

10th July 2019

To

The Principal,
S.K.S.D MahilaKalasala,
Tanuku.

Respected sir,

Sub: Guest Speaker Invitation

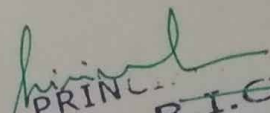
The department of Computer Science wishes to conduct a One-Day workshop on "Network Security & Cryptography" for II BSc I Semester students of our college on 18-07-2019 from 10 AM to 1 PM.

Kindly depute one of your Computer Science faculty members as a resource person to deliver an expert lecture on "**Network security & Cryptography**". We believe that your contribution to this field is unparalleled and a workshop on this topic will be of great benefit.



Thanking you.

Yours Sincerely


PRINCIPAL
Dr. B.V. R.I.C.E.
Vishnupur, BHIMAVARAM-534 202.



Smt. KONDEPATI SAROJANI DEVI MAHILA KALASALA

(DEGREE & P.G. COURSES) (AUTONOMOUS)

(Grant-in-Aid Institution, Affiliated to Adikavi Nannaya University)

Re - Accredited at the B⁺⁺ Level by NAAC

Dr. B. NAGA PADMAVATHI, M.A., Ph.D.
Principal (FAC)

Old Town, TANUKU - 534 211, W.G.Dt. (A.P.)
☎ 08819 - 222154 (O), Cell : 98481 87600
Fax : 08819 - 225369 Email : womens_sksd@yahoo.com

11th July 2019

To

The Principal,
B V Raju College,
Vishnupur,
Bhimavaram.

Respected sir,

Sub: Acceptance of Invitation to Seminar

Thank you for your invitation to the workshop on "Network Security & Cryptography" hosted by Department of Computer Science on 18-07-2019 from 10 AM to 1 PM.

I am happy to inform you that **Mr. N S V N A Kumar, M.C.A., (M.Tech.,) HOD of Computer Science** will be in the resource person. Please send more information about this workshop directly to my attention.

As mentioned in your letter, this is an excellent opportunity to enhance our working relationship. We look forward to it!.

Thanking you.

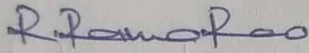
B. Naga Padma
Yours Sincerely
Principal (FAC)


S. K. S. D. Mahila Kalasala
(Degree & PG) (Autonomous)
Re-Accredited by NAAC at B⁺⁺
TANUKU - 534 211, W.G. Dt., (A.P.)

CIRCULAR

Date: 12th July 2019

It is informed to that; the department of Computer Science is conducting a One-Day workshop on “**Network Security & Cryptography**” for II BSc III Semester Computer Science students by **Mr. NSVNA Kumar, MTech HOD of Computer Science, SKSD MahilaKalasala, Tanuku** on 18th July 2019 from 10 AM to 1 PM. Interested students could consult Mr. B Naresh to enrol your names.


HOD


Principal

PRINCIPAL
Dr. B.V. R.I.C.E.
Vishnupur, BHIMAVARAM-534 202.

18th July 2019

To

Mr N S V N A Kumar,
HOD of Computer Science,
S K S D Mahila Kalasala,
Tanuku.

Dear Sir,

Sub: Letter of Appreciation.

Thank you very much for delivering an informative and thought provoking lecture on "Network Security & Cryptography" held on 18th July 2019 at B V Raju College, Vishnupur, Bhimavaram.

It is really a splendid lecture that exposed our students to the field practices. All the students appreciated and got benefitted from your views on the subject.

Looking forward for your cooperation for the promotion of compute education in future as well.



Thanking you.

Yours Sincerely,

hivind
PRINCIPAL
Dr. B.V. R.I.C.E.
Vishnupur, BHIMAVARAM-534 202.

B V Raju College
Vishaupur::Bhimavaram
Workshop on Network Security & Cryptography
Department of Computer Science

Date: 18-07-2019

II BSc (MECs, MPCs & MSCs)

Attendance Sheet

S No	Roll No	Student Name	Section	Signature
1	183117137269	AKULA HARI PRIYA	MECs	A.H Priya
2	183117137271	BALLA SIVANI	MECs	B. Sivani
3	183117137274	BHUPATHI RAJU KRUSHITHA	MECs	Bh. krushitha
4	183117137279	BOLLAM PRIYA RATNAM	MECs	B. Ratnam
5	183117137283	CHATRATHI TEJASRI	MECs	Ch. Tejasri
6	183117137284	CHAVAKULA NAVYA RENUKA	MECs	Ch. Navya Renuka
7	183117137287	CHODISETTI KALYANI	MECs	Ch. Kalyani
8	183117137289	DARABATTULA ANJALI	MECs	D. Anjali
9	183117137292	DATLA DURGANAGAMANI	MECs	D. Durgamani
10	183117137294	DEVAKI SRIJA	MECs	D. Srija
11	183117137304	GORRELA PAVANI	MECs	G. Pavani
12	183117137310	JOGI BHANU SRI	MECs	J. Bhanu Sri
13	183117137314	KADALI SRI HARSHINI	MECs	K.S. Harshini
14	183117137316	KANDI NAGA VENKATA SRIRAM	MECs	K. Venkata Sairam
15	183117137329	KOLLI MADHURI	MECs	K. Madhuri
16	183117137342	MANTENA BHAVITHA NAGA SAI LAKSHMI	MECs	M. P. N. Lakshmi
17	183117137349	MYPALA RAMYA	MECs	M. Ramya
18	183117137356	NERELLA POOJA	MECs	N. pooja
19	183117137369	PUSAPATI BHARGAVI PRIYA	MECs	P. Bhargavi Priya
20	183117137372	SHEIKH TANISHA	MECs	Sk. Tanisha
21	183117137380	VEGESNA VIDYA MADHURI	MECs	V. Vidya Madhuri
22	183117137382	VEJU NAGA RAJITHA	MECs	VN Rajitha

23	183117137384	VETUKURI VAISHNAVI DEVI	MECs	
24	183117137386	YALLA LIKHITHA	MECs	Y. Likhitha
25	183117102056	ALLURI ROSHINI	MPCs	A. Roshini
26	183117102060	BONDADA M N V DURGA SAI SUNANDH	MPCs	B. Sunandh
27	183117102064	CHERUKUMILLI SHANKAR	MPCs	Ch. Shankar
28	183117102070	DINTYALA AMBICA	MPCs	D. Ambica
29	183117102075	GORLA SIRISHA	MPCs	G. Sirisha
30	183117102080	GUNUMOLU DAVEEDU RAJU	MPCs	G. D. Raju
31	183117102086	JETTI MOUNIKA	MPCs	J. Mounika
32	183117102089	KANUBOYINA PREM SAI	MPCs	K. Prem Sai
33	183117102095	KEDHARISSETTI PUJITHA	MPCs	K. Pujitha
34	183117102099	KODURI PRAVALLIKA	MPCs	K. Pravallika
35	183117102103	KOTIPALLI SAI RAMA KRISHANA	MPCs	K. S. Rama Krishana
36	183117102108	MADICHARLA PRASANNA KUMARI	MPCs	M. Prasanna Kumari
37	183117102133	RAMANA PRABHAVATHI	MPCs	R. Prabhavathi
38	183117102143	SHEIK SHAHIDHA BEGUM	MPCs	S. H. Begum
39	183117102150	VASA PAVANI	MPCs	V. Pavani
40	183117109161	ARETI SAI DHARANI	MSCs	A. Sai Dharani
41	183117109167	GADIRAJU DEVI KRISHNA SUREKHA	MSCs	G. Nagara Raju
42	183117109173	INDUKURI NAGA RAJU	MSCs	I. Naga Raju
43	183117109178	KADIYAM PUJITHA DEVI	MSCs	K. Pujitha Devi
44	183117109189	KUTHADA SREE LAKSHMI	MSCs	K. Sree Lakshmi
45	183117109196	NALLA RUCHITA NAGA SRI	MSCs	N. Naga Sri
46	183117109201	PATHIKAYALA NANDINI	MSCs	P. Nandini
47	183117109203	POLAMURI HEMA LATHA	MSCs	P. Hema Latha
48	183117109206	RAGU INDU LATHA	MSCs	R. Latha
49	183117109215	VALIVETI SREE AVEKTHA	MSCs	

Network Security Cryptography

N S V N A Kumar, M.Tech
HOD, Department of Computer Science
S K S D Mahila Kalasala

18-07-2019

2

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—The Art of War, Sun Tzu

Prevention is better than Cure.

18-07-2019

3

Timeline: Art of WAR



18-07-2019

3

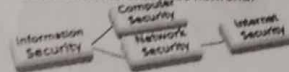
Information Security



Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers.

Network Security - measures to protect data during their transmission.

Internet Security - measures to protect data during their transmission over a collection of interconnected networks.



18-07-2019

4

Computer Security

- Protection to an automated information system.
- **Objective:** security with preserving Information system Resource with

- > Integrity
- > Availability
- > Confidentiality



18-07-2019

5

Levels of Impact

> There are 3 levels of impact from a security breach

1. Low
2. Moderate
3. High

18-07-2019

6

Low Impact

- Security Breach may have a limited adverse effect on organizational operations, organizational assets, or individuals.
- Ex: loss of confidentiality, integrity, or availability might
 1. cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
 2. result in minor damage to organizational assets;
 3. result in minor financial loss; or
 4. result in minor harm to individuals.

18-07-2019

7

Moderate Impact

- May have a serious adverse effect on organizational operations, organizational assets, or individuals.
- Ex: The loss might
 1. cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
 2. result in significant damage to organizational assets;
 3. result in significant financial loss; or
 4. result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

18-07-2019

8

High Impact

- May have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- Ex: The loss might
 1. cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
 2. result in major damage to organizational assets;
 3. result in major financial loss; or
 4. result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

18-07-2019

9

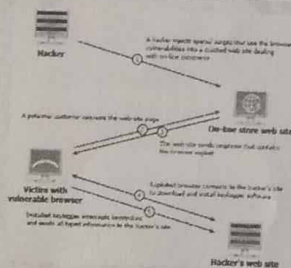
Examples of Security Requirements

- Confidentiality – student grades
- Integrity – patient information
- Availability – authentication service
- Authenticity (Origin Integrity)-admission Ticket
- Non-Repudiation-stock sell order

18-07-2019

10

HACKING Ex: exploiting Browser Vulnerability



18-07-2019

11

Computer Security Challenges

1. Not simple – easy to get it wrong
2. Must consider potential attacks
3. Procedures used counter-intuitive
4. Involve algorithms and secret info
5. Must decide where to deploy mechanisms
6. "Unusable security is not secure"

18-07-2019

12

Standards Organizations

- National Institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)
- RSA Labs (de facto)

18-07-2019

13

Security Aspects

- There are **THREE** aspects of information security:
 - I. SECURITY ATTACK
 - II. SECURITY MECHANISM (CONTROL)
 - III. SECURITY SERVICE
- Difference Between Threat, Vulnerability and an Attack?
 - *Threat* - a potential for violation of security
 - *Vulnerability* - a way by which loss can happen
 - *Attack* - an assault on system security, a deliberate attempt to evade security services

18-07-2019

14

Classify Security Attacks

PASSIVE ATTACKS - eavesdropping on, or monitoring of, transmissions to:

- obtain message contents, or
- monitor traffic flows



ACTIVE ATTACKS - modification of data stream to:

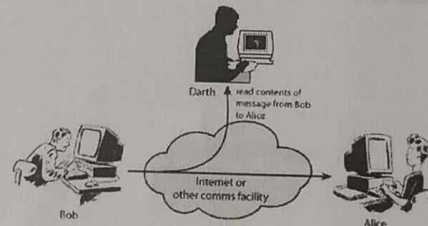
- masquerade of one entity as some other
- replay previous messages
- modify messages in transit
- denial of service



18-07-2019

15

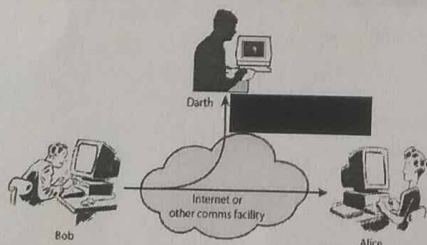
Passive Attack - Interception



18-07-2019

16

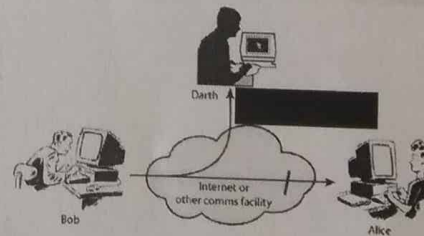
Passive Attack: Traffic Analysis



18-07-2019

17

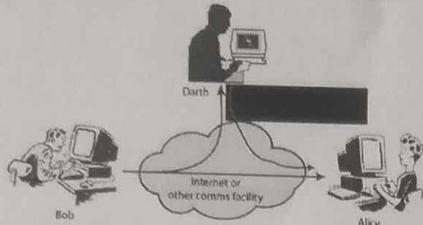
Active Attack: Interruption



18-07-2019

18

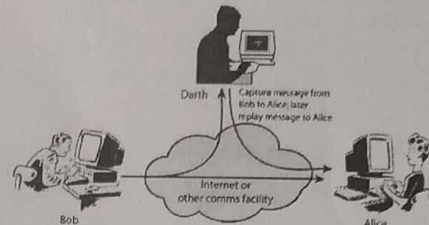
Active Attack: Fabrication



18-07-2019

19

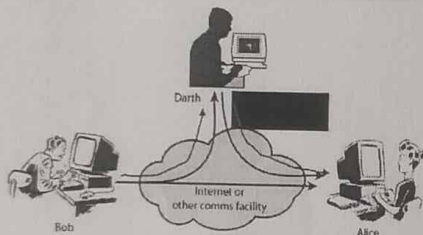
Active Attack: Replay



18-07-2019

20

Active Attack: Modification



18-07-2019

21

Handling Attacks

- **Passive attacks** – focus on Prevention
 - Easy to stop
 - Hard to detect
- **Active attacks** – focus on Detection and Recovery
 - Hard to stop
 - Easy to detect

18-07-2019

22

Security Services

- **X.800**: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- **RFC 2828**: a processing or communication service provided by a system to give a specific kind of protection to system resources
- X.800 defines it in 5 major categories

18-07-2019

23

Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
 - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

18-07-2019

24

OSI Security Architecture

- ITU-T X.800 "Security Architecture for OSI"
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

18-07-2019

25

Security Services (X.800)

- **AUTHENTICATION** - assurance that the communicating entity is the one claimed
- **ACCESS CONTROL** - prevention of the unauthorized use of a resource
- **DATA CONFIDENTIALITY** - protection of data from unauthorized disclosure
- **DATA INTEGRITY** - assurance that data received is as sent by an authorized entity
- **NON-REPUDIATION** - protection against denial by one of the parties in a communication.
- **AVAILABILITY** - resource accessible/usable

18-07-2019

26

Security Mechanisms (X.800)

- **Specific security mechanisms:**
 - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- **Pervasive security mechanisms:**
 - trusted functionality, security labels, event detection, security audit trails, security recovery

18-07-2019

27

Security Mechanisms (X.800)

- a.k.a. control
- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
 - **cryptographic techniques**
- hence our focus on this topic

18-07-2019

28

Security Mechanisms (X.800)

- **specific security mechanisms:**
 - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- **pervasive security mechanisms:**
 - trusted functionality, security labels, event detection, security audit trails, security recovery

18-07-2019

29

References

- William Stallings, "Cryptography and Network Security-Principles and Practices", 4e, Pearson-Printice Hall publications, ISBN 81-7768-774-9.
- Behrouz A. Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security" 2e, McGrawHill Publications, ISBN 978-0-07-070208-0.

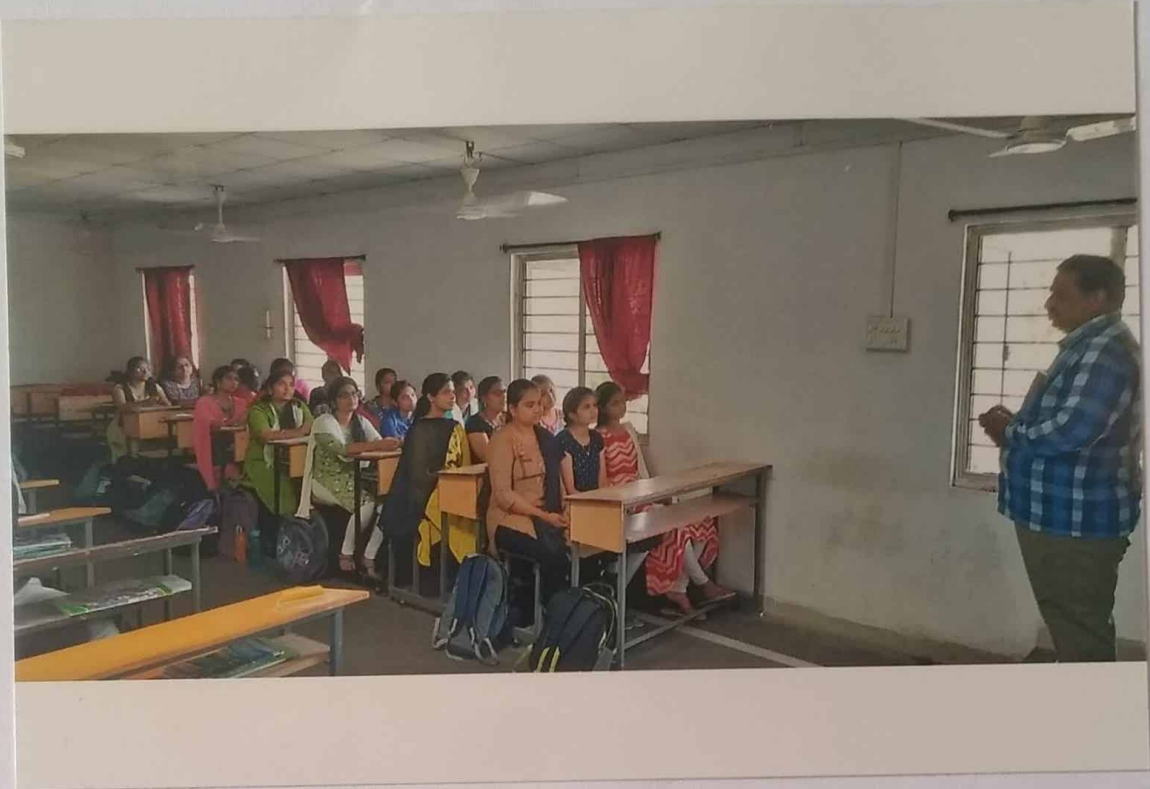
18-07-2019

30

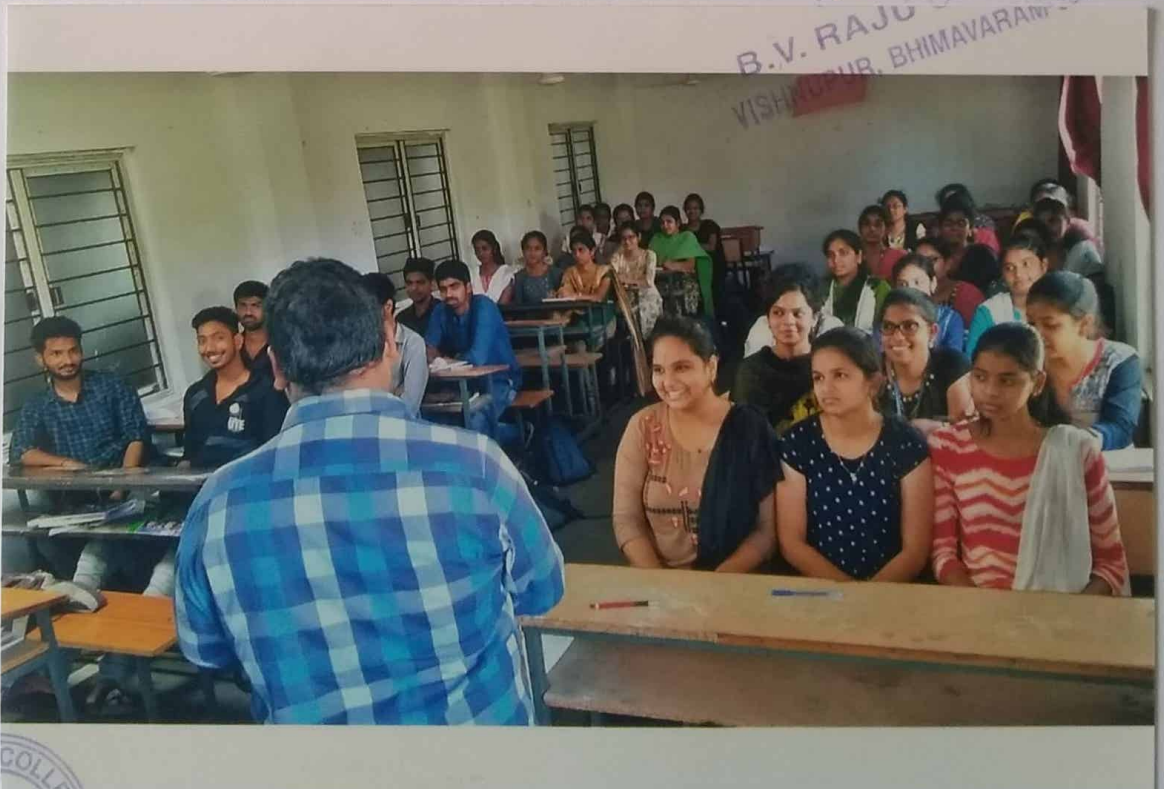
Date: 18th July '19.

Network Security & Cryptography

by Mr. N.S.V.N.A. KUMAR, M.Tech HOD of CS
S.K.S.D. Mahila Khasak, Tanuku.



Principal
B.V. RAJU COLLEGE
VISHNUPUR, BHIMAVARAM-534 202



B V RAJU COLLEGE

VISHNUPUR::BHIMAVARAM

DEPARTMENT OF COMPUTER SCIENCE

EVENT NAME: *network security & cryptography*

DATE: *18-7-2019*

PARTICIPANT FEEDBACK FORM

Name of the Student : *J. Mounika*

Register Number : *183117102086*

Course & Group : *III MPCS*

Contact Number : *9491728788*

Email ID : *Mounika 91@gmail.com*

Future events you are expecting :

How do you rate the event conducted: *1/2/3/4/5* ✓

Are you satisfied with event conduction: *Yes/No* ✓

Comments or Suggestions :

J. Mounika
Signature of the student

B V RAJU COLLEGE

VISHNUPUR::BHIMAVARAM

DEPARTMENT OF COMPUTER SCIENCE

EVENT NAME: Network Security & cryptography

DATE: 18-07-2019

PARTICIPANT FEEDBACK FORM

Name of the Student : Gr. Pavani
Register Number : 183117137304
Course & Group : MECS
Contact Number : 9652992649
Email ID : Pavani.Gorjala@gmail.com
Future events you are expecting :
How do you rate the event conducted: 1/2/3/4/5
Are you satisfied with event conduction: Yes/No
Comments or Suggestions :

Gr Pavani
Signature of the student

B V RAJU COLLEGE

VISHNUPUR::BHIMAVARAM

DEPARTMENT OF COMPUTER SCIENCE

EVENT NAME: Network Security & Cryptography

DATE: 18-07-2019

PARTICIPANT FEEDBACK FORM

Name of the Student : Ch. Tejassri
Register Number : 183117137283
Course & Group : MECs
Contact Number : 9030944334
Email ID : Tejassri.chatrati@gmail.com
Future events you are expecting :
How do you rate the event conducted: 1/2/3/4/5
Are you satisfied with event conduction: Yes/No
Comments or Suggestions :

Ch. Tejassri
Signature of the student

B V RAJU COLLEGE

VISHNUPUR::BHIMAVARAM

DEPARTMENT OF COMPUTER SCIENCE

EVENT NAME: Network security & Cryptography

DATE: 18-07-2019

PARTICIPANT FEEDBACK FORM

Name of the Student : A. Haripriya

Register Number : 183117137269

Course & Group : MECS

Contact Number : 7993483398

Email ID : Haripriya.akula@gmail.com

Future events you are expecting :

How do you rate the event conducted: 1/2/3/4/5 ✓

Are you satisfied with event conduction: Yes/No ✓

Comments or Suggestions :

Haripriya
Signature of the student

B V RAJU COLLEGE

VISHNUPUR::BHIMAVARAM

DEPARTMENT OF COMPUTER SCIENCE

EVENT NAME: Network ~~see~~ security & cryptography.

DATE: 18-7-2019

PARTICIPANT FEEDBACK FORM

Name of the Student : N. Pooja
Register Number : 183117137356
Course & Group : MECS - III
Contact Number : 8341899857.
Email ID : pooja137@gmail.com.
Future events you are expecting :
How do you rate the event conducted: 1/2/3/4/5
Are you satisfied with event conduction: Yes/No
Comments or Suggestions : No suggestions.

N. Pooja.
Signature of the student