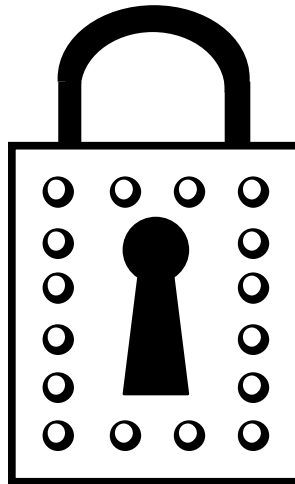


Goals of Secure Communication



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.

Goals of cryptographic communication

There are several goals of cipher-based communication...

- Confidentiality

- This is provided by using a strong cipher and secret key

- Authentication

- This is provided by the use of digital certificates, such as X509

- Integrity (also known as *message authentication*)

- This is provided by a MAC (message authentication code)

- Non-repudiation (discussed on the next slide)

Goals of cryptographic communication (cont')

■ Non-repudiation

- *Repudiate* means to deny, disown or reject as untrue.
- *Non-repudiation* means the ability to prove whether or not somebody sent a message

■ Example of the need for non-repudiation:

- An investor thinks the IBM share price will drop
- He tells his stockbroker to sell his IBM shares
- Soon afterwards, IBM shares increase in value
- The investor pretends he never told his stockbroker to sell his shares
- The stockbroker uses non-repudiation to prove the investor is lying

Authorization

- Authorization is an important goal in security
- However, authorization is distinct from cryptography:
 - It is *not* provided by cryptography
 - However, authorization *does* rely upon authentication