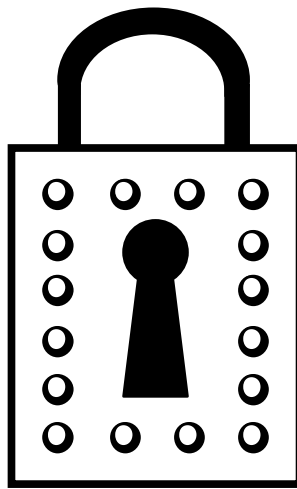


# Secure Communication Concepts Explained Simply



*A concise, self-teachable training course for people who want to understand the concepts of secure communications but don't need to know the details .*

---

## Copyright License

---

Copyright © 2008 Ciaran McHale

Permission is hereby granted, free of charge, to any person obtaining a copy of this training course and associated documentation files (the "Training Course"), to deal in the Training Course without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Training Course, and to permit persons to whom the Training Course is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Training Course.

THE TRAINING COURSE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE TRAINING COURSE OR THE USE OR OTHER DEALINGS IN THE TRAINING COURSE.

---

## About the Author

---

Ciaran McHale has a Ph.D. in computer science from Trinity College Dublin. He has been working for IONA Technologies ([www.iona.com](http://www.iona.com)) since 1995, where he is a principal consultant. His primary talent is the ability to digest complex ideas and re-explain them in simpler ways. He applies this talent to subjects that stir his passion, such as multi-threading, distributed middleware, code generation, configuration-file parsers, and writing training courses. You can find details of some of his work at his personal web site: [www.CiaranMcHale.com](http://www.CiaranMcHale.com). You can email him at [Ciaran@CiaranMcHale.com](mailto:Ciaran@CiaranMcHale.com).

---

## Table of Contents

---

1. Purpose of this Course

### **Part I — Cryptography**

2. Introduction to Cryptographic Terminology
3. Symmetric and Asymmetric Ciphers
4. Goals of Secure Communication
5. SSL and TLS
6. Miscellaneous Terminology

### **Part II — Access Control List**

7. Access Control List (ACL)

### **Part III — LDAP**

8. Introduction to LDAP
9. Organization of Data in LDAP