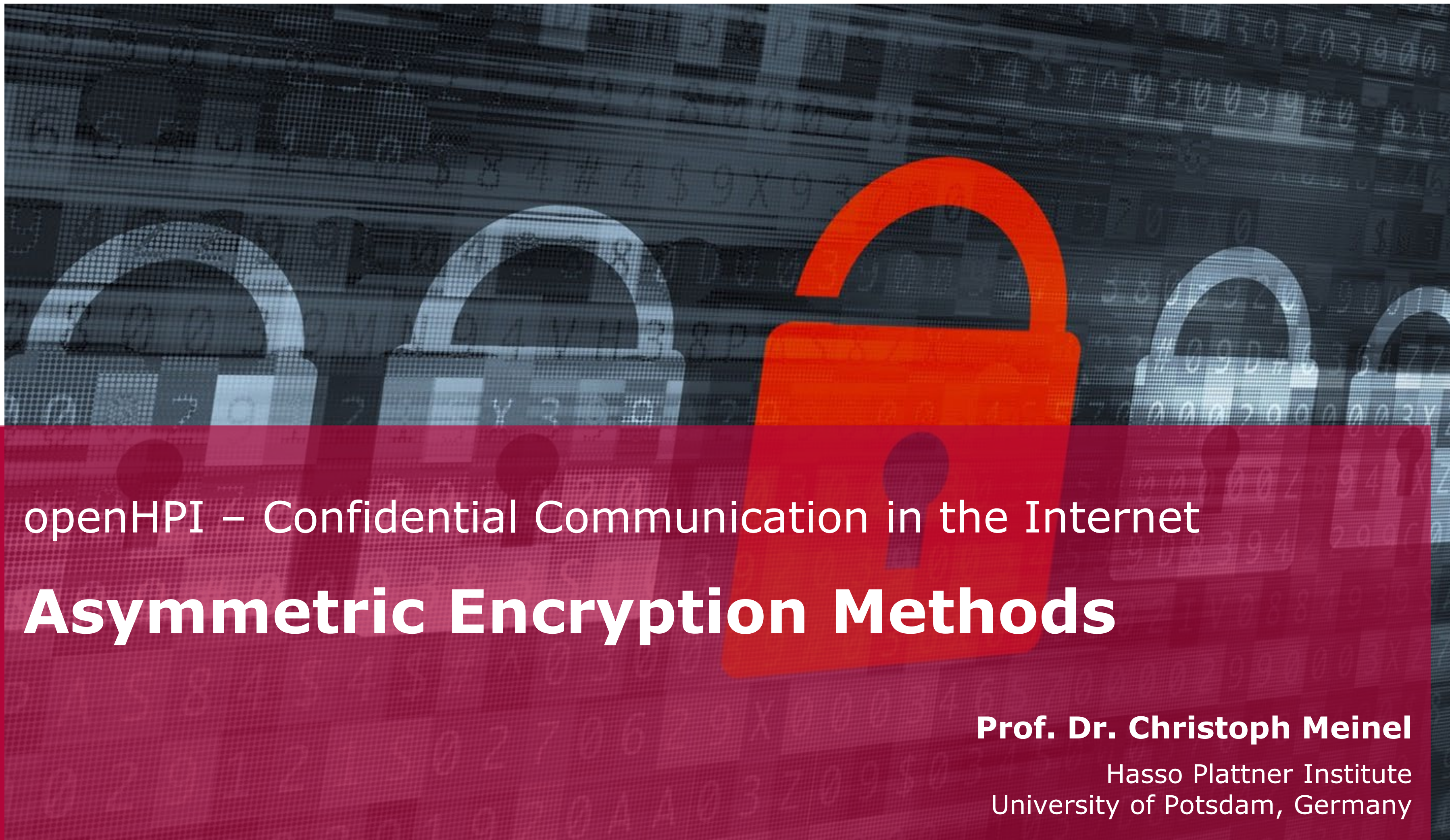

openHPI – Confidential Communication in the Internet

Asymmetric Encryption Methods

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Underlying Operating Principles

Use of key pairs for encryption and decryption:

- **Private Key**:
  - must be kept secret from any other communication partner
- **Public Key**:
  - will be made available to all other communication partner
- A message encrypted with a **public key** can only be decrypted with the corresponding **private key**
- A message encrypted with a **private key** can only be decrypted with the corresponding **public key**
- It is practically **impossible to construct** the private key from the public key

Asymmetric Encryption Procedures: **Encryption and Decryption** (1/2)

Prerequisite:

- All participants have a kay pair:
  - **private key** to be kept secret and
  - publicly accessible **public key**
- Private key can be securely assigned to a participant

Encryption of a message with a subscriber's **public key** allows only the subscriber to decrypt the message with his **private key**

$$F_{decrypt}(K_{Private}, F_{encrypt}(K_{Public}, Text)) = Text$$

Encrypted message stays **confidential**

Asymmetric Encryption Procedures: **Encryption and Decryption** (2/2)

Encryption of a message with a subscriber's **private key** allows anyone to verify that the message really originates from the sender, if the message can be decrypted with the subscriber's **public key**

$$(F_{decrypt} (K_{Public} , F_{encrypt} (K_{Private} , Text)) = Text$$

Ensuring the **legal** binding of the message and its sender and the **authenticity** of the sender

... but both approaches only work if:

- the public key is not compromised and
- the private key was kept secret

Asymmetric Encryption Algorithm: RSA (1/6)

RSA encryption is the most famous and most widespread asymmetric 2-key encryption method

- Developed 1977 by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman
- RSA is based on the practically (in realistic time) unsolvable mathematical problem of **factorization**:
  - product of two very large, randomly selected prime numbers practically (i.e. in realistic time) cannot be factorized without knowledge of the two prime numbers practically ...

Asymmetric Encryption Algorithm: RSA (2/6)

RSA procedure (Example shows as its work only with small numbers)**:**

Starting point:

1. Selection of two prime numbers, e.g. $p = 17$ and $q = 31$
2. Calculation of the product:

   $N = p * q$, e.g. $N = 17 * 31 = 527$

3. Calculation of the so-called Eulerian Phi-Function:

   $\varphi(N) = \varphi(p) * \varphi(q) = (p-1)*(q-1)$,

   (Explanation: φ(prime number) = (prime number-1))

   e.g. $\varphi(N) = 16 * 30 = 480$

Generation of a key pair for participants: ...

Asymmetric Encryption Algorithm: RSA (3/6)

Generation of a key pair for participants:

4. Election of a number e with $e < \varphi(N)$ that is coprime to $\varphi(N)$, e.g., $e = 13$

   $(e,N) = (13, 527)$ is the **public key**

5. Calculation of the multiplicative inverse d to e with regard to $\varphi(N)$, i.e., $e * d \bmod \varphi(N) = 1$

   e.g. $d = 37$, $e * d \bmod \varphi(N) = 13 * 37 \bmod 480 = 1$

   $(d,N) = (37, 527)$ is the **private key**

Remark:

- In the end, only e, d, N are needed to generate the public key (e,N) and the private key (d,N)

Asymmetric Encryption Algorithm: RSA (4/6)

Application of the procedure:

- Encrypt / decrypt with public / private key
  - cipher = message^{e} mod N
  - Message = cipher^{d} mod N
- Encrypt / Decrypt with private / public key
  - cipher = message^{d} mod N
  - Message = cipher^{e} mod N

Asymmetric Encryption Algorithm: RSA (5/6)

Application of the process – our example:

Communication partner B wants to send message "456" to A:

- B gets the public key **(e,N) = (13, 527)** from A and encrypts message "456":

$$456^{e} \bmod N \rightarrow 456^{13} \bmod 527 = 447$$

- B sends encrypted message "447" via the open Internet to A
- A can decrypt "447" with his private key (**d,N) = (37, 527)**:

$$447^{d} \bmod N \rightarrow 447^{37} \bmod 527 = 456$$

Asymmetric Encryption Algorithm: RSA (6/6)

Correctness of the RSA procedure is based on

Here some math is needed: **Fermat's little theorem**

- For any a and prime number p applies:

$$a^{p-1} \equiv 1 \textit{ mod } p, \text{ if a is not a multiple of p}$$

Chain of evidence:

- If $e*d \equiv 1 \textit{ mod } (p-1)*(q-1)$

  $\rightarrow \exists x: e*d - 1 = x * (p-1)*(q-1) \ldots$