EC-Council Certified Encryption Specialist (ECES)

Introduction

The EC-Council Certified Encryption Specialist (ECES) program introduces professionals and students to the field of cryptography. The participants will learn the foundations of modern symmetric and key cryptography including the details of algorithms such as Feistel Functions, DES, and AES.

Key Outcomes

- Develop skills to protect critical data in organizations with encryption
- Develop a deep understanding of essential cryptography algorithms and their applications
- Make informed decisions about applying encryption technologies
- Save time and cost by avoiding common mistakes in implementing encryption technologies effectively
- Develop working knowledge of cryptanalysis

Course Outline

- Introduction and History of Cryptography
- Symmetric Cryptography and Hashes
- Number Theory and Asymmetric Cryptography
- Applications of Cryptography
- Cryptanalysis

Prerequisites

- Participants who wish to take part in the ECES certification training should have a minimum of 1-year experience in the information security domain along with basic knowledge of cryptanalysis.

- If a participant is looking to clear their ECES certification exam, they should attend an instructor-led ECES training from an EC-Council Accredited Training Center

Target Audience

Job roles that can take up ECES training include, but are not limited to:

- Ethical Hackers
- Penetration Testers
- IT Security Administrator
- Encryption Analysts
- Encryption Specialists
- Information security Analyst
- SOC Security Analyst
- Vulnerability Assessment Analysts
- Solution Architect
- Senior Security Consultant
- Security Compliance Analyst
- Mid-level Security Assurance Auditor
- System Security Administrator
- Network Security Engineer
- Aspiring Encryption Specialists
- Professionals who are looking to clear their ECES certification exam

Duration

24 hours training course