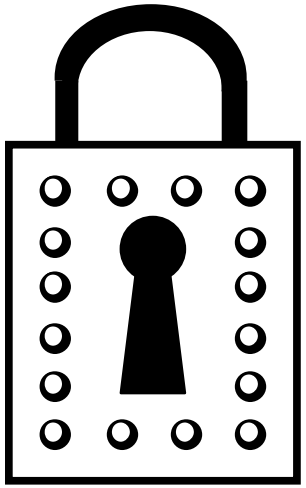
Goals of Secure Communication



License

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