

**Event Category : Expert Talk**

**Event Name: “ Elliptic curve Cryptography”**

**Date: 22<sup>nd</sup> December to 08<sup>th</sup> January 2022.**

**Department of Information Science and Engineering**  
JNNCE, Shivamogga

Report on

**Elliptic Curve Cryptography**

By

**Prof. Sheela S**

EC Dept.,  
JNNCE, Shivamogga.

**Elliptic Curve Cryptography (ECC)** is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.

Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. Elliptic curves are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic-curve factorization.

Students of 7th sem ISE have selected Cryptography(18CS744) as elective. They learn ECC in module-3.

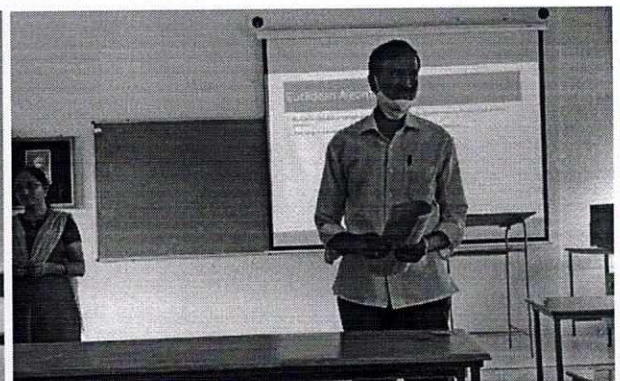
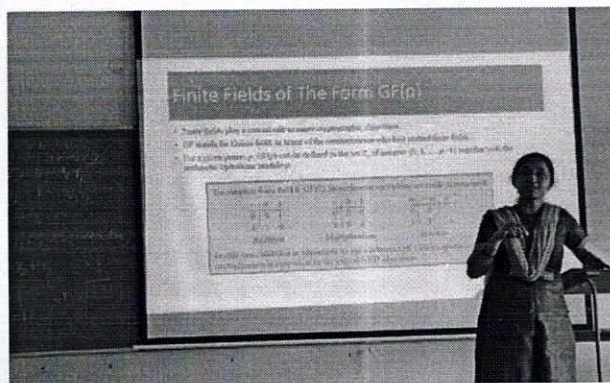
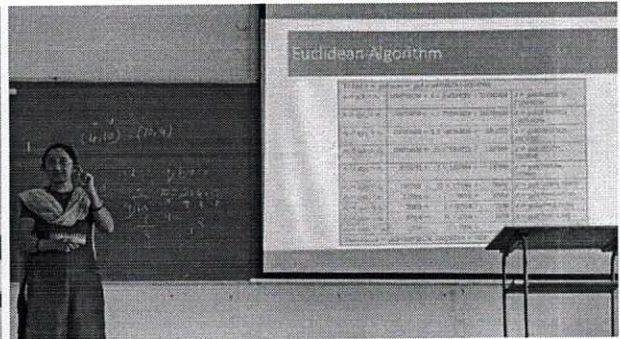
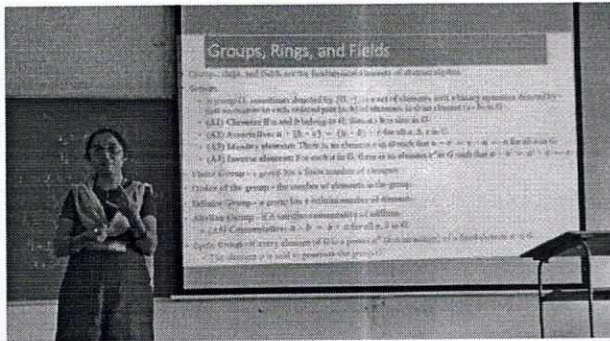
We approached **Prof. Sheela S**, Research Scholar, EC dept. to conduct and interact with the students.

She conducted four sessions from 22-12-2022 on ECC with introduction to Groups, Rings and Fields. Finite fields of the form  $GF(P)$ . Euclidean Algorithm is also dealt with examples.

Later, she explained Elliptic Curve arithmetic, Elliptic curve encryption/ decryption, security of Elliptic curve cryptography and Pseudorandom number generation.

**Syllabus of ECC in Cryptography(18CS744)** : Elliptic curve arithmetic, abelian groups, elliptic curves over real numbers, elliptic curves over  $Z_p$ , elliptic curves over  $GF(2^m)$ , Elliptic curve cryptography, Analog of Diffie-hellman key exchange, Elliptic curve encryption/ decryption, security of Elliptic curve cryptography, Pseudorandom number generation based on an asymmetric cipher, PRNG based on RSA.





72 students have attended the invited talk.





National Education Society (R.)

**J N N College of Engineering, Shivamogga** (Approved by IS&E)



AICTE, New Delhi, Certified by UGC 2f & 12B, Accredited by NAAC – 'B',  
UG Programs: CE, ME, EEE, ECE, CSE, ISE, TCE accredited by NBA: 1.7.2019 to 30.6.2022,  
Recognized by Govt. of Karnataka and Affiliated to VTU, Belagavi)

**Department of Information Science and Engineering**

Date: 16-6-2022

### Summary Report on “Industrial certification courses”

Department of IS & E, JNNCE organized a technical talk on “**Industrial certification courses**” on 14-6-2022 at 1.10 pm. The resource person for the seminar was Mr. Yogish M, team Leader, Ethnos group. The event was coordinated by Mrs. Rashmi R, Associate Professor, Dept. of IS&E

This Industry Outreach Programs aims to connect and collaborate with leaders in academia, industry, and government to create industry readiness and foster development in future discoveries and scientific applications.

#### **Microsoft Certified: Azure Fundamentals**

The certification validates students basic knowledge of cloud services and how those services are provided with Azure. Candidates should be able to demonstrate a fundamental knowledge of cloud concepts, along with Azure services, workloads, security, privacy, pricing, and support.



**The Microsoft Certified: Azure Fundamentals certification could be a great fit for students:**

Dept of IS&E

- Prove students knowledge of cloud computing concepts, models, and services, such as public, private, and hybrid cloud, in addition to infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Show your expertise on how Azure supports security, privacy, compliance trust.
- It is recommended to have familiarity with concepts of networking, storage, compute, application support, and application development. students can use your Azure Fundamentals certification to reinforce your basics for other Azure role-based or specialty certifications, but it isn't a prerequisite for any of them.

**Skills measured**

- This list contains the skills measured on the exam associated with this certification. For more detailed information, visit the exam details page and download the study guide.
- Describe cloud concepts
- Describe Azure architecture and services
- Describe Azure management and governance

A total of 26 students attended the seminar. The seminar was very much interactive and useful. The seminar ended at 2.10 PM.

**Event Coordinator**

*RK*  
Rashmi R

**HoD, ISE**

*R.S.K*  
Dr. R Sanjeev Kunte

*Professor and Head*  
Dept. of Information Science & Engg.  
J.N.V. College of Engineering  
SHIMOGA-577 204



## List of the students attended the workshop

Sl No.	Student Name	signature
1.	ANANYA . S. ARAVINDA	Ananya
2.	NIKITHA . KV.	Nikitha
3.	ARZA FATHIMA FAIYA Z	Arza
4.	ANA KHAN	Ana Khan
5.	Ananya . Babu . Naik	Ananya
6.	Sohana . G . R	Sohana
7.	Prathiksha . H . P	Prathiksha
8.	Niyam . L . Gingade	Niyam
9.	Raksha . S.	Raksha
10.	Velas . N	Velas . N
11.	Nandkesh kumar S.H	Nandkesh
12.	Nayashree M.T	Nayashree
13.	Aishwarya Sait	Aishwarya
14.	Basavaraj . R . Ganiga	Basavaraj
15.	Srihari . G . Kashyap	Srihari
16.	Deepati . R . Bhat	Deepati Bhat
17.	Nayana . M . Uppin	Nayana
18.	Aditya . Basavaraj . Halgal	Aditya
19.	Sachin . S . Hegde	Sachin
20.	Pohar . D	Pohar
21.	Siddarth . P	Siddarth
22.	Samarth . M . S	Samarth
23.	Shashank . S	Shashank
24.	Shree Harsha M	Shree Harsha
25.	Bharathi Hegade SR	Bharathi
26.	Nikitha . A	Nikitha



ರಾಷ್ಟ್ರೀಯ ಶಿಕ್ಷಣ ಸಮಿತಿ(ಓ.), ಶಿವಮೊಗ್ಗ

National Education Society(R.) Shivamogga

Jawaharlal Nehru New College of Engineering(JNNCE), Shivamogga



ಜವಾಹರ್‌ಲಾಲ್ ನೆಹರು ನ್ಯೂ ತಾಂತ್ರಿಕ ಮಹಾವಿದ್ಯಾಲಯ, ಶಿವಮೊಗ್ಗ

(Approved by A.I.C.T.E.New Delhi, Certified by UGC 2f & 12B, Accredited by NAAC - 'B', NBA Accredited UG Programs : CE, ME, EEE, ECE, CSE, ISE, ETE for the period : 01.07.2019 to 30.06.2022, Recognised by Govt. of Karnataka and Affiliated to VTU, Belagavi)

**Department of Information Science and Engineering**

Ref. No.: JNNCE/ISE/84/21-22

Date:22-01-2022

**Letter of Appreciation**

To

**Prof. Sheela S**

Assistant Professor

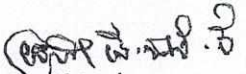
Dept. Of ECE

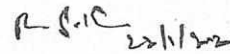
JNNCE, Shivamogga

Dear sir/Madam

We would like to take this opportunity to express our heartfelt thanks to you for your active participation as a resource person in covering **Elliptic Curve Cryptography** from 22-12-2020, four session. It is part of the course Cryptography(18CS744) for 7<sup>th</sup> Sem ISE.

You have shared your knowledge with your skill and expertise. Your effort in making our students understand the concepts and it's usage is highly appreciated. We look forward to your continued support in future.

  
Staff incharge

  
22/1/22

HOD

Professor and Head  
Dept. of Information Science & Eng.  
J.N.N. College of Engineering  
SHIMOGA-577 204