1.3 安全性、可靠性与系统性能评测基础知识

本节主要考点

1、对称加密技术
2、非对称加密技术
3、信息摘要
4、数字签名和数字加密
5、计算机可靠性

对称加密技术

- 对称加密技术：文件加密和解密使用相同的密钥，或者虽然不同，也可以从其中一个很容易地推导出另一个。

1101100010 → 1000110111 → 1101100010

明文　　密文　　明文

代表算法：

（1）DES：主要采用替换和移位的方法加密。它用56位密钥对64位二进制数据块进行加密。

（2）3DES：用两个56位的密钥。

（3）RC-5

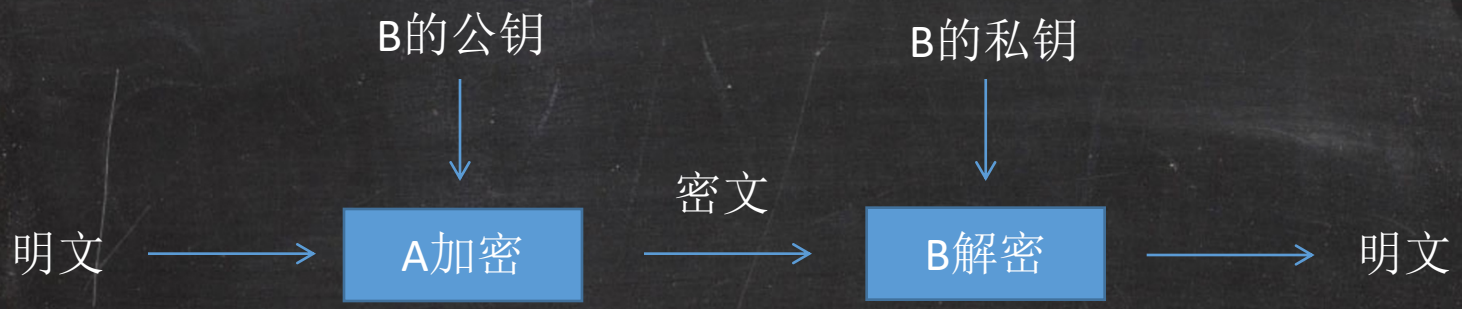
（4）IDEA：类似于DES，其密钥长度为128位。

（5）AES：基于排列和置换运算。

非对称加密技术

- 非对称加密技术：同样使用两个密钥：加密密钥和解密密钥，一个是公开的，一个是非公开的私有密钥。他们是一对，只有使用对应的密钥才能解密。
- 非对称加密有两个不同的体制：加密模型和认证模型。

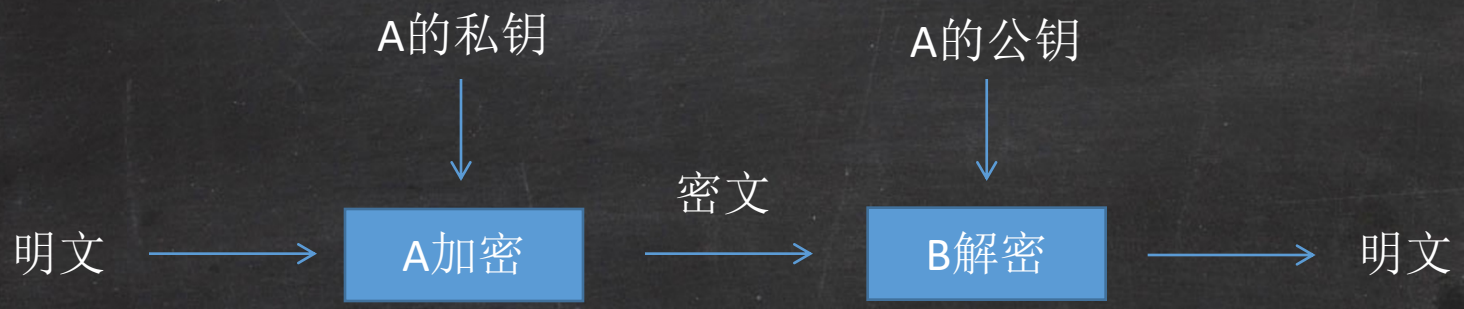
（1）加密模型：



A为发送者，B为接收者。

非对称加密技术

（2）认证模型：



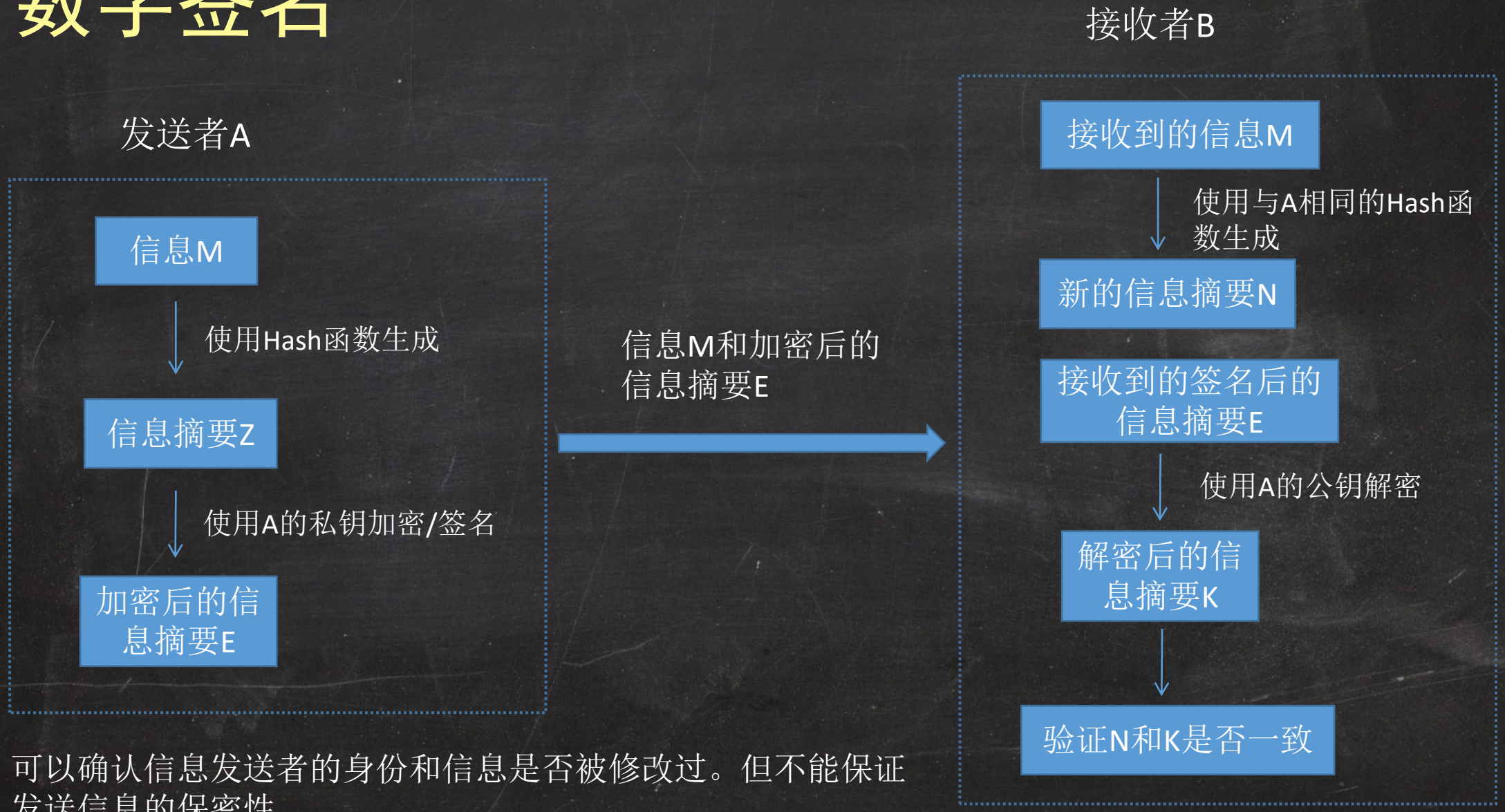
非对称加密算法的保密性较好，它消除了最终用户频繁交换密钥的需要，但加密和解密花费时间长、速度慢，不适合于对文件加密，而只适用于对少量数据加密。

代表算法：RSA，基于大素数分解的困难性。

信息摘要

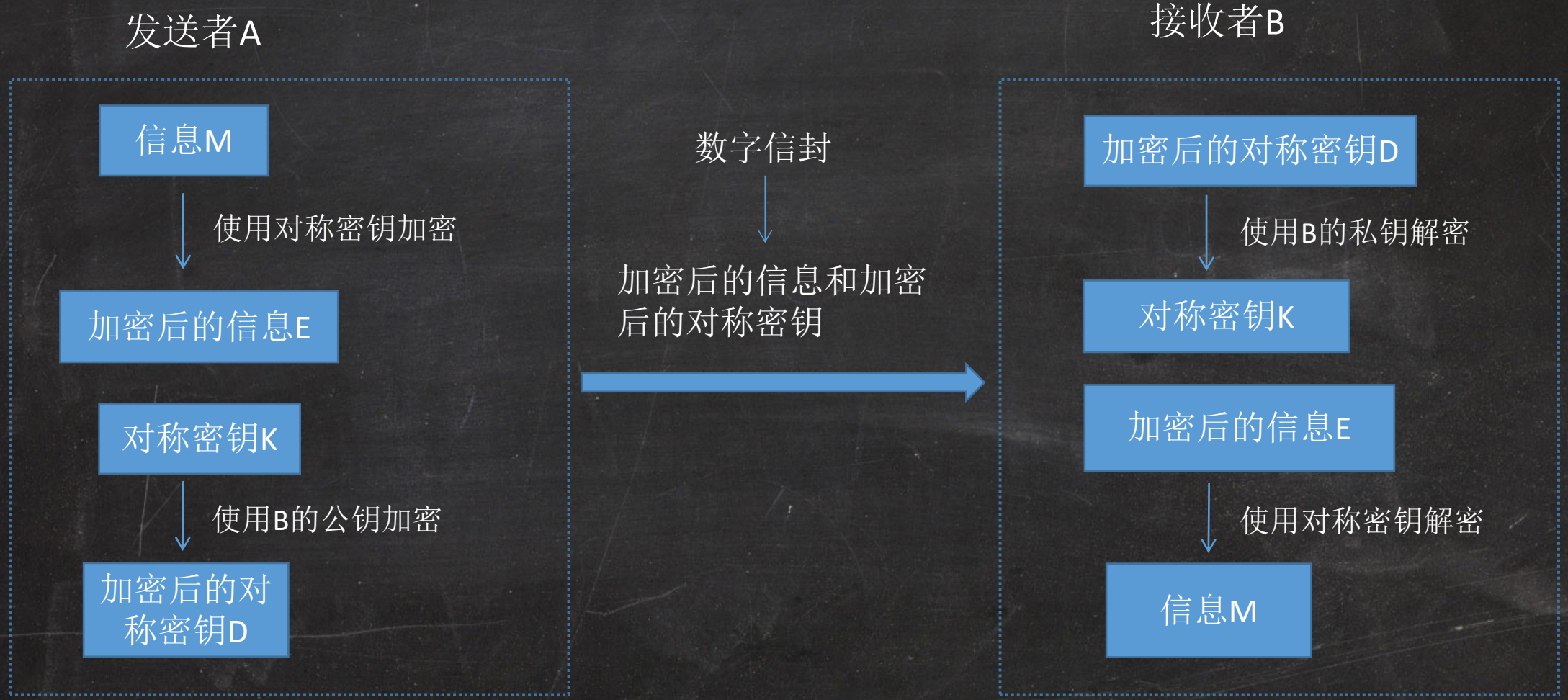
- Hash函数：输入一个长度不固定的字符串，返回一串固定长度的字符串，又称Hash值。
- 单向Hash函数用于产生信息摘要。
- 对于特定的文件而言，信息摘要是唯一的。
- 在某一特定的时间内，无法查找经Hash操作后生成特定Hash值的原报文，也无法查找两个经Hash操作后生成相同Hash值的不同报文。
- 在数字签名中，可以解决验证签名和用户身份验证、不可抵赖性的问题。
- MD2、MD4和MD5是被广泛使用的Hash函数，它们产生一种128位的信息摘要。

数字签名



可以确认信息发送者的身份和信息是否被修改过。但不能保证发送信息的保密性。

数字加密



可以保证发送信息的保密性，但是不能确认发送者的身份。

数字签名和数字加密的区别和联系

- 数字签名使用的是发送方的密钥对，任何拥有发送方公开密钥的人都可以验证数字签名的正确性。数字加密使用的是接收方的密钥对，是多对一的关系，任何知道接收方公开密钥的人都可以向接收方发送数据，但只有唯一拥有接收方私有密钥的人才能对信息解密。
- 数字签名只采用了非对称加密算法，它能保证发送信息的完整性、身份认证和不可否认性，但不能保证发送信息的保密性。
- 数字加密采用了对称密钥算法和非对称密钥算法相结合的方法，它能保证发送信息的保密性。

计算机可靠性

（1）计算机系统的可靠性：是指从它开始运行（t=0）到某时刻t这段时间内能正常运行的概率，用R(t)表示。

（2）计算机系统的失效率：是指单位时间内失效的元件数与元件总数的比例，用λ表示。

（3）平均无故障时间（MTBF）：两次故障之间能正常工作的时间的平均值称为

平均无故障时间MTBF=1/λ

（4）计算机系统的可维修性：一般平均修复时间（MTRF）表示，指从故障发生到机器修复平均所需的时间。

（5）计算机系统的可用性：指计算机的使用效率，它以系统在执行任务的任意时刻能正常工作的概率A表示。

A=MTBF/(MTBF+MTRF)

计算机可靠性

（1）串联系统的可靠性：

$$R=R_1 \times R_2 \times R_3 \times \cdots R_N$$

（2）并联系统的可靠性：

$$R=1-(1-R_1)(1-R_2)(1-R_3)\cdots(1-R_N)$$

1.3 安全性、可靠性与系统性能评测基础知识

【12年第7题】甲和乙要进行通信，甲对发送的消息附加了数字签名，乙收到该消息后利用（ ）验证该消息的真实性。

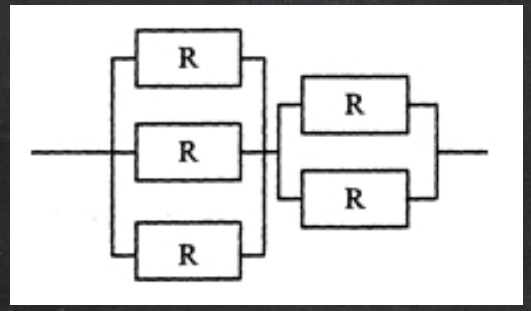
A.甲的公钥　　B.甲的私钥　　C.乙的公钥　　D.乙的私钥

【13年第7题】利用报文摘要算法生成报文摘要的目的是（ ）。

A. 验证通信对方的身份，防止假冒　　B. 对传输数据进行加密，防止数据被窃听

C. 防止发送方否认发送过的数据　　D. 防止发送的报文被篡改

【17年第4题】某系统由下图所示的冗余部件构成。若每个部件的千小时可靠度都为R，则该系统的千小时可靠度为（ ）。



A.$(1-R^3)(1-R^2)$　　B.$(1-(1-R)^3)(1-(1-R)^2)$

C.$(1-R^3)+(1-R^2)$　　D.$(1-(1-R)^3)+(1-(1-R)^2)$

【17年第8题】以下加密算法中适合对大量的明文消息进行加密传输的是（ ）。

A.RSA　　B.SHA-1　　C.MD5　　D.RC5

1.3 安全性、可靠性与系统性能评测基础知识

【17年第9题】假定用户A、B 分别从I1、I2两个CA取得了各自的证书，下面（　　）是A 、B 互信的必要条件。

A.A、B 互换私钥　　B.A、B 互换公钥
C.I1、I2互换私钥　　D.I1、I2互换公钥

【18年第11题】数字信封技术能够（　　）。

A. 保证数据在传输过程中的安全性　　B.隐藏发送者的真实身份
C. 对发送者和接收者的身份进行认证　　D.防止交易中的抵赖发生

【18年第12、13题】在安全通信中，S 将所发送的信息使用（　　）进行数字签名，T 收到该消息后可利用（　　）验证该消息的真实性。

A. S 的公钥　　B.S 的私钥　　C.T 的公钥　　D.T 的私钥
A. S 的公钥　　B.S 的私钥　　C.T 的公钥　　D.T 的私钥

【19年第4题】某系统由3个部件构成，每个部件的千小时可靠度都为R，该系统的千小时可靠度为$(1-(1-R)^2)R$，则该系统的构成方式是（　　）

A. 3个部件串联
B. 3个部件并联
C.前两个部件并联后与第三个部件串联
D. 第一个部件与后两个部件并联构成的子系统串联

1.3 安全性、可靠性与系统性能评测基础知识

【20年第12题】以下关于哈希函数的说法中，不正确的是（　）

A. 哈希表是根据键值直接访问的数据结构

B. 随机预言机是完美的哈希函数

C. 哈希函数具有单向性

D. 哈希函数把固定长度输入转换为变长输出

【22年第13题】

（　）属于公钥加密算法。

A.AES　　B.RSA　　C.MD5　　D.DES

【22年第14题】

确保计算机系统机密性的方法中不包括（　）。

A.加密　　B. 认证　　C. 授权　　D. 备份