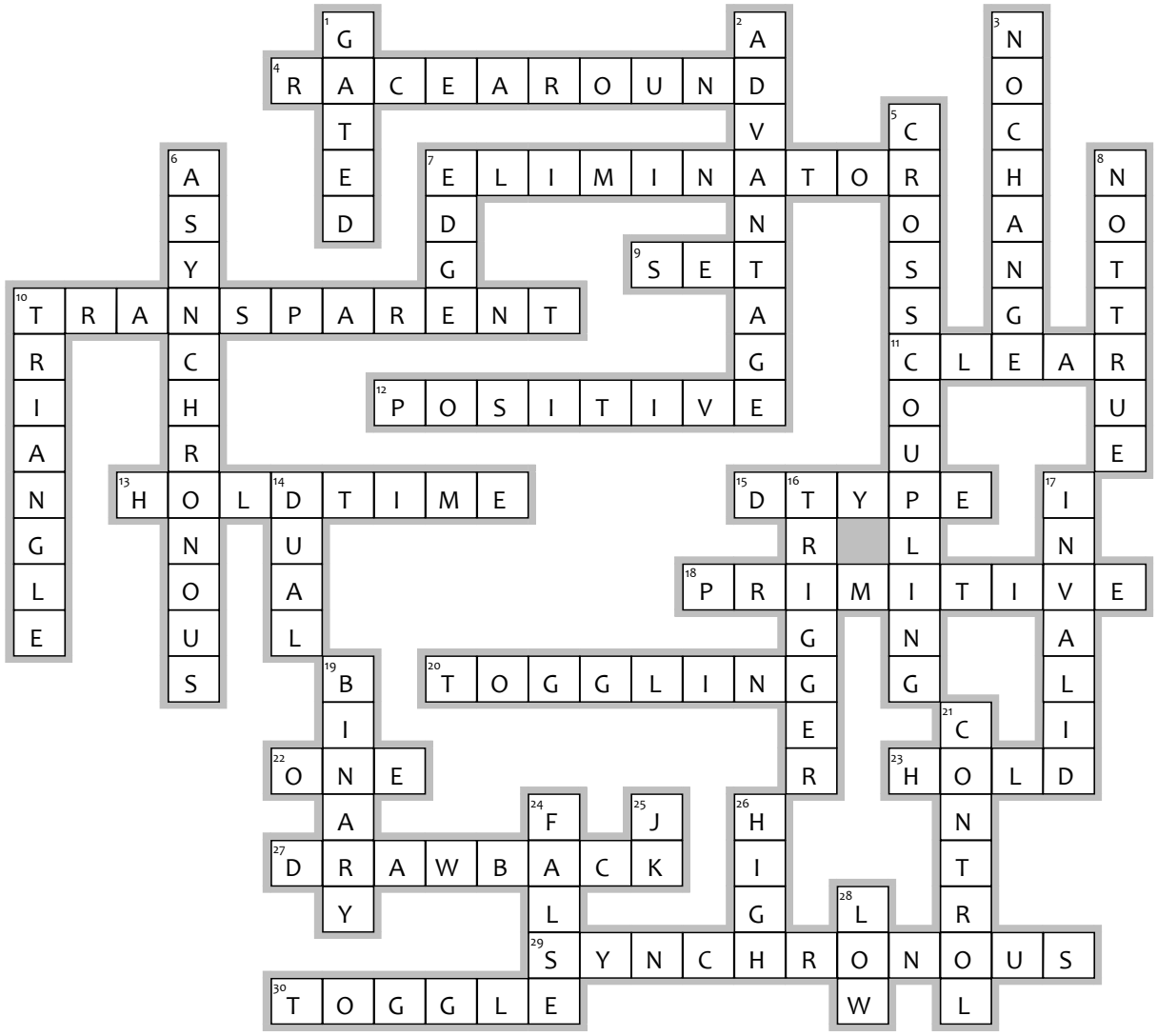
DOWN

1. Characteristics tables define ..... properties of a Flip-flop. (7)
2. For a D Flip-flop, the next state is .....equal to the D input. (6)
3. The next state for the T Flip-flop is the same as the ..... state Q if T = 0 and complemented if T = 1 (7)
4. Characteristics tables..... logical properties of a Flip-flop. (6)
6. A RS Flip-flop is presently in a SET state and must go to the RESET state on the next clock pulse. S input must be 0 and R must be..... (3)
7. The next state for the T Flip-flop is the..... as the present state Q if T = 0 and complemented if T = 1 (4)
10. Characteristics Equation of the circuit are used to describe its behavior in..... form. (9)
11. A JK Flip-flop is presently in the SET state and must remain ..... on the next clock pulse. Then J must be = 0 and K must also be = 0. (3)
14. A JK Flip-flop is presently in the..... state and must go to the SET state on the next clock pulse. J must be 1 and K must be X(Don't care) (5)
17. The next state for the.....is the same as the present state Q if T = 0 and complemented if T = 1 (9)
18. For a D Flip-flop, the next state is always equal to the..... (6)

Editorial team of SPEED e-Newsletter

Dr. (Mrs.) Deepa Ramane (Editor)	ramanedeepa@yahoo.co.in	+9199210 48350
Prof. (Mrs.) Sapana Rane	spna_rane@rediffmail.com	+919890968884
Prof. R. K. Nerkar	rknerkar@rediffmail.com	+9194235 81016
Dr. (Mrs.) Jayshree Bengali	Jayashri789@yahoo.com	+919423581927
Prof. Sunil Chuadhari	misunil@gmail.com	+919422616727
Dr. Y. B. Gandole	ygandole@gmail.com	+919421737928

ANSWER KEY FOR VOLUMR 4 ISSUE 3



National Conference Alert

Dear Sir / Madam,

Electronic and Computer Science Department of Kannada Sangha Pune's Kaveri College of Arts, Science and Commerce is organizing a National Level Conference on **"Application of Computer and Electronic Science"** on **20th to 21st January 2017**.

We request you to bring this to the notice of your post graduate students, research students, research faculties and anyone interested in the conference topics.

All the participants including contributing paper authors are required to confirm their registration by sending a mail to **kcasc.nlc@gmail.com**. The accepted paper received with registration fees will be published in the proceedings of conference with ISBN Number: 978-81-926543-2-4.

For any query, please contact convener Dr.Jayashri Bangali Ph: 09423581927