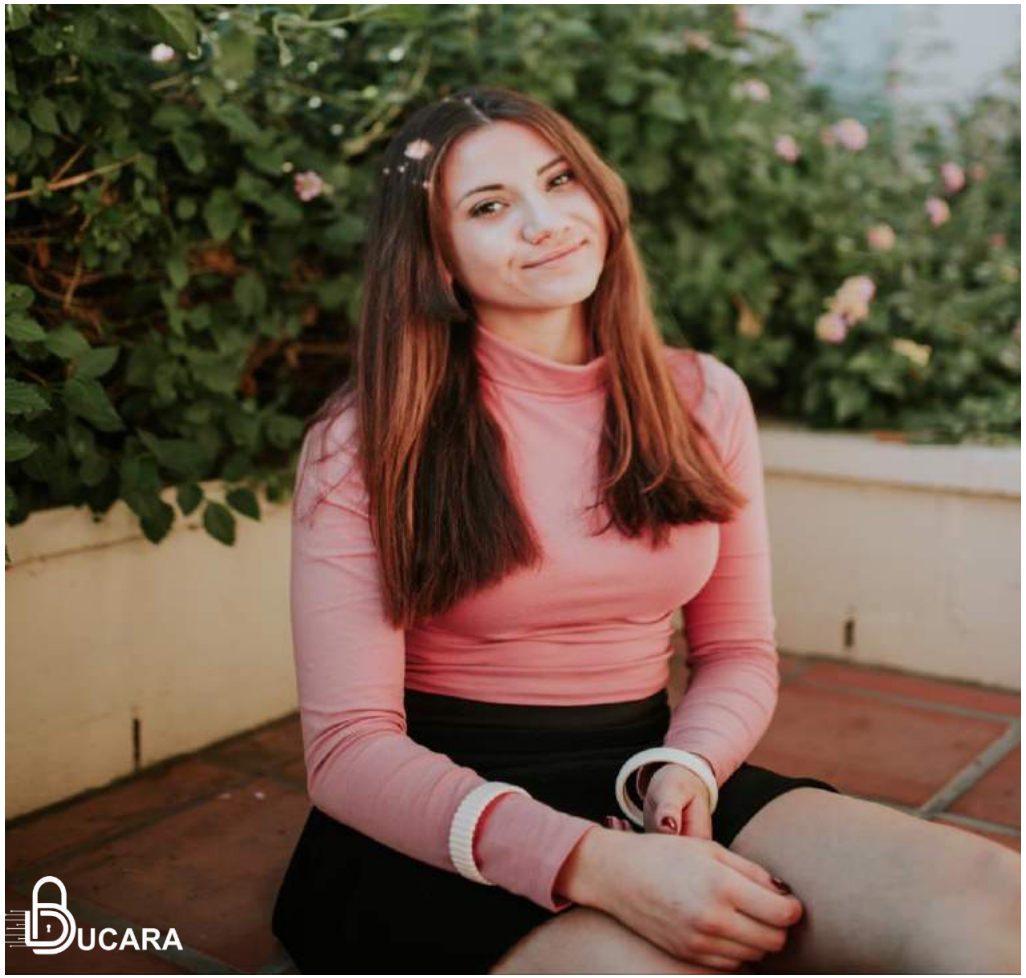
C|PTSI

Certified PKI & TLS Security Implementer

Ducara Info Solutions (P) Ltd.

DUCARA

Why Certified PKI & TLS Security Implementer?



C|PTSI Training Course will help you gain expertise in cryptography security development, architecture, design, applications, and operations.

This course give step by step guidance and easy-to-follow detailed explanation on every facet of cloud security. Opportunity for industry, research and academia communities, and government sectors.

Have a broad overview of the use of encryption technology in **Public Key Infrastructure** and **Transport Layer Security**. This includes an analysis of the most prolific attacks against crypto systems.

Develop an understanding of the concepts behind public key infrastructure, transport layer security and their application in real life.

What is the Course Outcome?

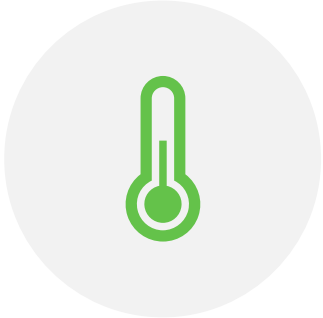
The C|PTSI certification training focuses to impart a deep and clear understanding of:

Standardize

Understanding of the fundamentals of cryptography, cipher, hashing algorithms and concept of Public Key Cryptography Standards.

Monitor

Securing website from unsolicited monitoring is essential to ensure the confidentiality of data that transit through the web. Key management concepts will also be introduced.



Decrypt

A practical use of encryption will be explored. Key management concepts will also be introduced. Encrypting and decrypting files with Bit locker.

Encrypt

Basics of encryption, the Encrypting File System currently used by Windows. Complemented with extensive exercises using the software discussed.

Create

The creation of a PKI using a variety of software and looking at tools which can exploit flaws in the implementation of a PKI.

Who can get the Course benefits?

Security Professionals

Network Security Developer

Security Analyst

Security Auditor

Cyprto-System Professionals

PKI implementer

Cyprto Analysts

Encryption Specialist

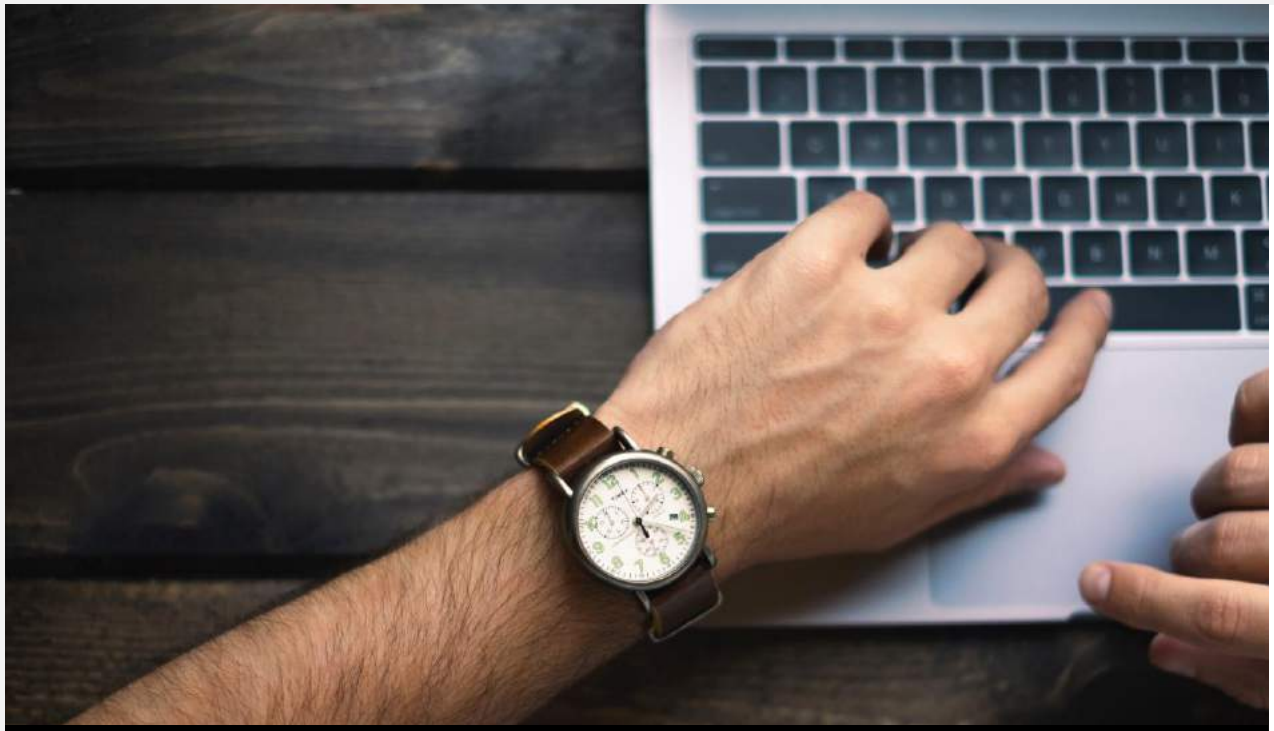
IT Professionals

IT Engineer

IT Developer

IT Consultant

Course Duration: 16 Hrs



What is the Course Outline?

Topics covered

1. Cryptography Fundamentals
2. Introduction to Public Key Infrastructure (PKI)
3. Governance and Enterprise Risk Management
4. Installing Certificate Authority Hierarchy
5. Transport Layer Security (TLS)

Module 1

Cryptography Fundamentals

1. CIA Triad
2. History of cryptography
3. Real world application of cryptography
4. Block and Stream Ciphers
5. Symmetric encryption
6. Symmetric encryption algorithms
7. Asymmetric encryption
8. Cryptographic Signatures
9. Hashing Algorithms
10. Windows password analysis

Module 2

Introduction to Public Key Infrastructure (PKI)

1. Definition and PKI components
2. X.509 certificates
3. Certificate Signatures
4. Public Key Cryptography Standards (PKCS)

Module 3

Disc Encryption

1. Disc Encryption technologies
2. Encrypting File System
3. BitLocker
4. Trusted Platform Modules
5. Attacking Disc Encryption
6. Investigating Encryption File System

Module 4

Installing Certificate Authority Hierarchy

1. Certificate of Authority (CA)
2. Types of Certification Authority
3. CA Hierarchy Design Guidelines
4. Root Certificate Authority
5. Analysis of problems with CA
6. Certification Revocation
7. Installing an Offline Root Certification Authority
8. Installing and Issuing Certificate Authority
9. Administering Certificate Templates
10. Installing an Online Responder

Module 5

Transport Layer Security (TLS)

1. Securing Web sites
2. TLS Traffic Analysis (Wireshark)
3. Creating a TLS-enabled Web Site
4. Analyzing TLS Traffic
5. Revoking a Certificate


Connect Us!
DUCARA
Ducara help harnessing latest security trends & enhancing skills to simplify IT security complexity efficiently.
info@ducarainfo.com
www.ducarainfo.com