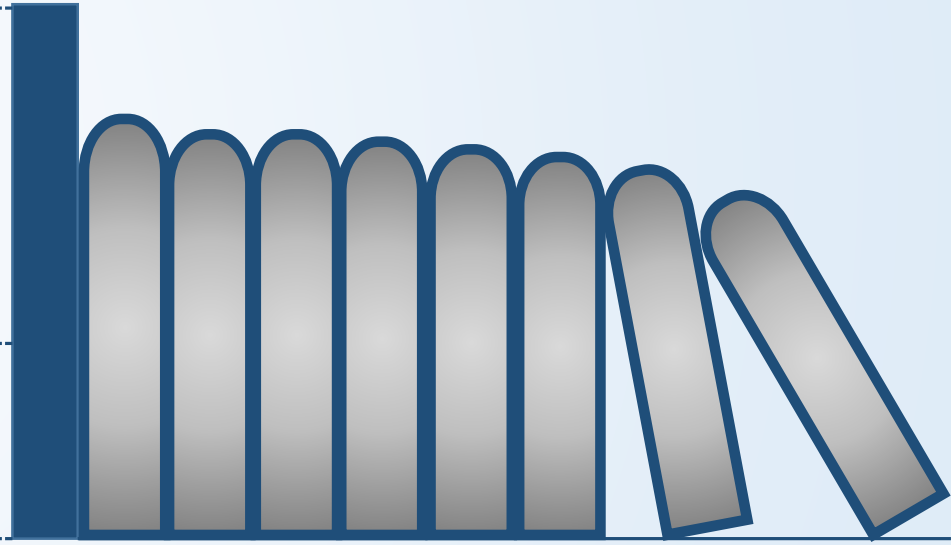
哈爾濱工業大學(深圳)

HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

RSA数字签名

主讲教师：蒋琳

实验教师：苏婷



实验目的

- 数字签名的基本原理，理解数字签名的作用
- 掌握 数字摘要算法的基本原理
- 掌握数字签名算法的实现

实验内容

1、计算一个文件test.txt的摘要（SHA1）；

2、对计算出的摘要进行数字签名；

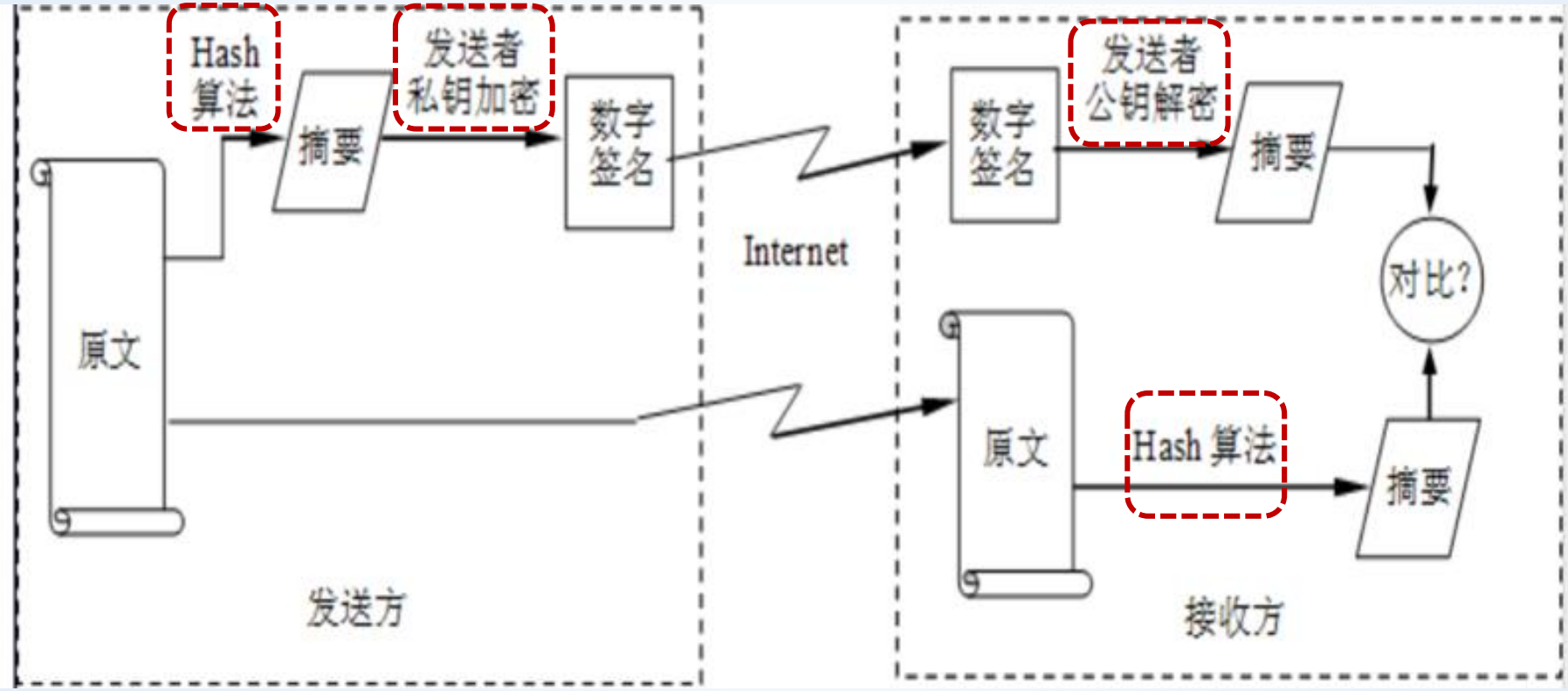
3、对数字签名进行验证:

1)test.txt不变，进行验证比对

2)test.txt改变一些字符，进行验证比对

实验原理

数字签名的原理图



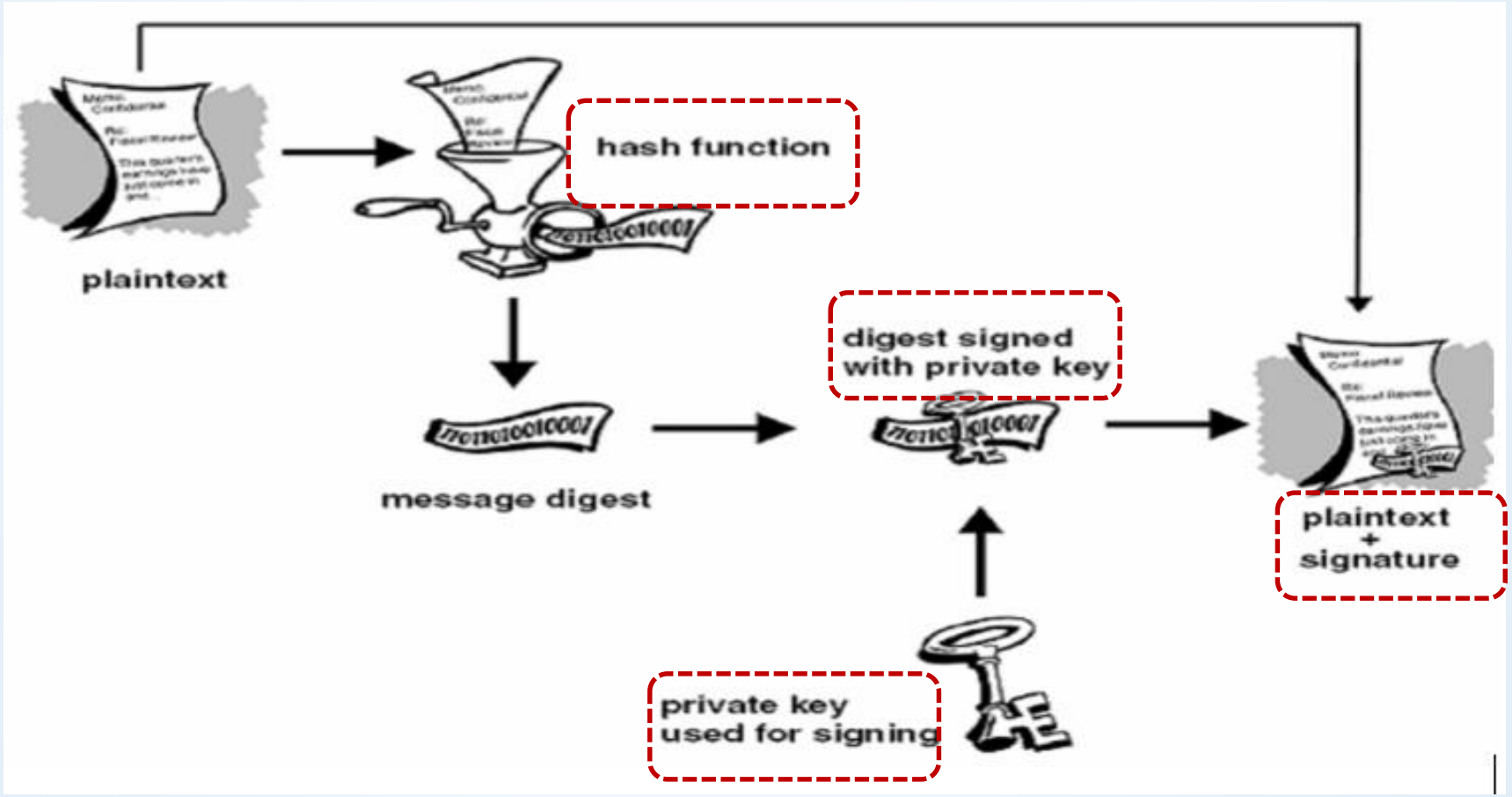
实验原理

➢ 数字签名的处理过程

- 适用Hash函数对消息进行编码，将发送文件加密产生160 bit的数字摘要
- 发送方用自己的私钥对摘要加密，形成数字签名；
- 将明文和加密的摘要同时传给对方；
- 接收方用发送方的公共密钥对摘要解密，同时对收到的文件用Hash函数产生同一摘要；
- 将解密后的摘要和收到的文件在接收方重新加密产生的摘要相互对比，如果两者一致，则说明在传送过程中信息没有被破坏和篡改，否则，则说明信息已经失去安全性和保密性。

实验原理

- 基于RSA的数字签名算法



实验原理

➢ RSA的数字签名算法---密钥生成

1、选两个保密的大素数p和q，计算$n=p\times q$，$\varphi(n)=(p-1)(q-1)$；

2、选一整数e，满足$1<e<\varphi(n)$，且$\gcd(\varphi(n),e)=1$；

3、计算d，满足$d\cdot e\equiv 1 \bmod \varphi(n)$；

4、以{e,n}为公钥, {d,n}为私钥。

实验原理

- **RSA的数字签名算法---签名算法**

设消息为m ∈Zn，对其签名为

$s=Sig_{sk}(m)\equiv m^d \bmod n$

$s=Sig_{sk}(H(m))\equiv H(m)^d \bmod n$

消息m的签名为s

注意：加入Hash函数的RSA数字签名更安全

实验原理

➢ RSA的数字签名算法---验证算法

接收方在收到消息m和签名s后，验证

$$m \overset{?}{\equiv} s^e \bmod n$$

加入了Hash函数的验证算法

$$H(m) \overset{?}{\equiv} s^e \bmod n$$

如果等式成立，则s是消息m的有效签名；反之，则是无效签名。

实验内容

1、计算一个文件test.txt的摘要（SHA1）；

2、对计算出的摘要进行数字签名；

3、对数字签名进行验证:

1)test.txt不变，进行验证比对

2)test.txt改变一些字符，进行验证比对

4、要求：至少用一个自己实现的算法（SHA1或RSA）

实验要求

- **请把电子版实验报告及源代码打包成一个zip上传到系统中，命名格式如下：**

  压缩包：“学号_姓名_实验5_RSA-SHA1数字签名”

  http://10.249.12.98:8000/#/login

有兴趣的同学可以参考查看RSA-PSS签名算法的实现

1、附件 RSA-PSS.pdf

2、链接

https://blog.csdn.net/ggj0727/article/details/115910385

https://blog.csdn.net/qq_34911465/article/details/78790377

请同学们开始实验！