为前程添彩！

我能过软考

第3章 密码学基本理论2
(数字签名知识补充、RSA、3.4节)

作品登记证书

登 记 号：黔作登字-2020-V-00113855

作品/制品名称：建群网培信息安全工程师系列视频教程　　作品类别：录像制品

作　　者：张建群[redacted]　　著作权人：[redacted]

创作完成日期：2017年05月28日　　首次发表/出版/制作日期：2017年12月07日

以上事项，由 张建群 申请，经 贵州省版权局 审核，根据《作品自愿登记试行办法》规定，予以登记。

登记日期：2020年08月20日　　登记机构签章

贵州省版权局 作品登记专用章

中华人民共和国国家版权局统一监制

严禁
盗录、
非法下载、
非法盗版

强烈鄙视天博软考
盗版建群网培的信安课程，
通过云盘发给学员

主要内容

我能过软考

作品登记证书

登 记 号：黔作登字-2020-V-00113855

作品/制品名称：建群网培信息安全工程师系列视频教程　　作品类别：录像制品

作　　者：张建群　　著作权人：

创作完成日期：2017年05月28日　　首次发表/出版/制作日期：2017年12月07日

以上事项，由 张建群 申请，经 贵州省版权局 审核，根据《作品自愿登记试行办法》规定，予以登记。

登记日期：2020年08月20日　　登记机构签章

作品登记专用章

中华人民共和国国家版权局统一监制

01 乘法逆元

02 传统密码体制存在一些问题

03 公钥密码体制设计思想

04 公开密钥密码的基本工作方式

利用扩展欧几里德算法求乘法逆元

- 模n乘法逆元
- 对于整数a、n，如果存在整数b，满足ab mod n =1，则说，b是a的模n乘法逆元。
- 定理：a存在模n的乘法逆元的充要条件是gcd(a,n) = 1

求：67 mod 119的逆元

求解过程

- Y3=0,则无逆元
- Y3=1，则Y2就是逆元
- Q=max_int(X3/Y3)

Q	X1	X2	X3	Y1(T1)	Y2(T2)	Y3(T3)				
-	1	0	119	0	1	67				
1	0	1	67	1	-1	52	Q=1	T1=X1-Q*Y1=1	T2=X2-Q*Y2=-1	T3=X3-Q*Y3=52
1	1	-1	52	-1	2	15	Q=1	T1=0-1=-1	T2=1+1=2	T3=67-52=15
3	-1	2	15	4	-7	7	Q=3	T1=1+3=4	T2=-1-6=-7	T3=52-45=7
2	4	-7	7	-9	16	1	Q=2	T1=-1-8=-9	T2=2+14=16	T3=15-2*7=1

如果Y2为负数，则加上n

利用代入法，求解逆元选择题

67 mod 119的逆元是（）。

A．52　　B．67　　C．16　　D．19

A. 67*52-1=3483 3483/119=29.26	B. 67*67-1=4488 4488/119=37.71
C. 67*16-1=1071 1071/119=9	D. 67*19-1=1272 4488/119=10.69

参考答案：C

负数求模

加模再取模

如：-12 mod17

求模：（-12+17）mod17=5

例如求13/14mod11

解：1）当分子或分母大于模数时，可以用分子、分母mod N，使分子分母变小

13/14 mod11 =(13mod11)/(14mod 11) mod 11

=2/3 mod11

=2*3^{-1}mod11（变成了求3关于模11的乘法逆元，使用转展相除

这里数字比较小，可以猜出逆元为4）

=2*4mod11

=8mod 11

=8

主要内容

我能过软考

作品登记证书

登 记 号：黔作登字-2020-V-00113855

作品/制品名称：建群网培信息安全工程师系列视频教程　　作品类别：录像制品

作　　者：张建群　　著作权人：

创作完成日期：2017年05月28日　　首次发表/出版/制作日期：2017年12月07日

以上事项，由 张建群 申请，经 贵州省版权局 审核，根据《作品自愿登记试行办法》规定，予以登记。

登记日期：2020年08月20日　　登记机构签章

贵州省版权局 作品登记专用章

中华人民共和国国家版权局统一监制

01 乘法逆元

02 传统密码体制存在一些问题

03 公钥密码体制设计思想

04 公开密钥密码的基本工作方式

传统密码体制存在一些问题

- 密钥管理困难
  - 传统密钥管理两两分别用一对密钥时，则n 个用户需要C(n, 2)= n(n- 1)/ 2 个密钥，当用户量增大时密钥空间急剧增大。如:

    n= 100 时C(100,2)= 4,950

    n= 5000 时C(5000,2)= 12,497,500

- 陌生人间的保密通信问题 （密钥发送）

  比如：陌生人之间的密码传递问题

- 数字签名的问题

  传统加密算法无法实现抗抵赖的需求

主要内容

我能过软考

作品登记证书

登 记 号：黔作登字-2020-V-00113855

作品/制品名称：建群网培信息安全工程师系列视频教程　　作品类别：录像制品

作　　者：张建群　　著作权人：

创作完成日期：2017年05月28日　　首次发表/出版/制作日期：2017年12月07日

以上事项，由 张建群 申请，经 贵州省版权局 审核，根据《作品自愿登记试行办法》规定，予以登记。

登记日期：2020年08月20日　　登记机构签章

贵州省版权局 作品登记专用章

中华人民共和国国家版权局统一监制

01 乘法逆元

02 传统密码体制存在一些问题

03 公钥密码体制设计思想

04 公开密钥密码的基本工作方式

公钥密码体制设计思想

- Diffie和Hellman提出：

  1） 密码算法有一对密钥：一个用于加密，称为加密密钥；一个用于解密，称为解密密钥。 $K_e \neq K_d$ （非对称密码）

  2）加密密钥是公开的，而解密密钥是保密的，且加密密钥的公开不会危及解密密钥的安全。

- 实现加密消息是自由的，但解密受限！（保密通信）
- 可实现一个用户使用秘密密钥处理信息，允许多个用户使用公开密钥解读处理过的信息。（数字签名）

公钥密码体制设计思想

单向函数

- 一个函数y=f(x),如果满足以下两个条件，则称为单向函数：
  1）如果对于给定的x，可以很容易计算出y
  2）而对于给定的y，很难计算出X

➢正变换可以加密，但是，加密后不能还原。

单向陷门函数

- 一个函数y=f(x),且f具有陷门，如果满足以下两个条件，则称为单向陷门函数：
  1）如果对于给定的x，可以很容易计算出y
  2）而对于给定的y，如果不掌握陷门，很难计算出X，而如果掌握陷门要计算出X就很容易。

➢如果利用单向陷门函数构造密码：用正变换作加密，加密效率高，用逆变换作解密，安全；
➢把陷门信息作为密钥，且只分配给合法用户，确保合法用能够方便的解密，而非法用户不能破译。

三个单向性很好的函数

1）**大合数的因子分解问题**： 大素数的乘积容易计算，如（p*q=n），而大合数的因子分解困难（n推出p和q)

2）**有限域上的离散对数问题**： 有限域上大素数的幂乘容易计算（$a^b \rightarrow c$），而对数计算困难（$\log_a c \rightarrow b$)

公钥密码体制设计思想

一个公开密钥密码应当满足以下三个条件：

1）解密算法D与加密算法互逆，即对于所有明文M都有：
$D(E(M, K_e), K_d) = M$

构成密码的基本条件

2）在计算上不能由K_e求出K_d。

公开公钥密码的安全条件

3）算法E和D都是高效的。

公开公钥密码的实用条件

4）对所有明文M都有
$E(D(M, K_d), K_e) = M$

公开公钥密码确保数据真实性的充分条件

- 满足1、2、3条件确保数据的秘密性
- 满足1、2、4条件确保数据的真实性
- 满足1、2、3、4条件确保数据的秘密性和真实性 $D(E(M, K_e), K_d) = E(D(M, K_d), K_e) = M$

主要内容

我能过软考

作品登记证书

登 记 号：黔作登字-2020-V-00113855

作品/制品名称：建群网培信息安全工程师系列视频教程　　作品类别：录像制品

作　　者：张建群　　著作权人：

创作完成日期：2017年05月28日　　首次发表/出版/制作日期：2017年12月07日

以上事项，由 张建群 申请，经 贵州省版权局 审核，根据《作品自愿登记试行办法》规定，予以登记。

登记日期：2020年08月20日　　登记机构签章

贵州省版权局 作品登记专用章

中华人民共和国国家版权局统一监制

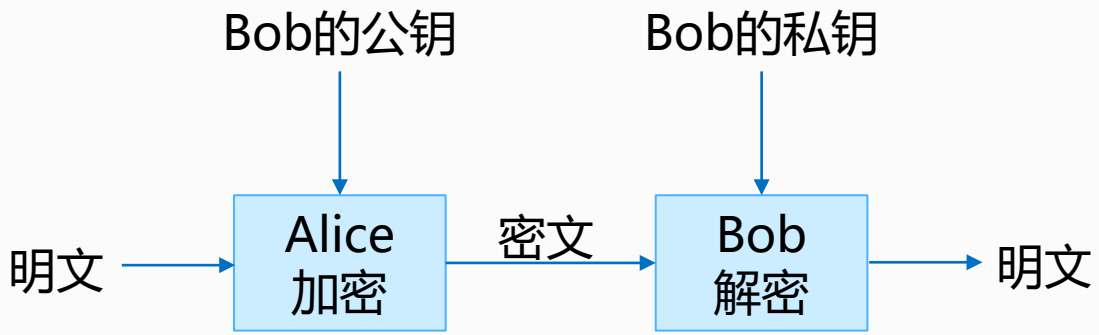
01 乘法逆元

02 传统密码体制存在一些问题

03 公钥密码体制设计思想

04 公开密钥密码的基本工作方式

公开密钥密码的基本工作方式



- 明文 M
- 密文 C
- E是加密算法
- D是解密算法
- K_e是加密密钥，公开
- K_d是解密密钥，保密
- 属于非对称密码

Bob	**Bob的K_e**
Alice	Alice的K_e

→ PKDB

公开密钥密码的基本工作方式

1. 确保数据的秘密性

➢发方：

① A首先查PKDB，查到 B 的公开的加密钥 K_{eB} 。

② A用 K_{eB} 加密 M 得到密文 C：

$$C=E(M, K_{eB})$$

③ A 发 C 给 B 。

保秘密性

➢收方：

① B 接受 C 。

② B用自己的保密的解密钥 K_{dB} 解密 C，得到明文 $M=D(C, K_{dB})$。

不保真实

2. 确保数据真实性

➢发方：

① A首先用自己的保密的解密钥 K_{dA} 解密 M，得到密文 C：

$$C=D(M, K_{dA})$$

② A 发 C 给 B 。

保真实

➢收方：

① B 接受 C 。

② B 查PKDB，查到A的公开的加密钥 K_{eA} 。

③ 用 K_{eB} 加密 C 得到 $M=E(C, K_{eA})$。

不保秘密性

3. 同时确保数据的秘密性和真实性

A —M→ B

➢发方：

① A首先用自己的保密的解密钥 K_{dA} 解密 M，得到中间密文 S：

$$S=D(M, K_{dA})$$

② 然后 A 查PKDB，查到 B 的公开的加密钥 K_{eB}。

③ A 用 K_{eB} 加密 S 得到最终的密文 C：

$$C=E(S, K_{eB})$$

④ A 发 C 给 B。

➢收方：

① B 接受 C。

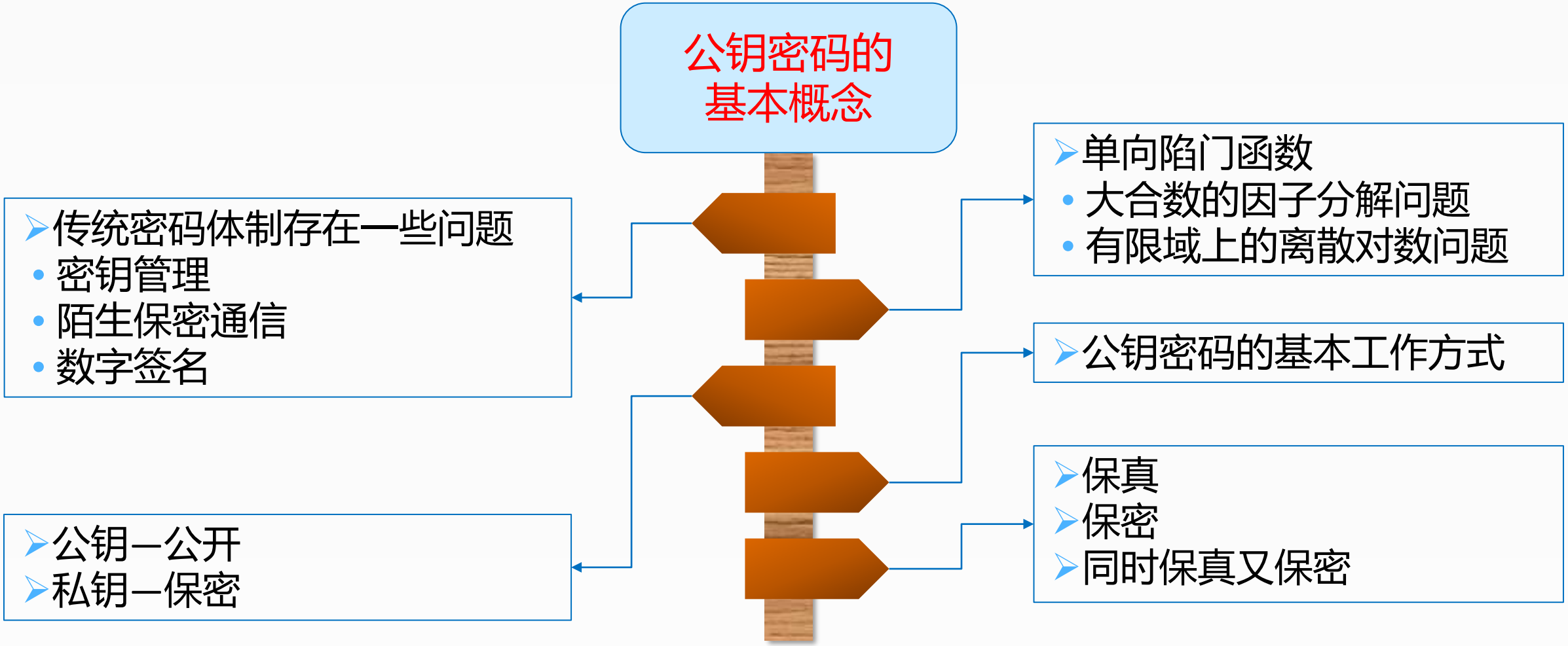
② B 用自己的保密的解密钥 K_{dB} 解密 C，得到中间密文$S=D(C, K_{dB})$

③ B 查PKDB，查到 A 的公开的加密钥 K_{eA}。用 K_{eB} 加密 S 得到 $M=E(S, K_{eA})$。

先签名后加密

1、利用公开密钥算法进行数据加密时，采用的方式是（）
A.发送方用公开密钥加密，接收方用公开密钥解密
B.发送方用私有密钥加密，接收方用私有密钥解密
C.发送方用公开密钥加密，接收方用私有密钥解密
D.发送方用私有密钥加密，接收方用公开密钥解密

小结



主要内容

作品登记证书

登 记 号：黔作登字-2020-V-00113855

作品/制品名称：建群网培信息安全工程师系列视频教程　作品类别：录像制品

作　　者：张建群　著作权人：

创作完成日期：2017年05月28日　首次发表/出版/制作日期：2017年12月07日

以上事项，由 张建群 申请，经 贵州省版权局 审核，根据《作品自愿登记试行办法》规定，予以登记。

登记日期：2020年08月20日　登记机构签章

中华人民共和国国家版权局统一监制

01 RSA概述

02 RSA算法加密解密过程

03 快速计算 $a^k \bmod n$

04 RSA密码的安全性

RSA算法概述

RSA
- R.L.Rivest
- A.Shamir
- L.Adleman

麻省理工大学
1978年

安全性高
广泛使用

- 基于大合数的因子分解的困难性
- 可用于加密
- 可用于数字签名

RSA算法加密解密过程

① 随机地选择两个大素数 p 和 q ，而且保密；

② 计算 n=pq ，将 n 公开；

③ 计算 φ$(n)=(p-1)(q-1)$ ，对 φ(n) 保密；

④ 随机地选取一个正整数 e， $1<e<$φ(n) 且 （e , φ(n) ） $=1$, 将 e 公开；

⑤ 根据 $ed=1$ mod φ(n)，求出d，并对d保密；

公钥：<e,n>
私钥：<p,q,Ø(n),d>

⑥加密运算：

$$C=M^e \mod n$$

⑦解密运算：

$$M=C^d \mod n$$

- φ(n) 是欧拉函数，表示小于n的正整数中，与n互素的数的个数。
- Ø(6)=2　在小于6的正整数中，只有1和5两个数与6互素

例1：假设RSA密码体制中，p=3，q=11，取加密密钥e为7，
1）求解密密钥d
2）写出相应的加密算法和解密算法
3）对明文M=8加密

解：　n=p*q=3*11=33, Ø(n)=(p-1)*(q-1)=2*10=20
　　由：　ed=1mod Ø(n)
　　即：7d=1 mod 20　，　　得：d=3　　(可以再看看求乘法逆的视频)

加密：
　　$C=M^e \bmod n$
　　$=8^7 \bmod 33$
　　$=2$

解密：
　　$M=C^d \bmod n$
　　$=2^3 \bmod 33$
　　$=8$

快速计算 $a^k \bmod n$

平方：从t0开始算，即a mod n
乘：把非0对应的t进行相乘，再模n

快速计算$a^k \bmod n$，可以采用“平方-乘”算法：
设k的二进制表示为：

$$k=a_0+ a_1 *2^1 +...+ a_r *2^r \quad , a_r=0 \text{ 或} 1$$

先连续“平方”，计算

$t_0 \equiv a(\bmod n)$

$t_1 \equiv t_0^2 \equiv a^2 \bmod n$

$t_2 \equiv t_1^2 \equiv (a^2)^2 \bmod n$

…

$t_r \equiv t_{r-1}^2 \equiv a^2 \bmod n$

求：$8^7 \bmod 33$

因为：$7=1+1*2+1*2^2$

因此，$t_0 \equiv 8(\bmod 33)$

$t_1 \equiv t_0^2 \equiv 8^2 \bmod 33 \equiv 31$

$t_2 \equiv t_1^2 \equiv (31)^2 \bmod 33$

$\equiv 4$

所以，$8^7 \bmod 33 = t_0 * t_1 * t_2$

$=8*31*4$

$=992$

$\equiv 2 \quad (\bmod 33)$

- 请大家计算$2^3 \bmod 33$

$8^7 \cdot \bmod 33$

7 转为二进制数 $0111=1*2^0+1*2^1+1*2^2$

利用平方-乘计算，上式中 2 的指数最高为 2，也就是说最多算到 t2

$t_0=8 \cdot \bmod 33=8$

$t_1=(t_0)^2 \cdot \bmod 33=8^2 \bmod 33=31$

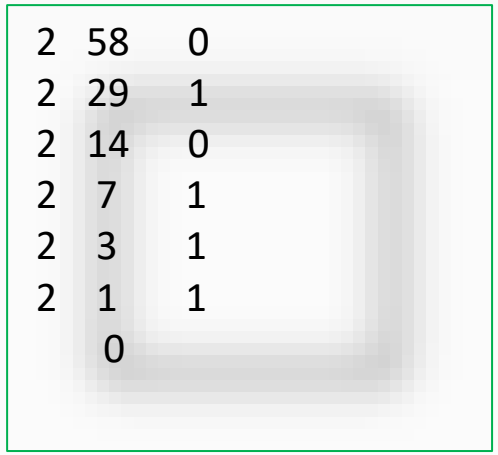
$t_2=(t1)^2 \cdot \bmod 33=31^2 \bmod 33=4$

7 转为二进制数 $0111=1*2^0+1*2^1+1*2^2$，这些 2^n 前面的系数都是 1，

则对应的 t_n 要参与相乘，如为 0，则对应的 t_n 不参与最后的相乘

$8^7 \cdot \bmod 33=(t_0*t_1*t_2) \bmod 33=8*31*4 \cdot \bmod 33=2 \cdot \bmod 33$

例 5^58 mod 97 =44



2	58	0
2	29	1
2	14	0
2	7	1
2	3	1
2	1	1
	0	

00111010

求：$5^{58} \bmod 97$

因为： $58=1*2+1*2^3+1*2^4+1*2^5$

因此， $t_0 \equiv 5 \pmod{97} = 5$

$t_1 \equiv t_0^2 \equiv 5^2 \bmod 97 \equiv 25$

$t_2 \equiv t_1^2 \equiv (25)^2 \bmod 97 \equiv 43$

$t_3 \equiv t_2^2 \equiv (43)^2 \bmod 97 \equiv 6$

$t_4 \equiv t_3^2 \equiv (6)^2 \bmod 97 \equiv 36$

$t_5 \equiv t_4^2 \equiv (36)^2 \bmod 97 \equiv 35$

所以， $5^{58} \bmod 97 = t_1 * t_3 * t_4 * t_5 \bmod 97$

$=25*6*36*35 \bmod 97$

$=44 \bmod 97$

RSA密码的安全性

1） p和q 要足够大

- 一般应用： p和q 建议1024位（二进制数），重要应用建议2048位

2） p和q 应为强素数

- 一般应用： p和q 建议1024位（二进制数），重要应用建议2048位
- (p-1)、（p+1）、（q-1）、（q+1）四个数中之一只有小的素因子，n就容易分解。

3） p和q 的差要大

4） (p-1)和（q-1） 的最大公因子要小

5） e的选择

- 随机且含1多更安全，但是计算慢。建议取$e=2^{16}+1=65537$

6） d的选择

- d不能太小，要足够大

7） 不要许多用户共用一个模n，易受共模攻击

1、设在RSA的公钥密码体制中，公钥为（e，n）=（13,35），则私钥d为（）

A、11　　B、13　　C、15　　D、17

解析：

已知公钥为（e，n）=（13,35），

n=pq=35，且p与q是素数，因此，可以推断出p与q分别是5与7，

Ø （n）=（p-1）*（q-1）=24，

而ed=1 mod ¢（n），

则13d=1mod24，

现在就变成了求乘法逆元，可以按照扩展欧几里得算法求解，当然，我们这里是选择题，可以把选项代进去试一试，11*13mod24=23,13*13mod24=1,因此，私钥d=13

关于求乘法逆元，请看看视频—利用扩展欧几里得算法求解乘法逆元

小结

- RSA概述
  - 基于大合数的因子分解的困难性
  - 可用于加密
  - 可用于数字签名
- RSA算法加密解密过程

RSA密码

- 快速计算 $a^k \bmod n$
- RSA密码的安全性

1、利用RSA算法运算，如果p=11，q=13, e=103,对明文3进行加密.求d及密文

解 n=p*q=11*13=143

$\Phi(n)=(p-1)(q-1)=10*12=120.$

$ed\equiv 1 \bmod \Phi(n)$

$103d\equiv 1 \bmod 120$

d=7

密文为 $c=m^e \bmod n = 3^{103} \bmod 143=16$

2、 在使用RSA的公钥体制中，已截获发给某用户的密文为c=10，该用户的公钥e = 5， n =35，那么明文m等于多少？为什么能根据公钥可以破解密文？

解 n=p*q (p和q都是素数)，n=35 故解出p=5 ， q=7 ；

Φ（n）=（p-1）*(q-1)=24 ；

又因为e*d≡1 modΦ（n），而e=5故可解出d=5;

m= c^d mod n=10^5 mod 35=5 。

因为RSA密码体制的安全性是基于分解大整数的困难性设计的。RSA算法的加密函数c= m^e mod n是一个单项函数，故对于解密密文的陷门是分解n=p*q ，只要知道这个分解就可以计算Φ（n）=（p-1）*(q-1)，然后用扩展欧几里德算法来求计算解密私钥d。由于本题中大整数比较小，该数的分解很容易，这样加密函数就不是一个单向函数，所以可以根据公钥能破解密文。

2020年信安案例分析试题二(共20分)

南读下列说明，回答问题1, 至问题8. 将解答填入答题纸的对应栏内。
[说明]密码学作为信息安全的关键技术。在信息安全领域有着广泛的应用。密码学中，根据加密和解密过程所采用密钥的特点可以将密码算法分为两类:对称密码算法和非对称密码算法。此外，密码技术还用于信息鉴别、 数据完整性检验、数字签名等，
[问题1](3分)信息安全的基本目标包括:真实性、保密性、完整性、不可否认性、可控性、可用性、可审查性等。密码学的三大安全目标C.I.A分别表示什么?

答：保密性、完整性、可用性
问题2] (3分)RSA公钥密码是一种基于大整数因子分解难题的公开密钥密码。 对于RSA密码的参数: p.q.n. Ø(n),e,d, 哪些参数是可以公开的

答：公开< n ， e>

[问题3] (2分)如有RSA密码算法的公钥为(55, 3),请给出对小王的年龄18进行加密的密文结果?

答：n=55，则p、q分别为5和11， Ø(n)=（5-1）*（11-1）=40

又因ed=1mod Ø(n)，即3d= 1mod40，得d=27

加密$C=m^e \bmod 55=18^3 \bmod 55=2$

[问题4] (2分)对于RSA密码算法的公钥(55, 3),请给出对应私钥。

答：私钥d为27

[问题5] (2分)在RSA公钥算法中，公钥和私钥的关系是什么?

答：公钥和私钥满足：

ed=1mod Ø(n)

其中：可以由私钥推出公钥，由公钥无法推出私钥。

[问题6] (2分)在RSA密码中，消息m的取值有什么限制?

答： 消息m的长度小于密钥的长度

[问题7] (3分)是否可以直接使用RSA密码进行数字签名?如果可以，请给出消息m的数字签名的方法。如果不可以，请给出原因。

答案：不能用RSA密码直接对明文进行签名。

原因：1、直接对明文进行签名存在安全隐患。

[问题8] (3分)上述RSA签名体制可以实现[问题1]所述的哪3个安全基本目标?

答案： 保密性、完整性认证、不可否认性

为前程添彩！

我能过软考

3.4.3 数字签名

作品登记证书

登 记 号：黔作登字-2020-V-00113855

作品/制品名称：建群网培信息安全工程师系列视频教程　　作品类别：录像制品

作　　者：张建群[redacted]　　著作权人：[redacted]

创作完成日期：2017年05月28日　　首次发表/出版/制作日期：2017年12月07日

以上事项，由 张建群 申请，经 贵州省版权局 审核，根据《作品自愿登记试行办法》规定，予以登记。

登记日期：2020年08月20日　　登记机构签章

贵州省版权局 作品登记专用章

中华人民共和国国家版权局统一监制

严禁盗录、
非法下载、
非法盗版

强烈鄙视天博软考
盗版建群网培的信安课程，通过云盘发给学员

3.4.3 数字签名

- 数字签名 (Digital Signature)
  - 概述
    - 使用私钥对签名数据的杂凑值做密码运算所得的结果。
    - 用签名者公钥验证
    - 用于
      - 确认待签名数据的完整性
      - 签名者身份的真实性
      - 签名行为的抗抵赖性
  - 满足条件
    - 1 非否认
    - 2 真实性 — 能验证，且不能伪造
    - 3 可鉴别性 — 第三方鉴别
  - 组成
    - 签名算法 — 签名密钥秘密
    - 验证算法 — 验证密钥公开
  - 典型方案
    - RSA签名体制
    - Rabin签名体制
    - ElGamal签名体制
    - DSS标准 (Data Signature Standard)

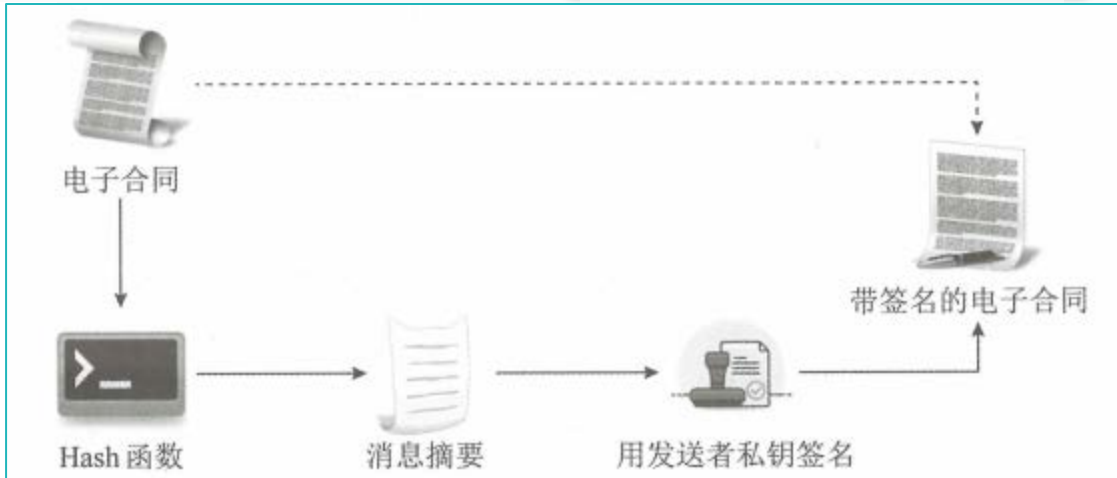


图 3-4　数字签名过程示意图

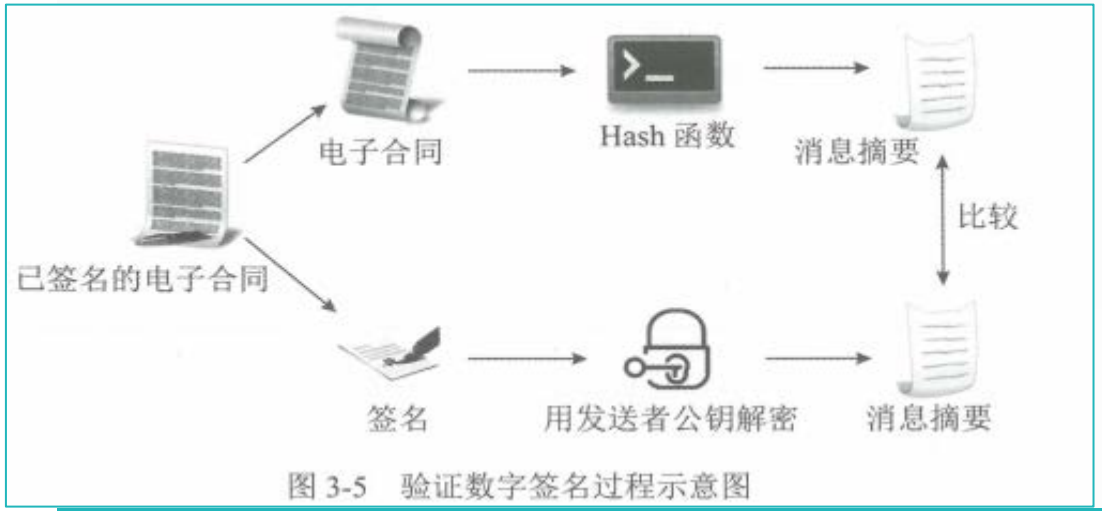


图 3-5　验证数字签名过程示意图

主要内容

- 数字签名的基本概念
- 数字签名与数据加密的区别
- 数据签名的基本模型
- 利用公钥密码实现数据签名
- 签名通信协议的问题
- 利用Hash函数辅助数据签名

1. 数字签名的基本概念

- 签名是证明当事者的**身份和数据真实性**的一种信息。
- 签名可以用不同的形式来表示：
  - 书面签名的形式:**手签、印章、手印**
  - 电子文件应采用**电子形式的签名，即数字签名**Digital Signature
- 数字签名主要建立在**密码的安全性**基础上。

- 完善的签名应满足以下三个条件
  - (1)签名者事后**不能抵赖**自己的签名
  - (2)任何其他人**不能伪造签名**
  - (3)如果当事的双方关于签名的真伪发生争执，能够在公正的仲裁者面前通过**验证签名来确认其真伪。**

1. 数字签名的基本概念-数字签名应具有的性质

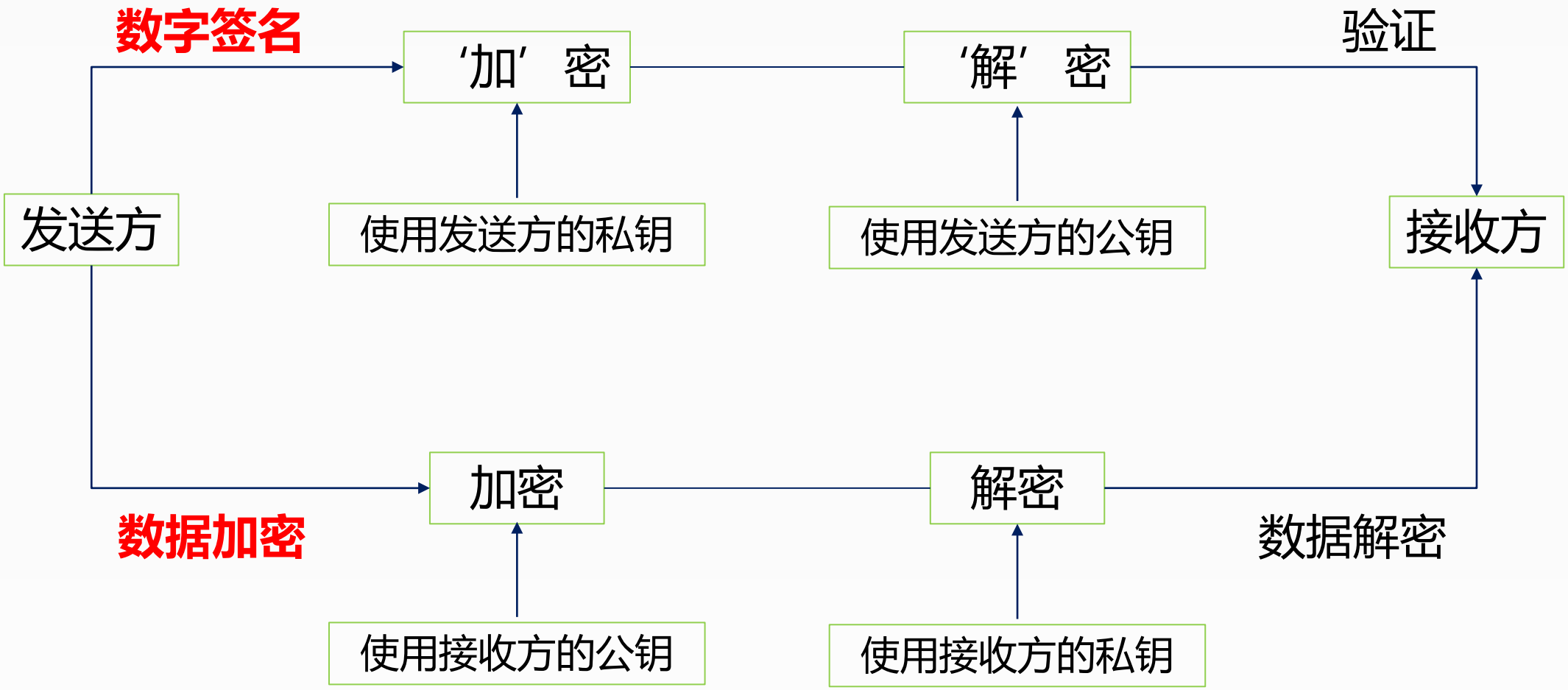
- 签名是对文档的一种映射，签名与文档具有一一对应关系（**精确性**）
- 签名应基于签名者的唯一性特征（如私钥），从而确定签名的不可伪造性和不可否认性（**唯一性**）
- 签名应该具有时间特征，防止签名的重复使用（**时效性**）

- 手写签名是模拟的，因人而异。
- 数字签名比手写签名有更强的不可否认和可认证性。

2. 数字签名与数据加密的区别

- 数字签名的加解密与数据加解密过程都可以使用公钥算法，但实现过程正好相反，使用的密钥对也不同。
- 数字签名使用发送方的密钥对，发送方利用自己的私钥进行加密（签名），接收方用发送方的公开密钥进行解密（验证）。
- 数字签名是一对多的关系，任何人都可以查找发送方公开密钥，以验证数字签名的正确性
- 数字签名大多采用非对称密钥加密算法，它能保证发送信息的完整性、身份的真实性和不可否认性。
- 数据加密采用了对称密钥和非对称密钥加密算法，能够保证发送信息的保密性。

2. 数字签名与数据加密的区别



3. 数字签名的基本模型

◆ 一个数字签名体制包括两个方面的处理：

- **施加签名**
- **验证签名**

- 施加签名：
  - 设施加签名的算法为SIG，产生签名的密钥为K，被签名的数据为M，产生的签名信息为S，则有：

$$S=SIG\ (M,\ K)$$

- 验证签名：
  - 设验证签名的算法为VER，用VER对签名S进行验证，可鉴别S的真假。即：

$$VER\ (S,\ K_{pu}) = \begin{cases} \text{真，} = M\text{，} \\ \text{假，} \neq M\text{，} \end{cases}$$

签名时M或M的$Hash$，会发送给接收方

3. 数字签名的基本模型

◆签名函数必须满足以下条件，否则文件内容及签名被篡改或冒充均无法发现：

➢1）当M’ ≠M时，有SIG（**M’**，K） ≠ SIG（**M**，K）

- 条件1）要求签名S至少和被签名的数据M一样长，当M较长时，应用很不方便，此时可以考虑对M进行分组，但可能产生碰撞；**Hash可以很好处理此问题**
- 将条件1）改为：虽然当M’ ≠M时，存在S=S’，但对于给定的M或S，要找出相应的**M’**在计算上是不可能的。

➢2） 签名S只能由签名者产生，否则别人便可伪造，于是签名者也就可以抵赖

➢3）收信者可以验证签名S的真伪。这使得当签名S为假时，收信者不致上当

➢4）签名者也应有办法鉴别收信者所出示的签名者签名是否是自己的签名，这就给签名者以自卫的能力

4. 利用公钥密码实现数字签名

1. 一般方法

对于一个公钥密码，如果满足：

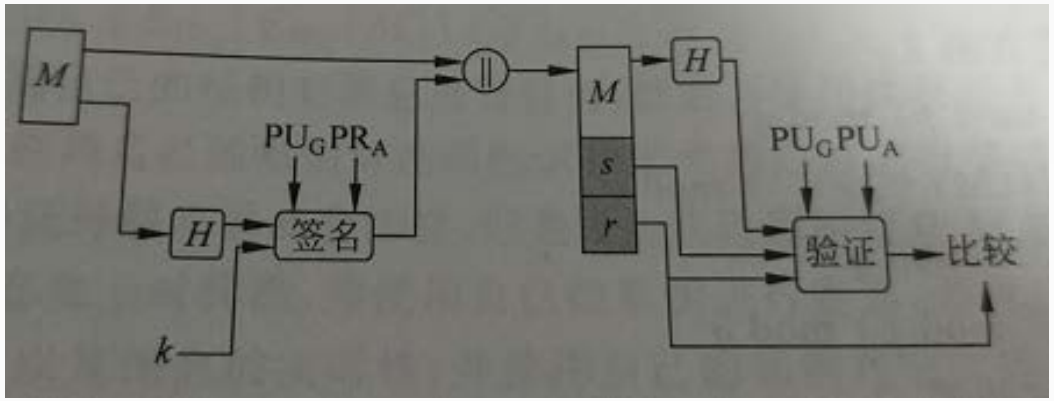
$E(D(M，K_d),K_e)=M,$

则可确保数据的真实性

- 凡是能够确保数据的真实性的公开密钥密码都可用来实现数字签名，例如RSA密码、ELGamal密码、椭圆曲线密码ECC、我国的SM2等都可以实现数字签名现数字签名。

数字签名标准DSS

- DSS采用了**SHA散列算法**，给出了一种新的数字签名方法，即数字签名算法DSA
- DSA本质上是基于Elgamal的签名算法
- ***DSA只提供数字签名，不可以用于加密或密钥分配。***



DSA算法的具体描述如下所示(如上图)。

- DSS方法便用Hash函数产生消息的散列值，和随机生成的k作为签名函数的输入，
- 签名函数依赖于发送方的私钥(PR_A)和组参数 ,这些参数为一组通信伙伴所共有，这组参数构成全局公钥PU_G。
- 签名由两部分组成，标记为r和s。
- 接收方对收到的消息计算散列值，和收到的签名(r,s)一起作为验证函数的输入，函数依赖于全局公钥和发送方公钥，若验证函数的输出等于签名中的r,则签名合法。

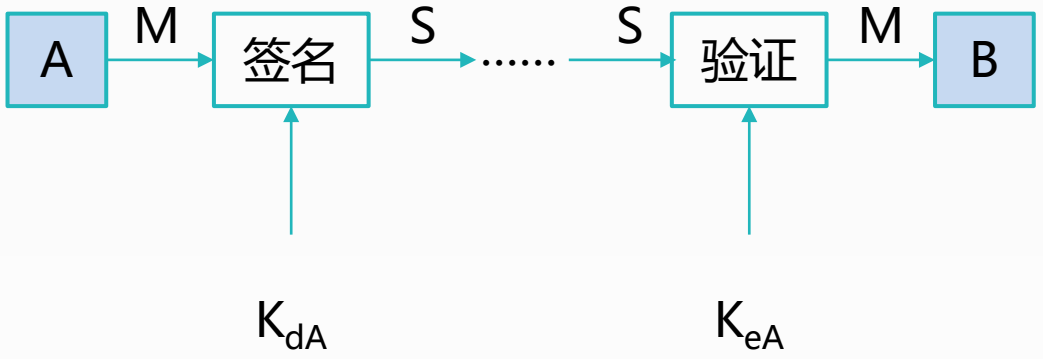
4. 利用公钥密码实现数据签名

签名通信协议：　A ⟶ B

1）A用自己的私钥K_{dA}对数据M进行签名

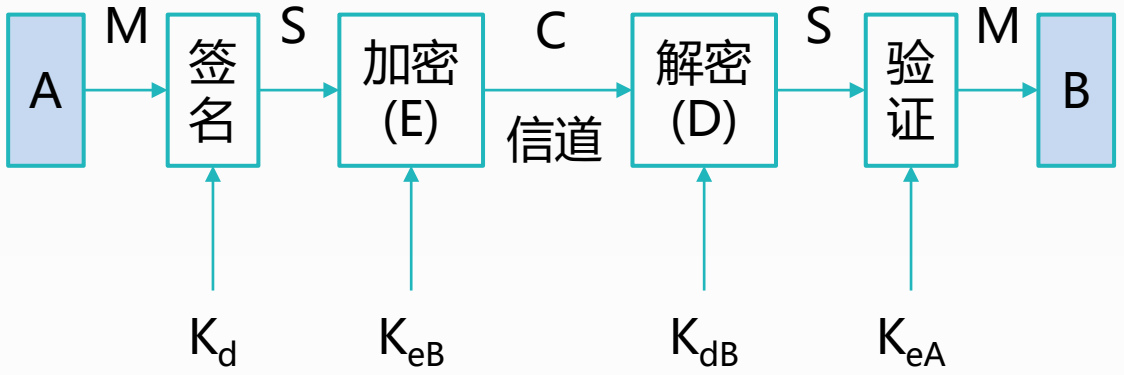
$S_A=D(M，\ K_{dA})$

2）如果不需要保密，则A直接将 S_A发给用户B



3）如果需要保密，则A查到B的公钥K_{eB}，并用K_{eB}对S_A再加密，得到密文C

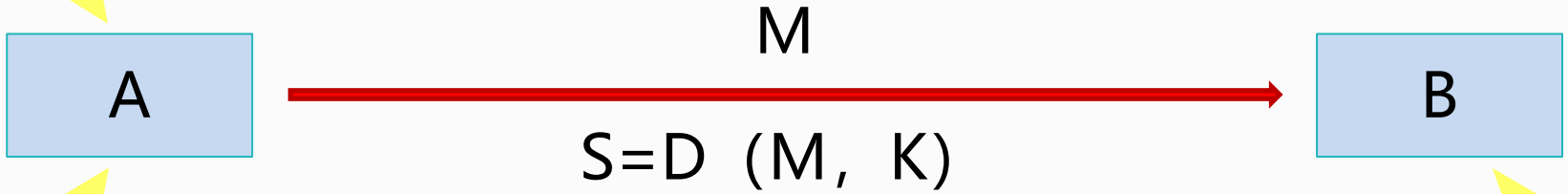
4）A把C发送B，并将S_A 或C留底



5. 签名通信协议的问题

M=“帮我买100股股票”

如果使用**对称算法**进行签名，即发送发和接收方共享密钥K



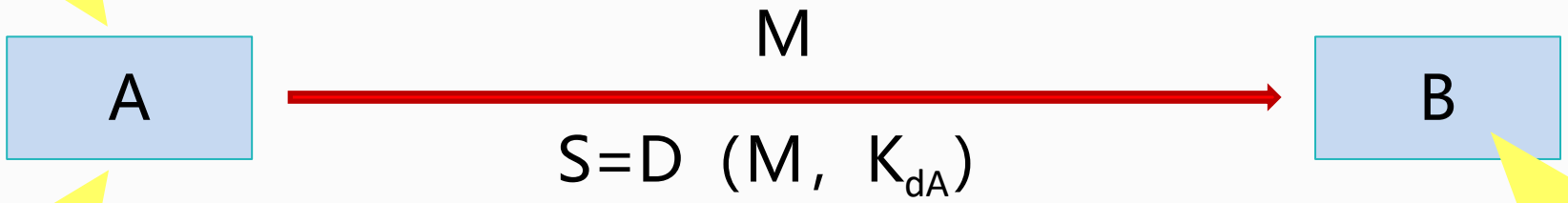
结果：股票暴跌，A想否认签名S，进而否认该笔交易

那么：B能没法证实A曾经下过订单，因为A和B都知道签名用的密钥。

5. 签名通信协议的问题

M= “帮我买100股股票”

如果使用公钥算法进行签名，即发送方**使用自己的私钥K_{dA}**



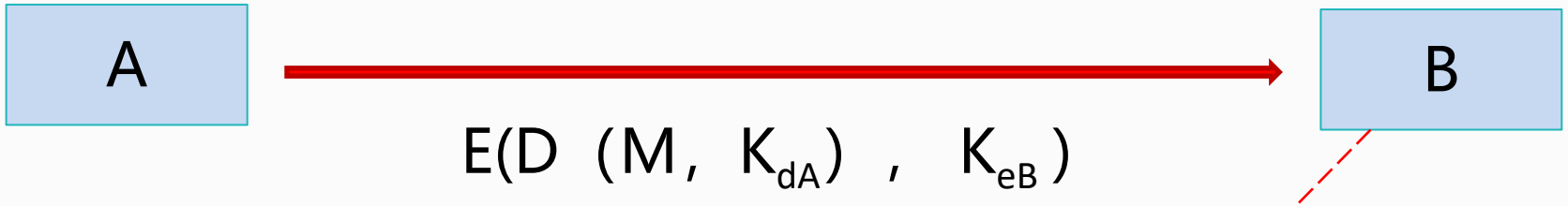
结果：股票暴跌，A想否认签名S，进而否认该笔交易

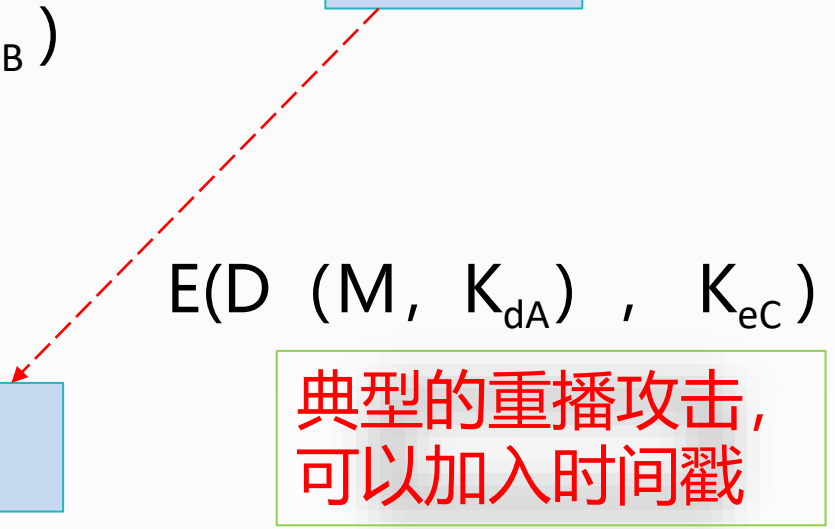
那么：B能否认证实A曾经下过订单呢?
B可以用A的公钥去验证A的签名。

5. 签名通信协议的问题

M= “我爱你....”

先签名再加密：使用公钥算法进行签名，即发送方使用自己的私钥K_{dA}，再用接收方的公钥K_{eB}进行加密



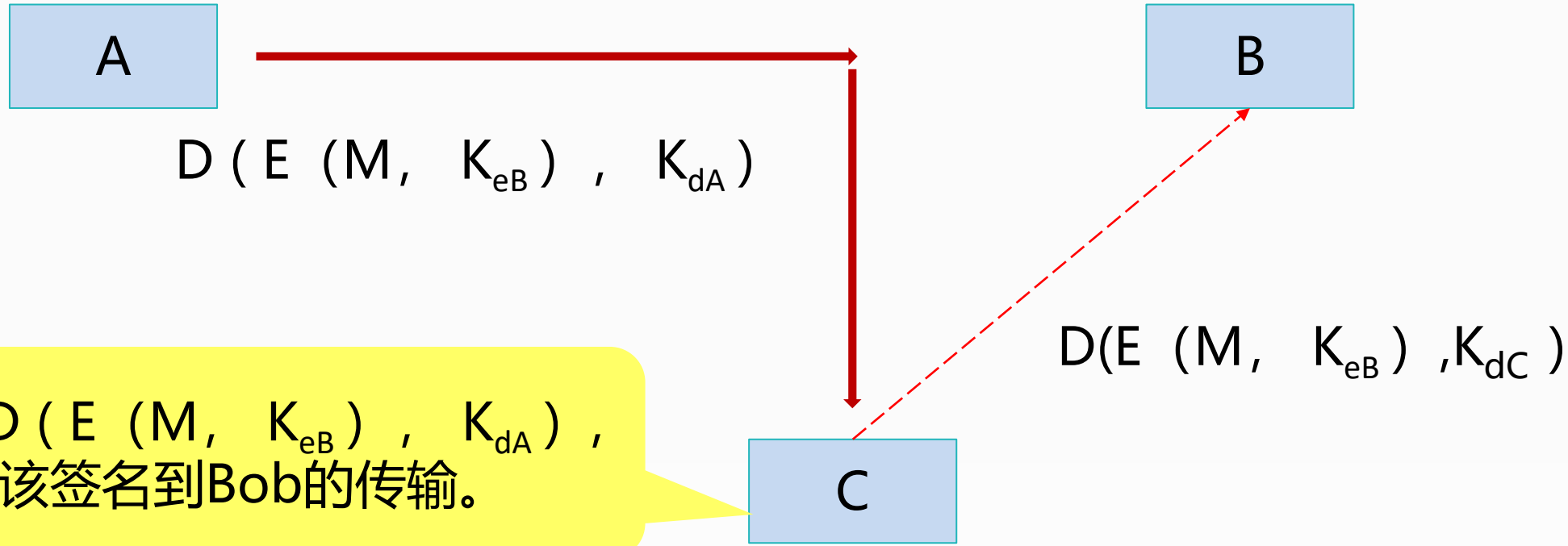


C认为是A说： “我爱你....”

5. 签名通信协议的问题

M= “我爱你....”

先加密再签名：使用接收方的公钥K_{eB}进行加密，再用公钥算法进行签名，即发送方使用自己的私钥K_{dA}



5. 签名通信协议的问题

- 1)验证签名的过程就是恢复明文的过程，而B事先并不知道明文M，否则就用不着通信了，那么B怎样判定恢复出的M是否正确呢

- 2)怎样阻止B或A用A以前发给B的签名数据，或用A发给其他人的签名数据来冒充当前A发给B的签名数据呢?

- **3)仅仅靠签名本身并不能解决这些问题。**

签名通信协议安全分析

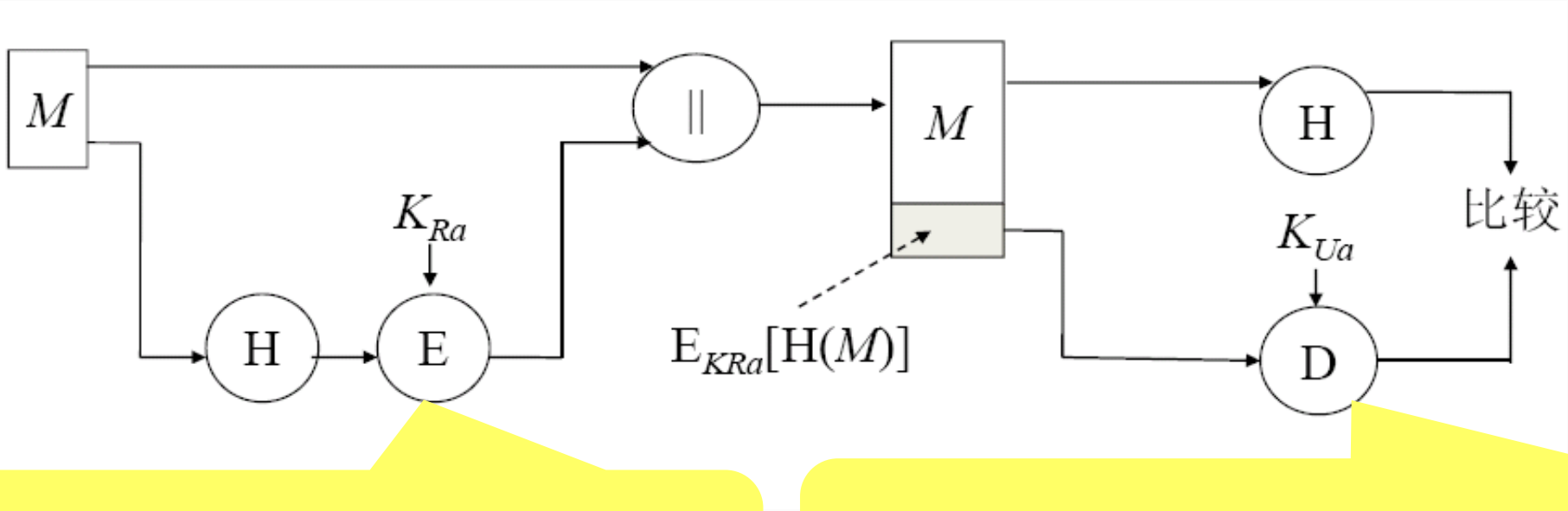
- 1)因为只有A才拥有K_{dA}，而且由公开的K_{eA}在计算上不能求出保密的解密密钥K_{dA}。因此，签名的操作只有A才能进行，任何其他人都不能伪造。所以K_{dA}就相当与A的印章或指纹，而SA就是A对M的签名。对此，A不能抵赖，任何人不能伪造。

- 2）事后如果A或B关于签名的真伪发生争执，则他们应向公正的仲裁者出示留底的签名数据，由仲裁者当众验证签名，解决纠纷。

6. 利用Hash函数辅助数字签名

发送方A

接收方B



发送方A：用A的私钥对Hash(M)进行签名

接收方B：用A的公钥验证签名，得到Hash(M)

小结

- 1. 数字签名的基本概念
- 2. 数字签名与数据加密的区别
- 3. 数据签名的基本模型
- 4. 利用公钥密码实现数据签名
- 5. 签名通信协议的问题
- 6. 利用Hash函数辅助数据签名


作品登记证书

登 记 号：黔作登字-2020-V-00113855

作品/制品名称：建群网培信息安全工程师系列视频教程　作品类别：录像制品

作　　者：张建群　著作权人：

创作完成日期：2017年05月28日　首次发表/出版/制作日期：2017年12月07日

以上事项，由 张建群 申请，经 贵州省版权局 审核，根据《作品自愿登记试行办法》规定，予以登记。

登记日期：2020年08月20日　登记机构签章

中华人民共和国国家版权局统一监制

谢谢！

我能过软考


作品登记证书

登 记 号：黔作登字-2020-V-00113855

作品/制品名称：建群网培信息安全工程师系列视频教程　作品类别：录像制品

作　　者：张建群　著作权人：

创作完成日期：2017年05月28日　首次发表/出版/制作日期：2017年12月07日

以上事项，由 张建群 申请，经 贵州省版权局 审核，根据《作品自愿登记试行办法》规定，予以登记。

登记日期：2020年08月20日　登记机构签章

中华人民共和国国家版权局统一监制