



openHPI –Internet Security How to Safeguard Communication on the Internet?

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

How to Safeguard Communication on the Internet?

- Every communication on the Internet takes place along open communication channels
 - without precaution, attackers can read and modify all communication content
- Confidentiality of communication and other security objectives can be protected by **encryption**
- The science of encryption - **cryptography** - has existed for thousands of years
 - in those days, relatively simple methods of encryption were used
 - nowadays, encrypting procedures are much more complex to withstand attacks by powerful modern computers

Our Program for Course Week 5: Information Security through Cryptography

In this course week, we provide a basic understanding of **cryptography** and introduce different **encryption techniques**

We will explain in detail

- the basic principles of cryptography,
- the 1-key (or secret key) and the 2-key (or public key) encryption
- popular **encryption protocols** on the Internet.

Then we consider **security protocols** to achieve various security objectives – **confidentiality, integrity** (of the message or the sender) – by means of encryption and also the necessary security infrastructures – **PKI**