

Practical Cryptography For Software Engineers

Learn via: **Classroom**

Duration: **2 Day**

Overview

Implementing a secure networked application can be difficult, even for developers who may have used various cryptographic building blocks (such as encryption and digital signatures) beforehand. In order to make the participants understand the role and usage of these cryptographic primitives, first a solid foundation on the main requirements of secure communication – secure acknowledgement, integrity, confidentiality, remote identification and anonymity – is given, while also presenting the typical problems that may damage these requirements along with real-world solutions.

In this course, after establishing the basics, the typical elements of cryptosystems and the most widely-used cryptographic algorithms in symmetric cryptography, hashing, asymmetric cryptography, and key agreement are detailed. Instead of presenting an in-depth mathematical background, these elements are discussed from a developer's perspective, showing typical use-case examples and practical considerations related to the use of crypto, such as public key infrastructures. Security protocols in many different areas of secure communication are introduced, with an in-depth discussion on the most widely-used protocol families such as IPSEC and SSL/TLS.

Prerequisites

There are no prerequisites for this course.

Who Should Attend

Developers, architects and testers developing security solutions.

What You Will Learn

- Understand basic concepts of security, IT security and secure coding
- Have a practical understanding of cryptography
- Understand the requirements of secure communication
- Understand essential security protocols
- Understand some recent attacks against cryptosystems
- Get sources and further readings on secure coding practices

Training Outline

- IT security and secure coding
- Requirements of secure communication
- Practical cryptography
- Security protocols
- Principles of security and secure coding
- Knowledge sources