

## EC-Council Certified Encryption Specialist ( ECES )

### Course Summary

#### Description

If you think that there is only one type of encryption – think again!

Secure organizations employ multiple levels of encryption – database encryption, VoIP encryption, portable storage encryption, mobile devices encryption, Wi-Fi encryption, e-mail encryption, file encryption – server/desktop, network link encryption, web server encryption, tape backup encryption and many more.

Some of the most recent attacks that have had serious consequences share one thing in common – they all had either none or little effective encryption. This resulted in thousands of users being affected and hundreds of millions in losses. It resulted in serious decline of brand value and public embarrassment.

To name a few – SONY PS3, RSA, iPhone, LinkedIn

#### Objectives

By the end of this course, participants will learn:

- Types of Encryption Standards and their differences
- How to select the best standard for your organization
- How to enhance your pen – testing knowledge in encryption
- Correct and incorrect deployment of encryption technologies
- Common mistakes made in implementing encryption technologies
- Best practices when implementing encryption technologies

#### Topics

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

#### Audience

- Penetration Testers
- Anyone involved in selecting, implementing VPN's or digital certificates
- Computer Forensics Specialists
- Anyone involved in information security operations

#### Prerequisites

No prior knowledge of cryptography is assumed, and no mathematical skills beyond basic algebra are required.

#### Duration

Three days