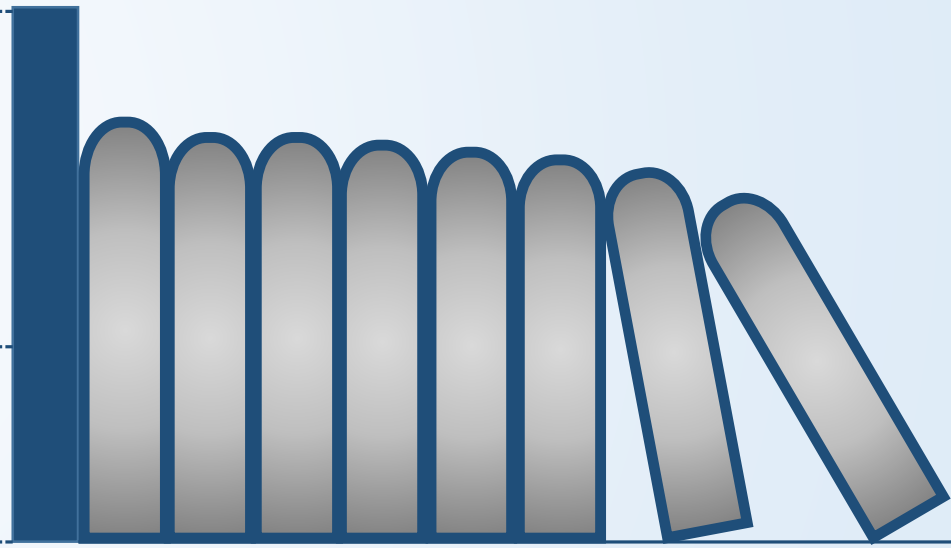
哈爾濱工業大學(深圳)

HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

RSA数字签名算法实验

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；

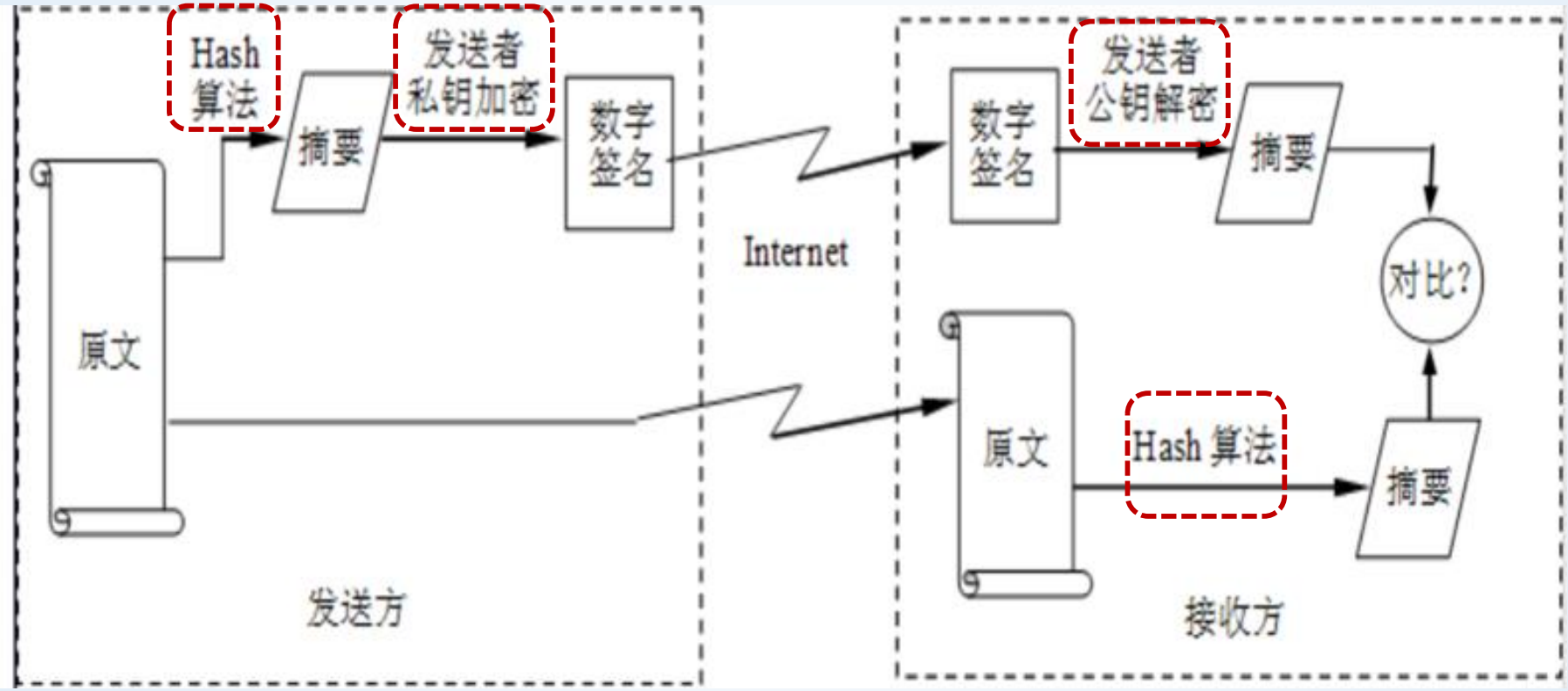
3、对数字签名进行验证:

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



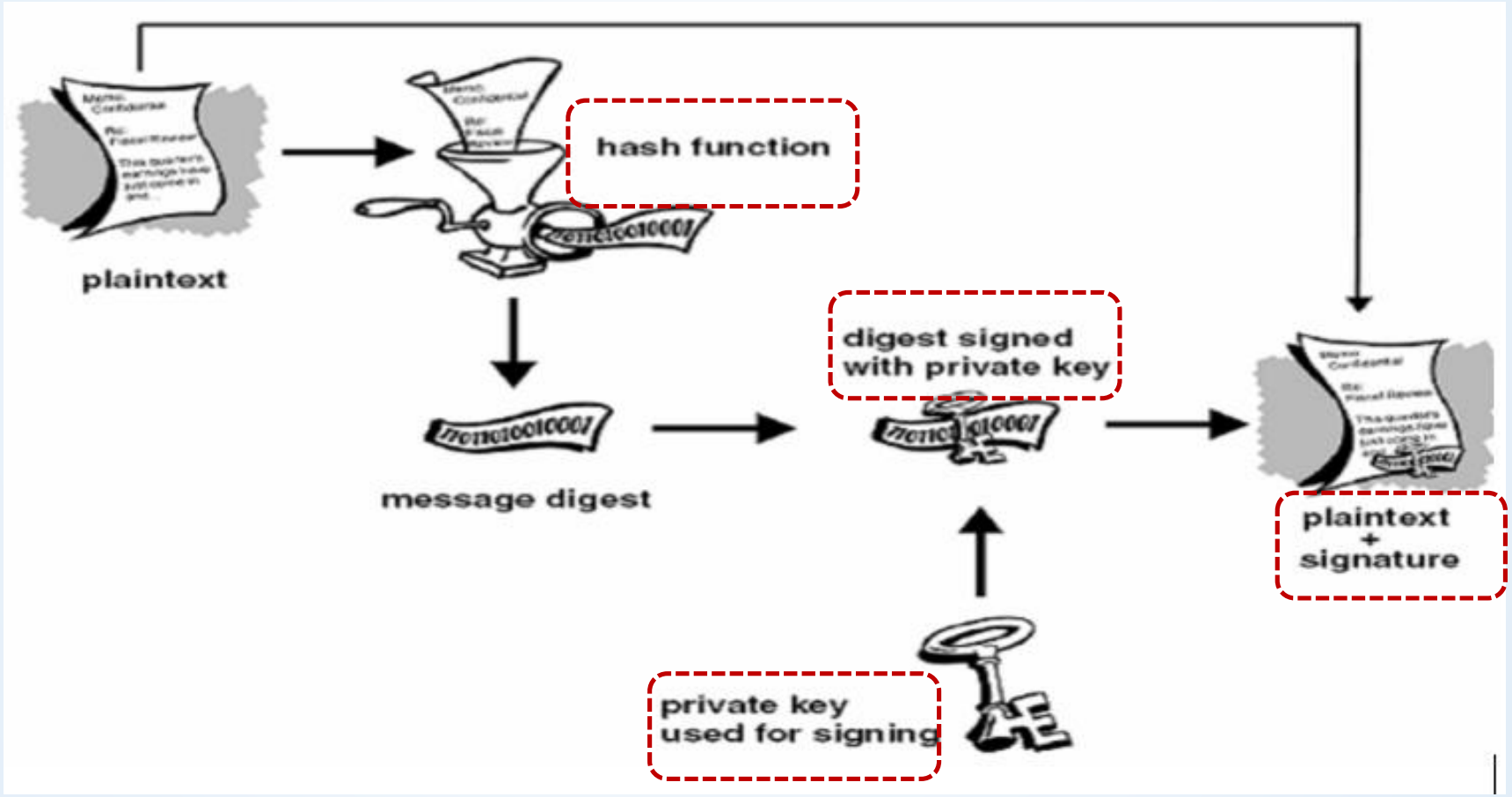
实验原理

➢ 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 /128 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×q，φ(n)=(p-1)(q-1)；

2、选一整数e，满足1<e<φ(n)，且gcd(φ(n),e)=1；

3、计算d，满足d·e≡1 mod φ(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/MD5）；

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：可调用大整数库，但是不能直接调用RSA接口。

https://blog.csdn.net/yang889999888/article/details/73442356

大家可参考大整数运算库gmp安装及使用

实验要求

➢ 截止时间

① 两周时间内提交（**2020-12-20 00:00**）

② 平台链接 http://10.249.182.83:8000/#/login

用户名/密码：学号/学号

初次登录，请修改密码！

➢ 提交内容

① 将源码和截图文件打成zip包上传

② 以学号_姓名命名

谢谢

实验原理

➢ 数字签名的密钥生成过程

1、设512≤L≤1024且L是64的倍数，选取2L-1 <p< 2L大素数, 其满足存在160比特的素数q|p-1

2、随机选取整数h，1<h<p-1且使g = $h^{(p-1)/q}$ mod p>1 q，p和g公开；

3、随机选取整数x,1≤x≤q-1，计算y =g^x mod p。

4、公钥为y，私钥为x

实验原理

➢ 签名算法

对于消息m，首先随机选取一个整数k, $1 \le k \le p-2$ ，然后计算：

$r = g^k \bmod p \bmod q$ ，

$s = (h(m)+xr)k^{-1} \bmod q$,

则m的签名为(r, s)，其中h为Hash函数SHA。

实验原理

➢ 验证算法

接收方在收到消息m和签名(r,s)后，计算

$u1 = h(m)s^{-1} \bmod q$

$u2 = rs^{-1} \bmod q$

验证等式

$g^{u1}y^{u2} \bmod p \bmod q = r$

- 如果等式成立，则(r,s)是消息m的有效签名；反之，则是无效签名。

实验原理

因为

$u1+xu2 \bmod q = (h(m)+xr)s^{-1} \bmod q = k$

所以

$g^{u1}y^{u2} \bmod p \bmod q = g^{u1+xu2} \bmod p \bmod q$

$= g^{k} \bmod p \bmod q = r$