

LIVE + SELF-PACED

CRYPTOGRAPHY CERTIFICATION COURSE (CCC)





COURSE OVERVIEW

The Cryptography Certification Course (CCC) offers participants a comprehensive and in-depth exploration of the fascinating world of cryptography. This course aims to provide individuals with a solid foundation in cryptographic principles, algorithms, and protocols. Students will learn to apply cryptographic techniques to protect data confidentiality, integrity, and authenticity. Through hands-on exercises and practical examples, participants will develop the necessary skills to design and implement secure communication channels and safeguard sensitive information from unauthorized access. Whether you're an aspiring cryptographer or a cybersecurity enthusiast, the CCC course will unlock the secrets of encryption, enabling you to address modern challenges and contribute to building secure digital systems.



COURSE OBJECTIVE

The Cryptography Certification Course (CCC) is designed to equip learners with advanced cryptographic knowledge and skills. Throughout this course, participants will delve into the intricacies of encryption, decryption, and secure communication protocols. By the end of the program, students will be proficient in employing cryptographic techniques to safeguard sensitive data and fortify digital communication against potential breaches.

WHAT YOU WILL LEARN

The Cryptography Certification Course (CCC) is a comprehensive program that immerses participants in the fascinating world of cryptography. Students will grasp the foundational principles of encryption and decryption techniques, exploring classical ciphers, modern symmetric and asymmetric cryptographic algorithms, and hashing functions. Through hands-on exercises and real-world examples, participants will develop a deep understanding of cryptographic protocols and their applications in various fields, including information security, digital signatures, secure communications, and data integrity.



Throughout the course, participants will gain insights into cryptographic vulnerabilities and attacks, learning how to analyze and defend against them. They will also delve into the importance of key management, random number generation, and certificate management to maintain the security of cryptographic systems effectively.

By the end of the CCC course, participants will be equipped with the expertise to design and implement secure cryptographic solutions, enabling them to contribute to the protection of sensitive information and critical data in modern digital environments.



COURSE SKILL SET

- Understand the basics of cybersecurity, its importance, and the role of a cybersecurity engineer.
- Learn about the three core principles of cybersecurity – Confidentiality, Integrity, and Availability.
- Study the various steps involved in the hacking process to better defend against attacks.
- Familiarize yourself with techniques used to manipulate people into revealing sensitive information.
- Gain knowledge about common cyber attacks like Brute Force, Phishing, DoS, DDoS, etc.
- Learn about different types of malware and cybersecurity breaches.
- Understand the methodologies used to simulate cyber attacks and identify vulnerabilities.
- Study the industry-accepted frameworks and standards for implementing cybersecurity measures.
- Explore the different categories of hackers and their motivations.
- Delve deeper into vulnerability assessment and penetration testing techniques.
- Learn about encryption, decryption, hashing, and digital signatures.
- Understand the differences between symmetric and asymmetric encryption algorithms.
- Study the RSA algorithm, which is widely used for secure data transmission.
- Get familiar with various authentication technologies used in modern systems.
- Explore biometric authentication methods like fingerprint recognition and facial recognition.
- Learn how to manage and control user identities in a secure manner.
- Understand the importance of setting strong account policies for enhanced security.
- Learn about securing email communications and protecting sensitive information.
- Study the concepts of Pretty Good Privacy and GNU Privacy Guard for secure email encryption.
- Explore techniques to maintain anonymity and use pseudonyms in email communications.

Instructor – **Ajay Gautam | Cyber Security Expert**

Instructor – **Aman Roy | Cyber Security Expert**

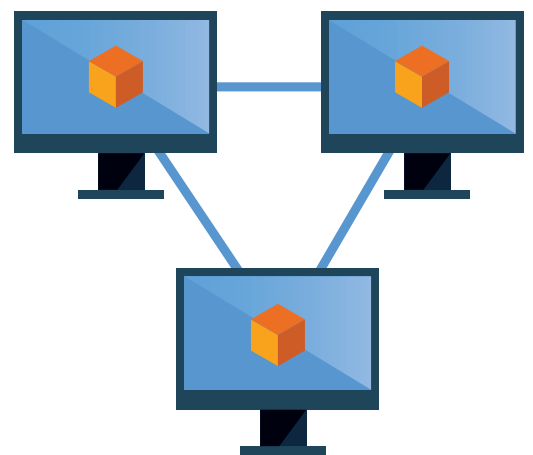
Duration – 1 Month

Eligibility – Any graduate with a Science stream

No. of Modules – 07 Modules

Language – English

Shareable certificate – Yes



PROGRAM SYLLABUS

Module 1 Introduction to Cybersecurity

- Session 1.1 Introduction
- Session 1.2 Why Cyber Security is Important?
- Session 1.3 Role of cyber security engineer
- Session 1.4 CIA Triad
- Session 1.5 The Hacking Methodology
- Session 1.6 The WhoIS Query
- Session 1.7 Social Engineering
- Session 1.8 Brute Force Attacks
- Session 1.9 Phishing
- Session 1.10 Bots and Botnets
- Session 1.11 DoS and DDoS
- Session 1.12 Pings
- Session 1.13 Man in the Middle Attacks (MITM)



Module 2 Cyber Security Building blocks

- Session 2.1 Malicious Codes and Terminologies
- Session 2.2 Cybersecurity Breaches
- Session 2.3 Penetration Testing and Methodologies
- Session 2.4 Frameworks and Standards for Cybersecurity

Module 3 Basic concepts of Vulnerability

- Session 3.1 Types of Hackers & Hacktivism
- Session 3.2 Understanding Terminologies
- Session 3.3 Vulnerability & Pentesting
- Session 3.4 Cyber Security Controls
- Session 3.5 Cyber Security Policies
- Session 3.6 CVE & CVSS

Module 4 Cryptography

- Session 4.1 Introduction to Cryptography
- Session 4.2 Types of attacks
- Session 4.3 Types of Crypto Systems
- Session 4.4 Encryption Introduction
- Session 4.5 Types of Encryption
- Session 4.6 Practical – Symmetric Encryption
- Session 4.7 DES & Working



Session 4.8 AES & Working
Session 4.9 Asymmetric Encryption
Session 4.10 Hashing & Hashing Algorithms
Session 4.11 RSA & Practical
Session 4.12 Message Authentication Codes.
Session 4.13 SHA & HMAC
Session 4.14 Digital Signatures
Session 4.15 Cryptographic Protocols
Session 4.16 Implementing SSL
Session 4.17 Public Key Infrastructure
Session 4.18 Cryptographic Use Cases and Weaknesses



Module 5 Architecture and Design

Session 5.1 Compare and Contrast Cryptographic Ciphers
Session 5.2 Cryptographic Modes of Operation
Session 5.3 Manage Certificates and Certificate Authorities -Part 1
Manage Certificates and Certificate Authorities -Part 2
Session 5.4 Implement PKI Management -Part 1
Implement PKI Management -Part 2
Session 5.5 Summarize Authentication Design Concepts -Part 1
Summarize Authentication Design Concepts -Part 2
Session 5.6 Implement Knowledge-Based Authentication
Session 5.7 Implement Authentication Technologies (JWT, SAML, OAUTH)
Session 5.8 Summarize Biometrics Authentication Concepts
Session 5.9 Identify Management Controls
Session 5.10 Implement Account Policies
Session 5.11 Implement Authorization Solutions -Part 1
Implement Authorization Solutions -Part 2
Session 5.12 Importance of Personnel Policies -Part 1
Importance of Personnel Policies -Part 2
Importance of Personnel Policies -Part 3



Module 6 Email: security, Privacy and Anonymity

Session 6.1 Introduction
Session 6.2 Clients, Protocols and Authentication
Session 6.3 Email Weaknesses
Session 6.4 PGP, GPG & Privacy



Session 6.5 PGP & GPG Clients

Session 6.6 PGP & GPG

Session 6.7 PGP & GPG Weaknesses

Session 6.8 Improving OpenPGP Security – Best Practices – Part 1

Improving OpenPGP Security – Best Practices – Part 2

Session 6.9 Improving OpenPGP Security – Primary and Subkeys – Part 2

Session 6.10 Email Tracking & Exploits

Session 6.11 Email Anonymity & Pseudonymity

Session 6.12 TorBirdy

Session 6.13 Remailers

Session 6.14 Choosing an Email Provider

Session 6.15 Email Alternatives (Guerrilla Mail)

Session 6.16 Email Spoofing

Module 7 Job roles

Session 7.1 Analyst Application Security

Session 7.2 Engineer Trainee

Session 7.3 Security Analyst

Session 7.4 Analyst Security Operations Centre





Sign up for

Webinars, Free courses and Paid Courses

starting from ₹499/- onwards only



Contact Us



+91 911177800



learn@aisectlearn.com



www.courses.aisectlearn.com