Department of Computer Science & Information Technology

Ref.No.:AJU/H/CS&IT/ **Date:12.04.22**

CIRCULAR

Dear Students,

Department of Computer Science & IT is organizing a Webinar on **"Introduction to Cryptography and Information Security"** on 18th April **2022**. The timing of the Value Added course from 01:00 PM till 03:00 PM.

It is suggested to all the students to participate in the Value Added. For the same, every student need to register with the link given below.

Registration Link:https://forms.gle/M4LhcWKPfoyUx4vF9

The Registration link will be active till **10:00AM – 17th April 2022.**

Mr. Arvind Kumar Pandey
Head, CS&IT
ARKA JAIN University,
Jharrkhand

Report on Value Added Course Introduction to Cryptography and Information Security

Held on 18-04-2022 to 09-05-2022

Date of Event	18-04-2022 to 09-05-2022
Name and Type of Event	Value Added Course Introduction to Cryptography and Information Security
Conducted by	Dr. ARUN KUMAR MARANDI, Dr. Arvind Kumar Pandey
No. Of Participant	38

The Value-Added Course - Introduction to Cryptography and Information Security was organized from 18-04-2022 to 09-04-2022, in the Department of Computer Science and IT ARKA Jain University, Jamshedpur. The Program was Coordinated by Dr. ARUN KUMAR MARANDI and Dr. Arvind Kumar Pandey, Head of CS and IT Department.

In this course, students were learned

• Summarize the main goals of cryptography and illustrate this with a number of examples of how cryptographic services are integrated into current applications, both in software and hardware

• describe goals and design principles for and common structures of secret key primitives such as block and stream ciphers and message authentication codes

• identify, analyze and explain various forms of attacks based on improper usage of primitives, modes, or Protocols

• explain how basic public key primitives can be defined based on the difficulty of mathematical problems such as the discrete logarithm problem or factoring and analyze variants of these systems

• explain the various roles of hash functions as parts of other cryptographic primitives and protocols and the requirements this place on hash functions

• exemplify when various notions of security, such as information-theoretic, computational, provable, and practical security, are applicable and describe the security guarantees provided

• explain basic key management techniques in both secret key and public-key Cryptography

The value-added course, was started on 18-04-2022 the Dept. of CS & IT Lab at 1:00 PM to 3:00 PM, all the participant students was joined the course and learned about the cryptography tenancies and how to securer public information through internet world. At the end of the day students given the test and qualify the above-mentioned value-added course.

Photos of the Event



Fig 1.1 Photo of the Event Value Added Course Introduction to Cryptography and Information Security



Fig 1.2 Photo of the Event Value Added Course Introduction to Cryptography and Information Security



Fig 1.3 Photo of the Event Value Added Course Introduction to Cryptography and Information Security



Fig 1.4 Photo of the Event Value Added Course Introduction to Cryptography and Information Security

Poster of the event



Brochure of the Event

PROGRAM SPECIFIC OUTCOMES

1. Prepare professionally trained in the area of programming, databases, software engineering, web designing, networking, and other application areas to acquire knowledge in various domain-based prospects.

2. Encourage them to communicate effectively and to improve their competency skills to solve real-time problems.

3. Understand to employ modern computer languages and applications for their successful career, create a platform to become entrepreneurs, and a relish for higher studies.

PROGRAM OUTCOMES

1. Apply knowledge of mathematics and science in solving computational problems
2. Understand the Computing concepts and their applications using the acquired board-based knowledge.
3. Design, set up, and conduct practical.
4. Use the techniques, skills, and modern Software tools for software development.
5. Identify and analyse software application problems in multiple aspects including coding, testing, and implementation in industrial applications.
6. Design, develop, and verify software systems to meet desired needs within realistic constraints, ensuring quality, reliability, security, and satisfying economical, ethical, social, and environmental constraints.
7. Apply Enterprise-level application software for the design of diverse software products.
8. Communicate effectively in diverse groups and exhibit leadership qualities.
9. Understanding of professional and ethical responsibility.

SHORT-TERM CERTIFICATION COURSE IN

Introduction to Cryptography And Information Security

JGi

ARKA JAIN University

Jharkhand (Jamshedpur)

ORGANIZED BY

Department of CS&IT

ARKA Jain University



COURSE OUTCOMES:

1. Identify basic security attacks and services.
2. Use symmetric and asymmetric key algorithms for cryptography
3. Design a security solution for a given application
4. Analyse Key Management techniques and the importance of number Theory
5. Understanding of Authentication functions in the manner in which Message Authentication Codes and Hash Functions work
6. To examine the issues and structure of Authentication Service and Electronic Mail Security

COURSE CONTENT:

UNIT I: 06 - Lecture
INTRODUCTION: Security trends, The OSI Security Architecture, Security Attacks, Security Services and Security Mechanisms, A model for Network security. CLASSICAL ENCRYPTION TECHNIQUES: Symmetric Cipher Modes, Substitute Techniques, Transposition Techniques, Rotor Machines, Stenography.

UNIT II 06 - Lecture
BLOCK CIPHER AND DATA ENCRYPTION STANDARDS: Block Cipher Principles, Data Encryption Standards, the Strength of DES, Differential and Linear Crypt Analysis, Block Cipher Design Principles.

UNIT III 06 - Lecture
ADVANCED ENCRYPTION STANDARDS: Evaluation Criteria for AES, the AES Cipher.
MORE ON SYMMETRIC CIPHERS: Multiple Encryption, Triple DES, Block Cipher Modes of Operation, Stream Cipher, and RC4.

UNIT IV 06 - Lecture
PUBLIC KEY CRYPTOGRAPHY AND RSA: Principles Public key crypto Systems, Define Hellman Key Exchange, the RSA algorithm, Key Management, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.

UNIT V 06 - Lecture
WEB SECURITY: Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET), Intruders, Viruses, and related threats.

ARKA JAIN University
Jharkhand

Convener: Prof. Arvind Pandey

COURSE DEVELOPERS:
Dr. ARUN KUMAR MARANDI
& Prof. ARVIND PANDEY

RESOURCE PERSONS:
Dr. ARUN KUMAR MARANDI
& Prof. ARVIND PANDEY

COURSE LOCATION:
ARKA JAIN University,
Jharkhand and online
(Google Meet)

Course Duration: 30 Hours
Commencement Date: 18.04.22
Batch No: - First

MASTERCLASSES EXPERTS:
A unique blend of Industry Experts and Academic Experts

BLENDED LEARNING:
On-Campus & Online Modules

WHO CAN ENROLL:
Faculty, Staff, and Students of ARKA JAIN University, Jharkhand

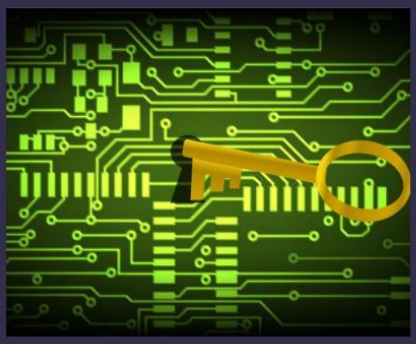


PROCESS OF ENROLMENT AND CERTIFICATION:

Interested candidates will fill the Enrolment form by downloading the same from the website of ARKA JAIN University and submitting the form to the Course Head. After Successful Registration, the Participants will attend the 30-hours course, in which 70% attendance will be mandatory. At the end of each module, the participant will be submitting an Assignment each and at the end of all the Modules, there will be an Assessment Paper. In order to qualify for receiving the Certificate, the participant must submit at least 4 Assignments out of 5 and obtain a minimum of 60 % marks in the Assignments and Assessment Paper, the Certificate from ARKA JAIN University, Jharkhand, will be awarded to the participant.

WHO IS THE PROGRAM FOR?

For candidates aspiring to learn the tending ways of using the internet, Cryptography is becoming increasingly important to enhance security in connection with data storage and communication and various kinds of electronic transactions. This course aims to give students a good knowledge of some commonly used cryptographic primitives and protocols, Cryptographic concepts, and methods.



LEARNING OBJECTIVES

- Summarize the main goals of cryptography and illustrate this with a number of examples of how cryptographic services are integrated into current applications, both in software and hardware
- describe goals and design principles for and common structures of secret key primitives such as block and stream ciphers and message authentication codes
- identify, analyse and explain various forms of attacks based on improper usage of primitives, modes, or Protocols
- explain how basic public key primitives can be defined based on the difficulty of mathematical problems such as the discrete logarithm problem or factoring and analyse variants of these systems
- explain the various roles of hash functions as parts of other cryptographic primitives and protocols and the requirements this places on hash functions
- exemplify when various notions of security, such as information-theoretic, computational, provable, and practical security, are applicable and describe the security guarantees provided
- explain basic key management techniques in both secret key and public-key Cryptography



ARKA JAIN University
Jharkhand

Topic of Value-Added Course Date and Time

S.NO.	DAY	TIME	Topic
1	18-04-2022 MONDAY	1:00 PM to 3:00 PM	**INTRODUCTION**: Security trends, The OSI Security Architecture, Security Attacks, Security Services, and Security Mechanisms, A model for Network security. CLASSICAL
2	19-04-2022 TUESDAY	1:00 PM to 3:00 PM	**ENCRYPTION TECHNIQUES**: Symmetric Cipher Modes, Substitute Techniques
3	20-04-2022 WEDNESDAY	1:00 PM to 3:00 PM	Transposition Techniques, Rotor Machines, Stenography. ADD-0N-
4	21-04-2022 THURSDAY	1:00 PM to 3:00 PM	**BLOCK CIPHER AND DATA ENCRYPTION STANDARDS**: Block Cipher Principles, Data Encryption Standards,
5	22-04-2022 FRIDAY	1:00 PM to 3:00 PM	The Strength of DES, Differential and Linear Crypt Analysis
6	25-04-2022 MONDAY	1:00 PM to 3:00 PM	Block Cipher Design Principles.
7	26-04-2022 TUESDAY	1:00 PM to 3:00 PM	**ADVANCED ENCRYPTION STANDARDS**: Evaluation Criteria for AES, the AES Cipher
8	27-04-2022 WEDNESDAY	1:00 PM to 3:00 PM	**MORE ON SYMMETRIC CIPHERS**: Multiple Encryption, Triple DES
9	28-04-2022 THURSDAY	1:00 PM to 3:00 PM	Block Cipher Modes of Operation, Stream Cipher, and RC4.
10	29-04-2022 FRIDAY	1:00 PM to 3:00 PM	**PUBLIC KEY CRYPTOGRAPHY AND RSA**: Principles Public key crypto Systems, Diffie Hellman Key Exchange,
11	04-05-2022 WEDNESDAY	1:00 PM to 3:00 PM	The RSA algorithm, Key Management
12	05-04-2022 THURSDAY	1:00 PM to 3:00 PM	Elliptic Curve Arithmetic, Elliptic Curve Cryptography.
13	06-04-2022 FRIDAY	1:00 PM to 3:00 PM	**WEB SECURITY:** Requirements, Secure Socket Layer (SSL)
14	07-04-2022 SATURDAY	4:00 PM to 6:00 PM	and Transport Layer Security (TLS), Secure Electronic Transaction (SET),
15	08-04-2022 SUNDAY	4:00 PM to 6:00 PM	Intruders, Viruses, and related threats

ARKA JAIN University
Jharkhand

List of Students

Full Name (Block Letters)	Registration Number	Course	YEAR	Email Address
KAWALJEET SINGH WALIA	AJU/200378	BCA	2nd	kawaljeetsingh5115@gmail.com
SHILPA KUMARI	AJU/201182	BCA	2nd	shilpa8608564@gmail.com
JAY KISHAN MAHATO	AJU/200899	BCA	2nd	jaykishanmahato68@gmail.com
SHRADDHA SANDIL	AJU/201093	BCA	2nd	shradhan236@gmail.com
PriyaKumari	AJU/211317	MCA	1st	priyamunda35@gmail.com
EshaKumari	AJU/201290	BCA	2nd	esha.kumari29@gmail.com
RAKESH KUMAR DAS	AJU/211240	MCA	1st	rakesuch@gmail.com
SANA AFRIN	AJU/210020	MCA	1st	sana.hussain21.sh@gmail.com
HARSHIT KUMAR SHARMA	AJU/190793	BCA	3rd	harshitkumarhks3@gmail.com
SAPNA GORAI	AJU/210019	MCA	1st	sapnagorai1998@gmail.com
MADHUMITA MUNDA	AJU/200857	BCA	2nd	madhumitaglory@gmail.com
AMAN KUMAR SINGH	AJU/210650	MCA	1st	kaman4422@gmail.com
ANUBHAV KARMAKAR	AJU/211506	MCA	1st	anubhavkarmakar70@gmail.com
ANUP KUMAR	AJU/200 669	BCA	2nd	anupkr8540@gmail.com
HARSH KUMAR	AJU/200499	BCA	2nd	harshrajputsingh122@gmail.com
BHAVNEET SINGH	AJU/210223	BCA	1st	bhavneetsingh772@gmail.com
UJJWAL KUMAR	AJU/210404	BCA	1st	ujjwalgupta12345911123@gmail.com
ABHAY SINGH	AJU/211713	MCA	1st	abhaysingh112000@gmail.com
Surajkumar saw	AJU/211620	MCA	1st	sawsooraj@gmail.com
VIKASH SHIT	AJU/210993	MCA	1st	vikashshit18@gmail.com
MAHESWAR SAREN	AJU/210785	MCA	1st	maheswarsaren117@gmail.com
DEEPAK JARIKA	AJU/210893	MCA	1st	deepakjarika8@gmail.com
ROHIT HANSDA	AJU/210786	MCA	1st	rohitjasonh@gmail.com
NIKHIL RAJAK	AJU/210044	MCA	1st	nikhilrajak437@gmail.com
PRIYA GHOSH	AJU/211385	MCA	1st	priyaghoshofficiall@gmail.com
AYUSHI KUMARI	AJU/210798	MCA	1st	ayukri0303@gmail.com
SANGITA KUMARI	AJU/210881	MCA	1st	rsangitasingh27rk@gmail.com
RAM KUMAR	AJU/201105	BCA	2nd	ramksahu8@gmail.com
SHIV	AJU/211565	MCA	1st	shivbhagat32@gmail.com
Aparajita Gaurav	AJU/210242	BCA	1st	12croll.5bioaparajita@gmail.com
HIRA LAL MAHATO	AJU/210584	MCA	1st	bablumahato0000@gmail.com
SHIVA GUPTA	AJU/211029	MCA	1st	shivagupta397@gmail.com
Suraj Kumar Dass	AJU/200997	BCA	4th	surajbksc002@gmail.com
KHUSHBOO KUMARI	AJU/201314	BCA	2nd	156khushbookumari@gmail.com
Aniket Kumar	AJU/200801	BCA	2nd	www.allinoneforyouhere@gmail.com
INDRAJEET CHOUHAN	AJU/211254	BCA	1st	indjchnn@gmail.com
ANIKET KUMAR SINGH	AJU/211512	BCA	1st	aniketsingh766747@gmail.com
SWEETY KHATRI	AJU/210876	BCA	1st	sweetykhatri856@gmail.com

Sample of the Certificate



JGi
ARKA JAIN University
Jharkhand (Jamshedpur)

CERTIFICATE

This is to certify that

Aniket Kumar Singh

from the BCA/MCA has participated in and completed successfully,

The Value Added Course on

"Introduction to Cryptography and Information Security"

organized by the Department of Computer Science and Information Technology,

ARKA JAIN UNIVERSITY, Jamshedpur held from 18-04-2022 to 09-05-2022

(DR. ARUN KUMAR MARANDI)
COORDINATOR
(CS & IT)

ARKA JAIN UNIVERSITY JHARKHAND

(DR. ARVIND KUMAR PANDEY)
HOD
(CS & IT)