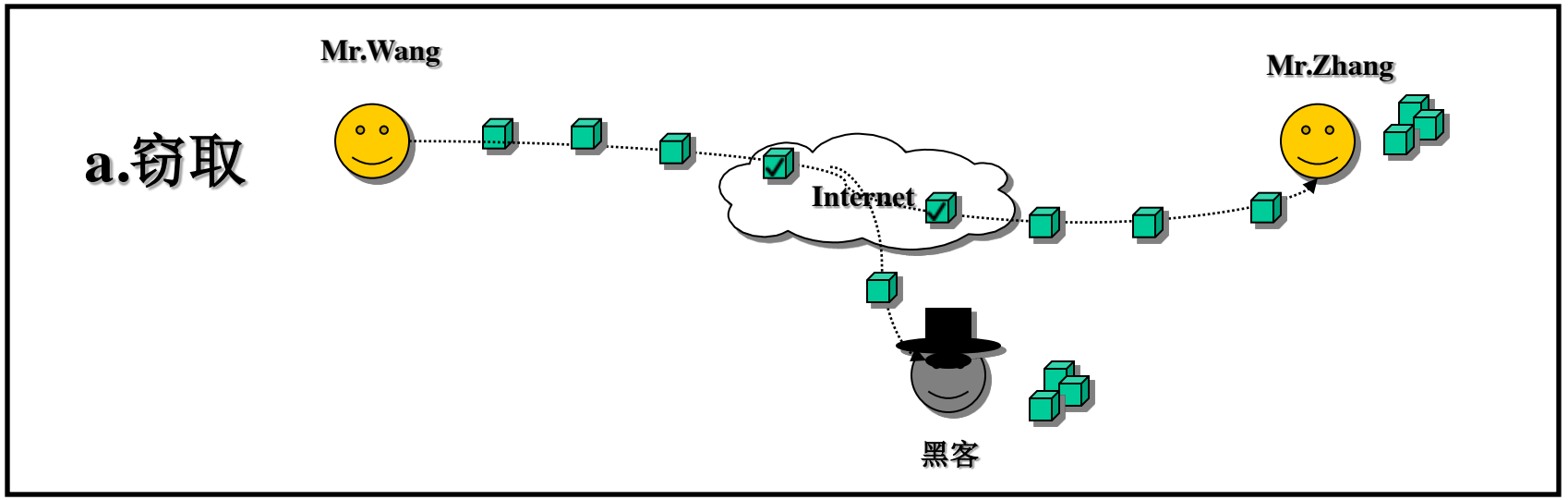
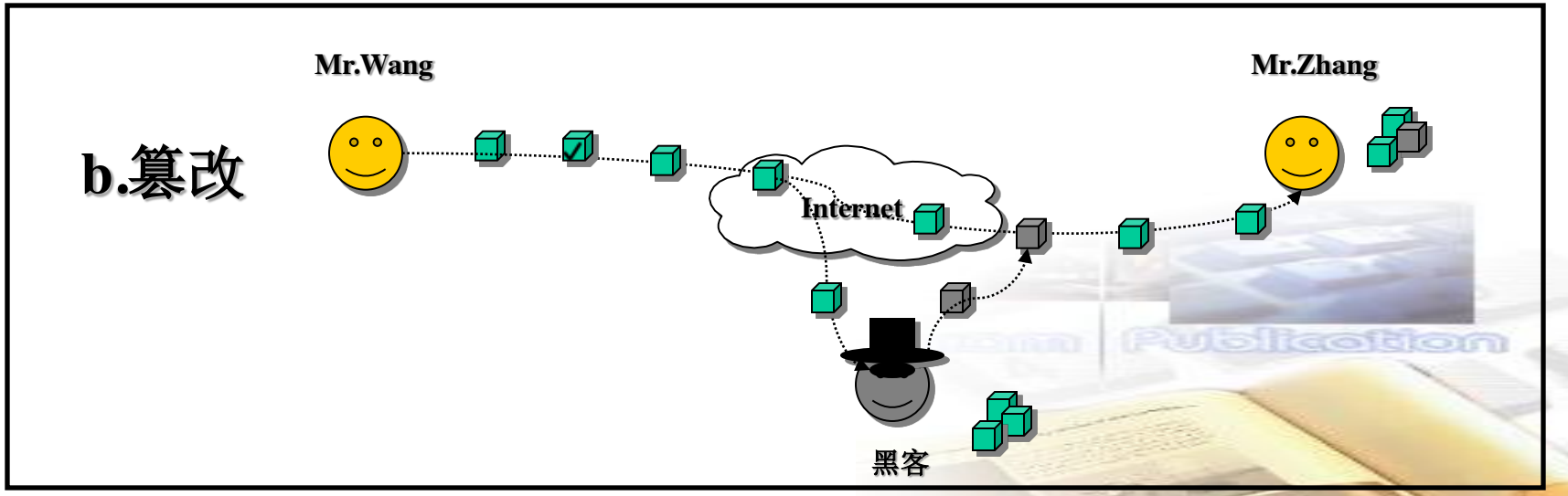
PKI基础

SUNING 苏宁

1、安全隐患--数据窃取和篡改

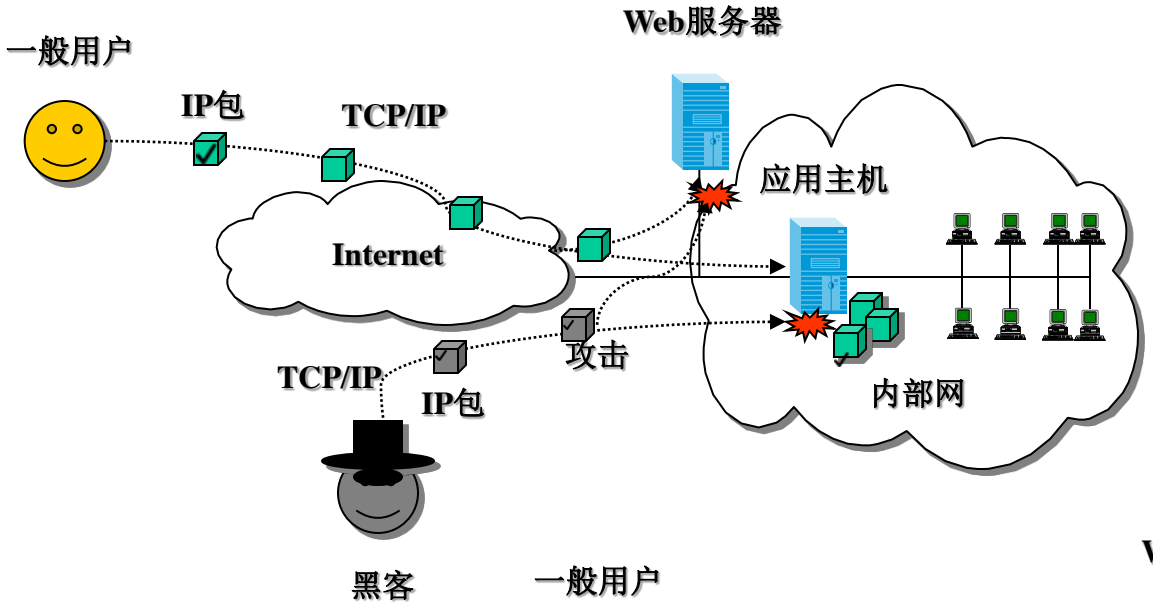


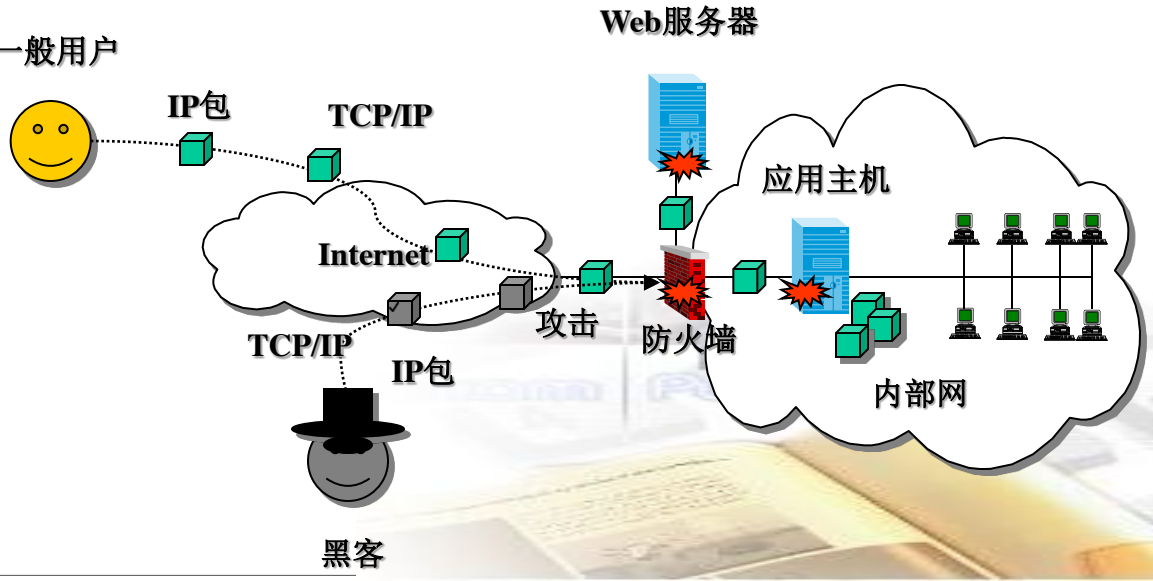


PKI基础

SUNING 苏宁

2、安全隐患--系统被攻击、侵占





PKI基础

PKI: Public key Infrastructure（公开密钥基础设施）

PKI是在公开密钥技术基础上发展起来的综合安全平台，它能够提供基于公开密钥的加解密、数字签名、身份认证等服务。

PKI为电子商务、电子政务等信息应用提供以下基本安全要求:

身份鉴别(Authentication): *在双方进行交易前，首先要能确认对方的身份,要求交易双方的身份不能被假冒或伪装。*

数据的机密性(Confidentiality):*对敏感信息进行加密，即使别人截获数据也无法得到其内容。*

数据的完整性(Integrity):*要求收方能够验证收到的信息是否完整,是否被人篡改，保障交易的严肃和公正。*

不可抵赖性(Non－Repudiation): *交易一旦达成，发送方不能否认他发送的信息，接收方则不能否认他所收到的信息。*

PKI基础-公钥密码学基础

1. 数据加密技术：

对称加密算法 (Symmetric encryption algorithm)

(Secret/Share key system)

非对称加密算法 (Asymmetric encryption algorithm)

(Public/Private key system)

2. 数据防篡改技术：

哈希算法 (Hash algorithm)

信息摘要算法 (Message Digest algorithm)

3. 数据签名技术：

Message Digest + Private Key Encryption=Digital signature

(Digital Fingerprint)

PKI基础-公钥密码学基础

1. Public/Private key system：

   RSA算法（模长为512、768、1024、2048比特）

   椭圆曲线密码算法 ,SM2

2. Secret key system：

   SSF33、DES、Triple-DES 、 SM1 、 SM4 、 RC4

   其中SSF33是国家密码管理办公室批准的常用对称加密算法

3. Hash or Message Digest

   MD2、MD5、SHA1 、 SHA256、 SM3

4. Digital Signature：

   DSA

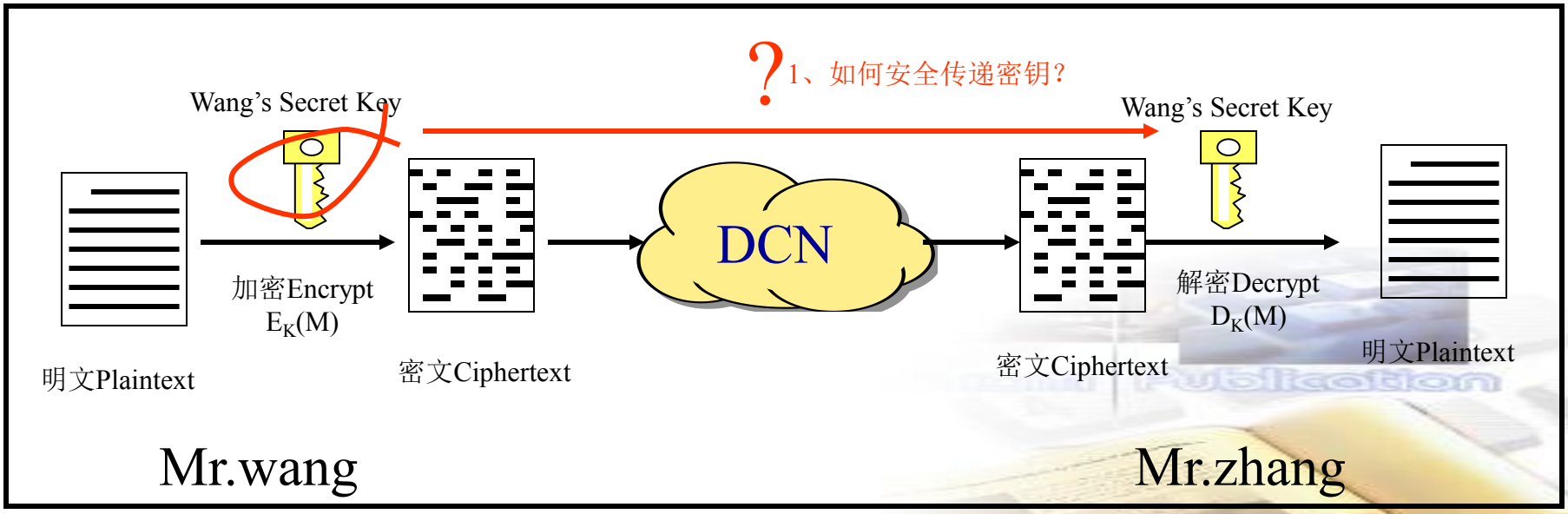
PKI基础-公钥密码学基础

1、Symmetric Algorithm

$E_k(M)=C$ $\quad$ $E(K,M)=C$

$D_k(C)=M$ $\quad$ $D(K,C)=M$

$D_k(E_k(M))=M$ $\quad$ $D(K,E(K,M))=M$



PKI基础-公钥密码学基础

算法类型和模式

对称密码算法有两种基本类型： 分组密码(Block cipher)
序列密码(Stream ciper)

密码模式有四种基本模式:

ECB(Electronic Code Book ——电子密码本模式)
CBC(Cipher Block Chaining ——密码分组链接模式)
CFB(Cipher Feed Back —— 密码反馈模式）
OFB(Output Feed Back —— 输出反馈模式）

PKI基础-公钥密码学基础

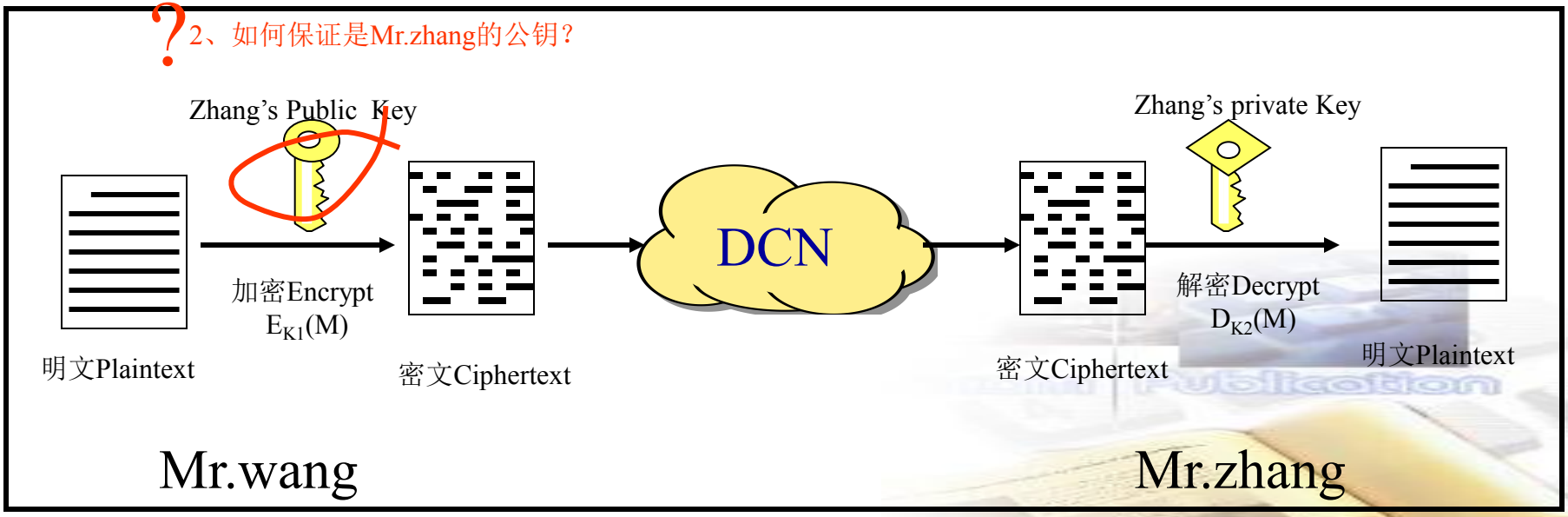
2、Asymmetric Algorithm

$E_{k1}(M)=C$
$D_{k2}(C)=M$

$E(K1,M)=C$
$D(K2,C)=M$

$D_{k2}(E_{k1}(M))=M$

$D(K1,E(K2,M))=M$



PKI基础-公钥密码学基础

RSA算法

公开密钥	(n,e)
n=pq	两素数p和q的乘积,p和q必须保密,且为大素数
gcd(e,(p-1)(q-1))=1	e<n,并与（p-1）(q-1)的乘积互素
私人密钥	(n,d)
$d=e^{-1} \bmod ((p-1)(q-1))$	ed-1 是(p-1)(q-1)的倍数
加密	$c=m^e \bmod n$
解密	$m=c^d \bmod n$

```
While (x>0) {
   g=x;
   x=y%x;
   y=g;
}
```

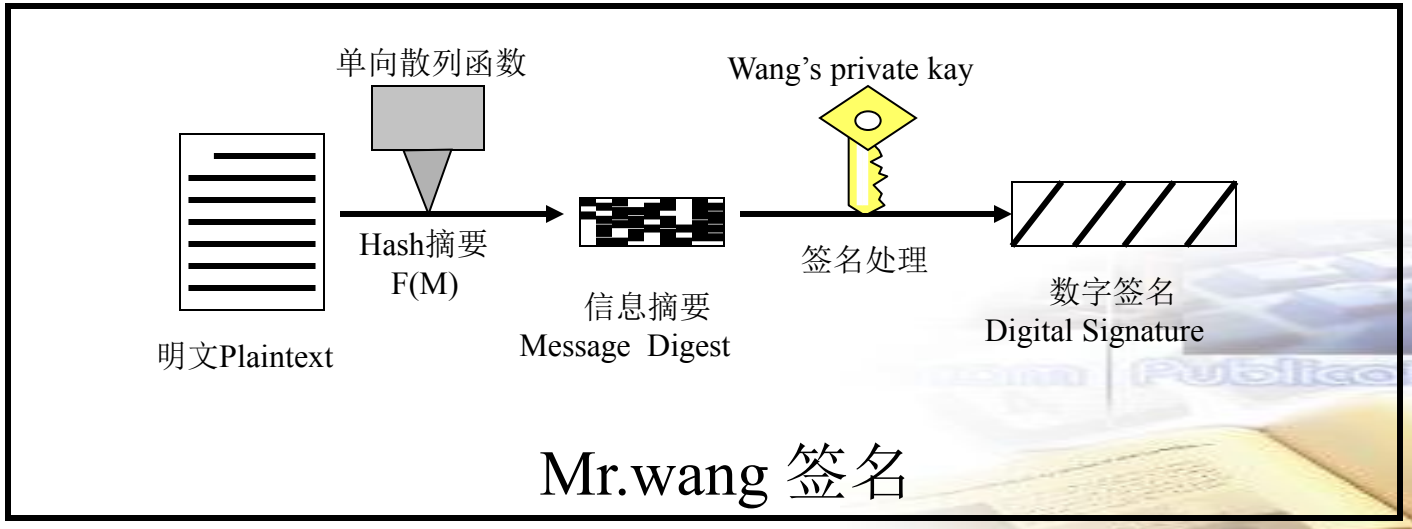
- P=3, q=5; n=15
- Choose e=3, e<n; and is prime to (p-1) (q-1)=8
- Choose d=11 so that (ed-1)=32 is divisible by (p-1) (q-1)=8.
- Public key (n,e)=(15,3); Private key (n,d)=(15,11)
- Cncyption Process
- —Original message m=2　cipher message c=m**e mod n=8
- Decryption Process
- —Cipher message c=2　Decrypted message m=c**d mod n=2

PKI基础-公钥密码学基础

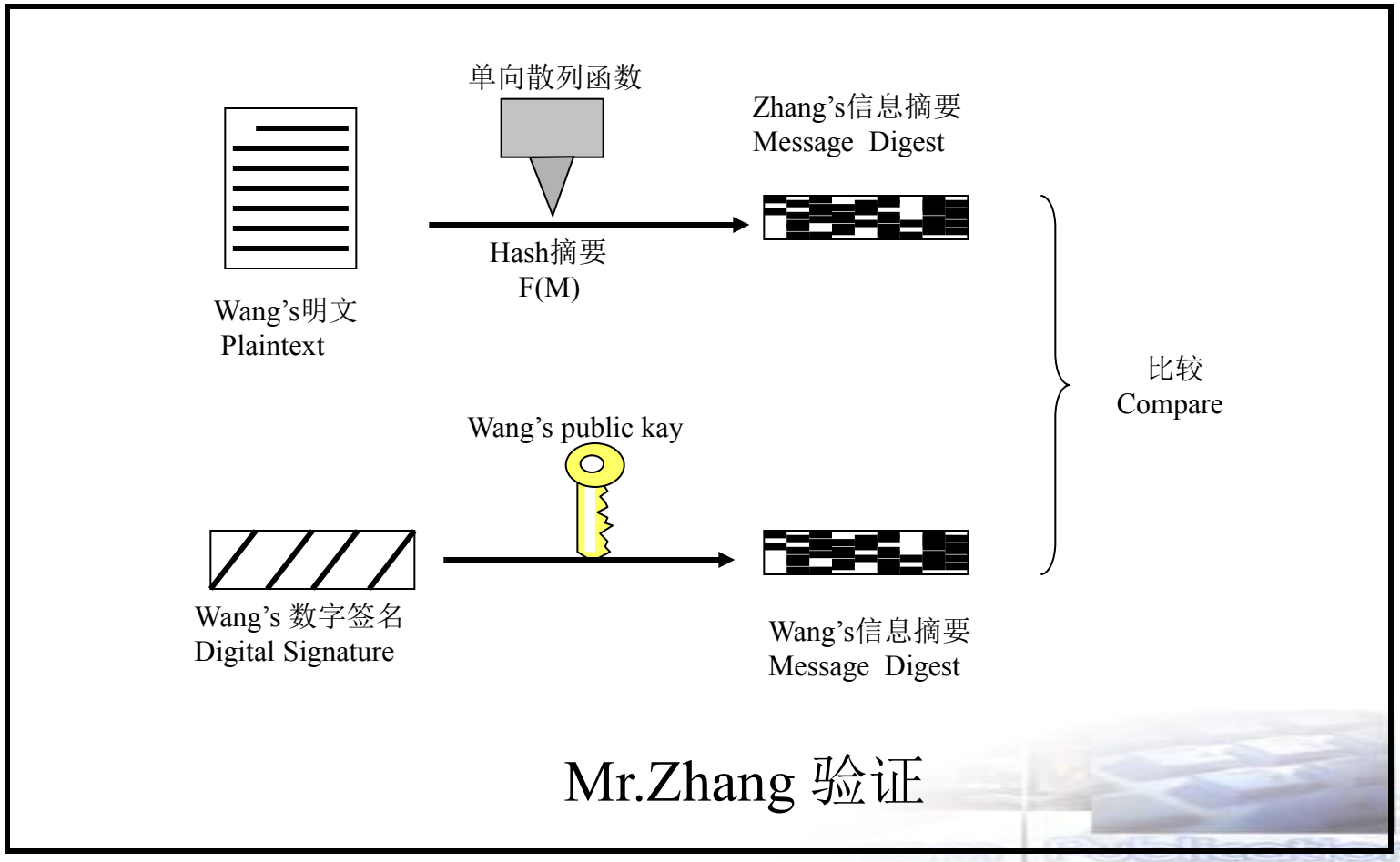
3、Message Digest/Digital Signature/Time Stamper

$F(M)=D$ $E_{pvk}(D)=S$

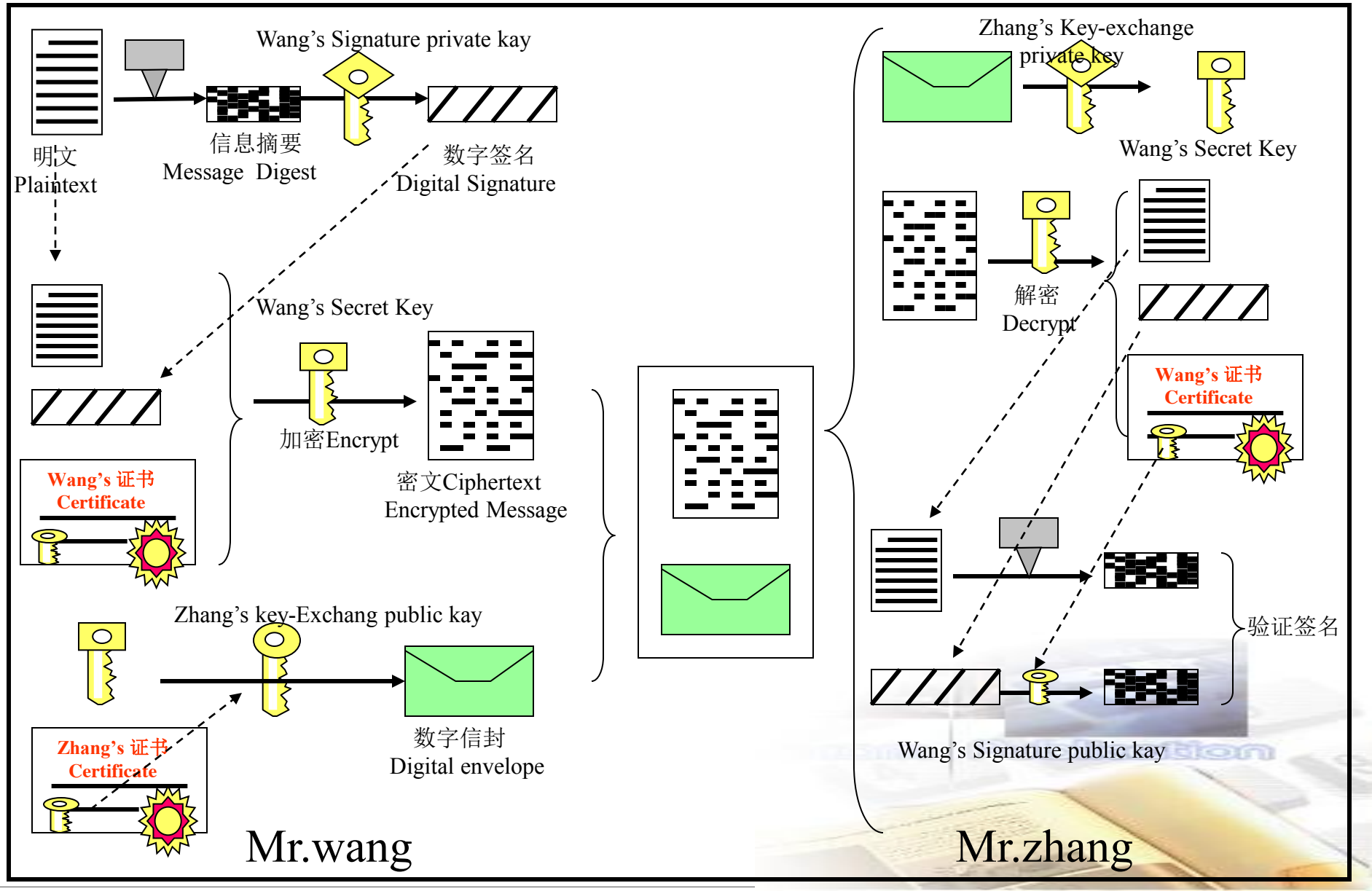
- 数字签名Digital Signature : 保证数据完整性、防篡改、以及不可抵赖性。
- 单向散列函数(One-way Hash Fuction) ： 已知 x,很容易计算F(x),但已知 F(x),却很难计算出x。
- “难”的定义：即使世界上所有的机器都来计算，也要花费数百万年的时间。
- 时间戳Time Stamper的关键是要产生可信任的时间源。



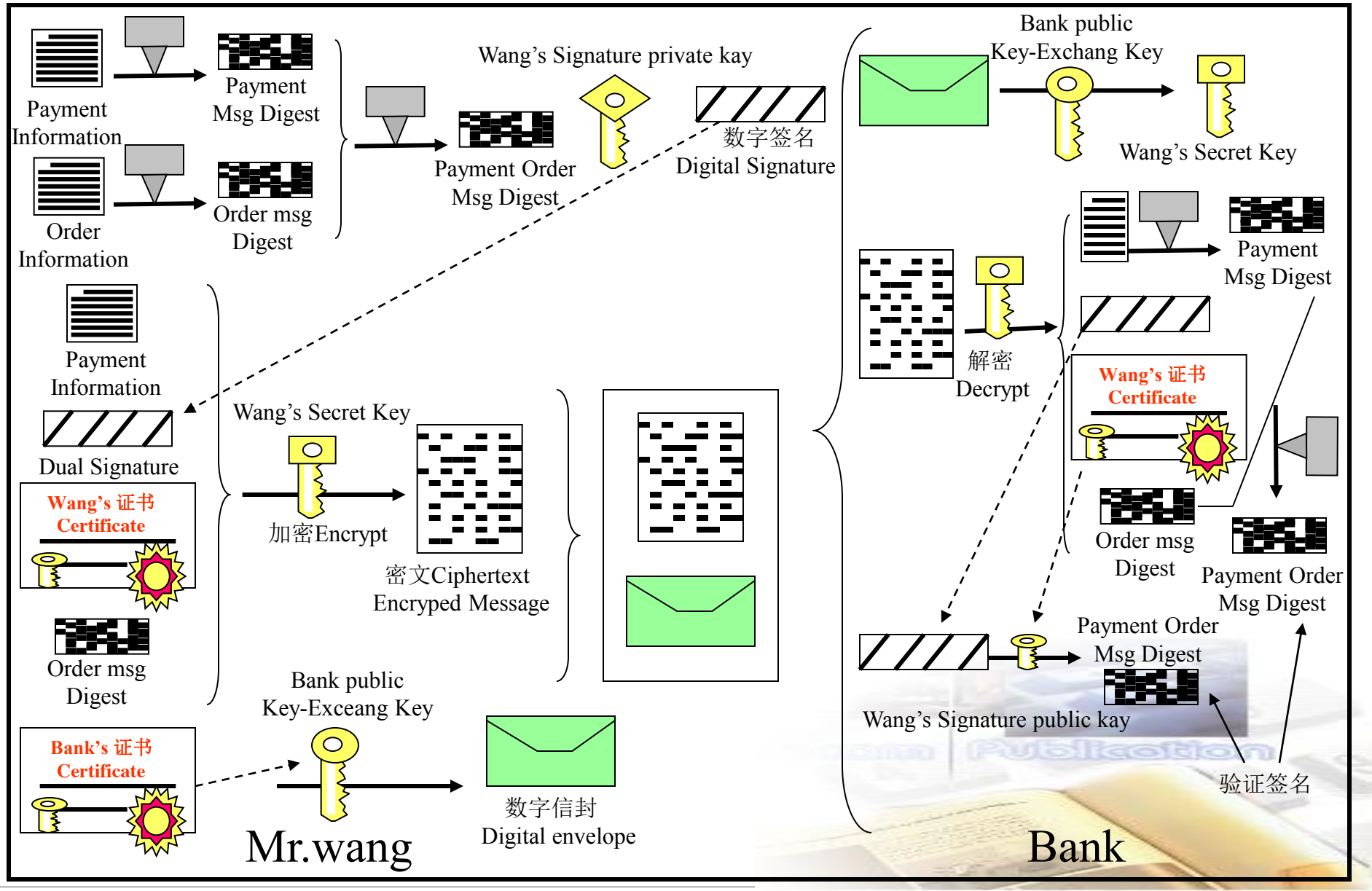
PKI基础-公钥密码学基础



严密的PKI数据加解密、数字签名与验证流程

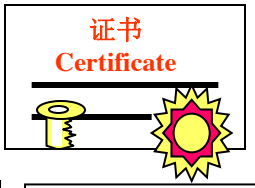


双重签名 Dual Signature



PKI基础

SUNING 苏宁

数字证书  的内容与格式： X.509 V3

基本项	可选项(Optional)	扩展项（Extend）
版本号 序列号 签名算法 发行机构 有效期（包括签发日期和作废日期） 姓名 公钥	发证机构ID号 用户身份证ID	扩展序号 密钥用法 黑名单库 用户地址 用户电话 证书级别

- 版本号
- 证书序列号
- 证书拥有者DN
- 算法标识
- 颁发者DN
- 有效期
- Hash函数标识
- 拥有者公钥
- 密钥用途
- 证书政策
- CRL 发布点
- CA签名
- 颁发者公钥
- ……

- 信任地表明身份和鉴别身份；
- 提供加密工具信任载体；
- 提供数字签名信任载体；

PKI基础

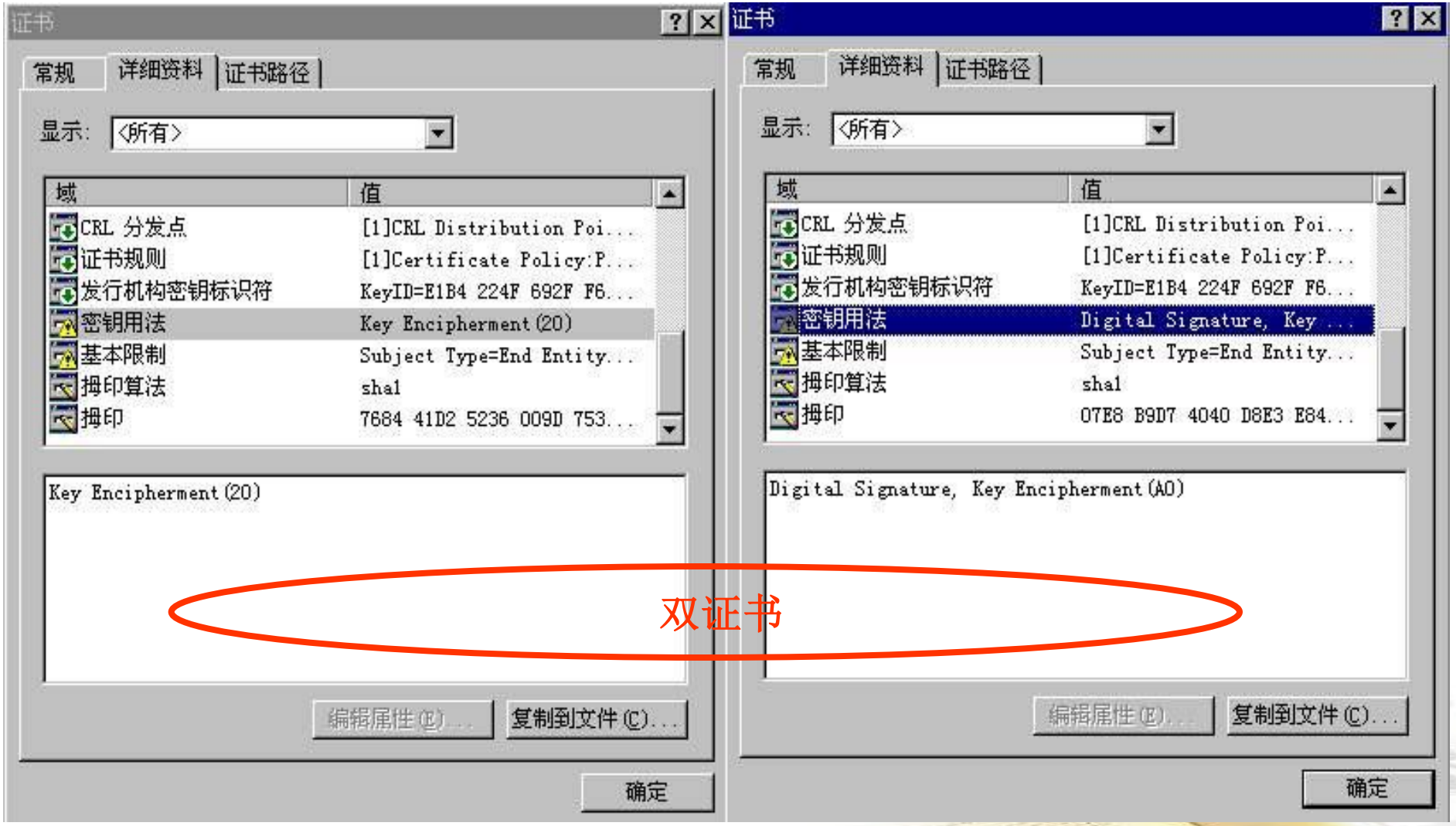
SUNING 苏宁

PKI基础


证书
常规
详细资料
证书路径
证书路径
ShenZhen EC Centre
steven
证书状态:
该证书是正确的。
证书
常规
详细资料
证书路径
证书信息
这个证书的目的是:
•Windows 系统组件验证
•Windows 硬件驱动程序验证
•允许加密磁盘上的数据
•允许 Internet 上的安全通讯
•允许您用数字签名证书委托列表
* 有关细节，请参考证书颁发者的说明。
颁发给: ShenZhen EC Centre
颁发者: ShenZhen EC Centre
有效期自 00-1-2 到 05-1-1
颁发者说明...
确定

PKI基础

SUNING 苏宁



PKI基础

SUNING 苏宁

双证书：

- 当签名私钥丢失后，虽然可注销证书，防止身份冒充，但无法解读原加密数据。
- 当签名私钥被集中托管时，其身份鉴别无权威性，不可抵赖性无法保证。

双证书：用户拥有两个证书：

一个是签名证书，一个是加密证书。

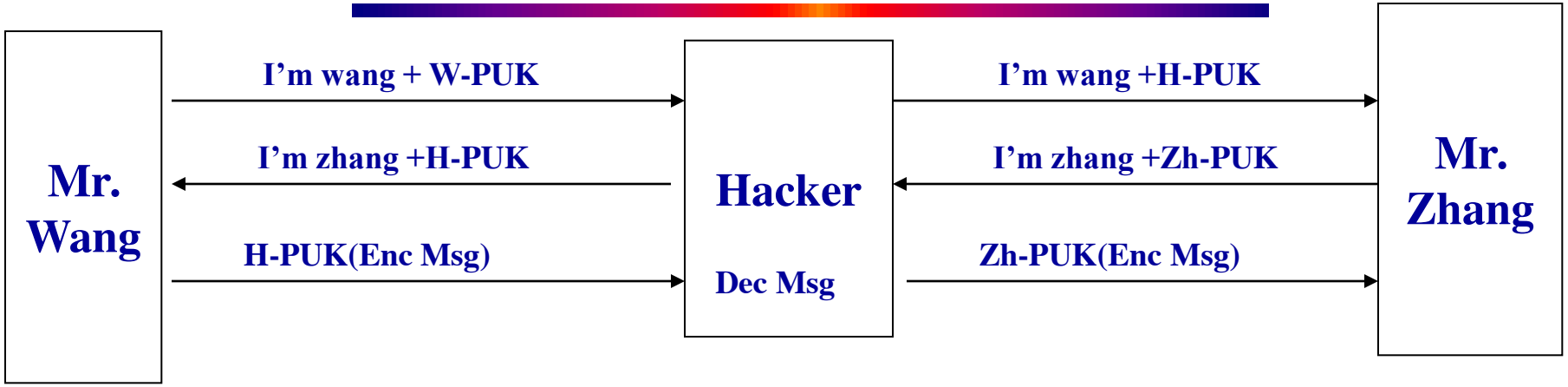
用户拥有两对密钥对：

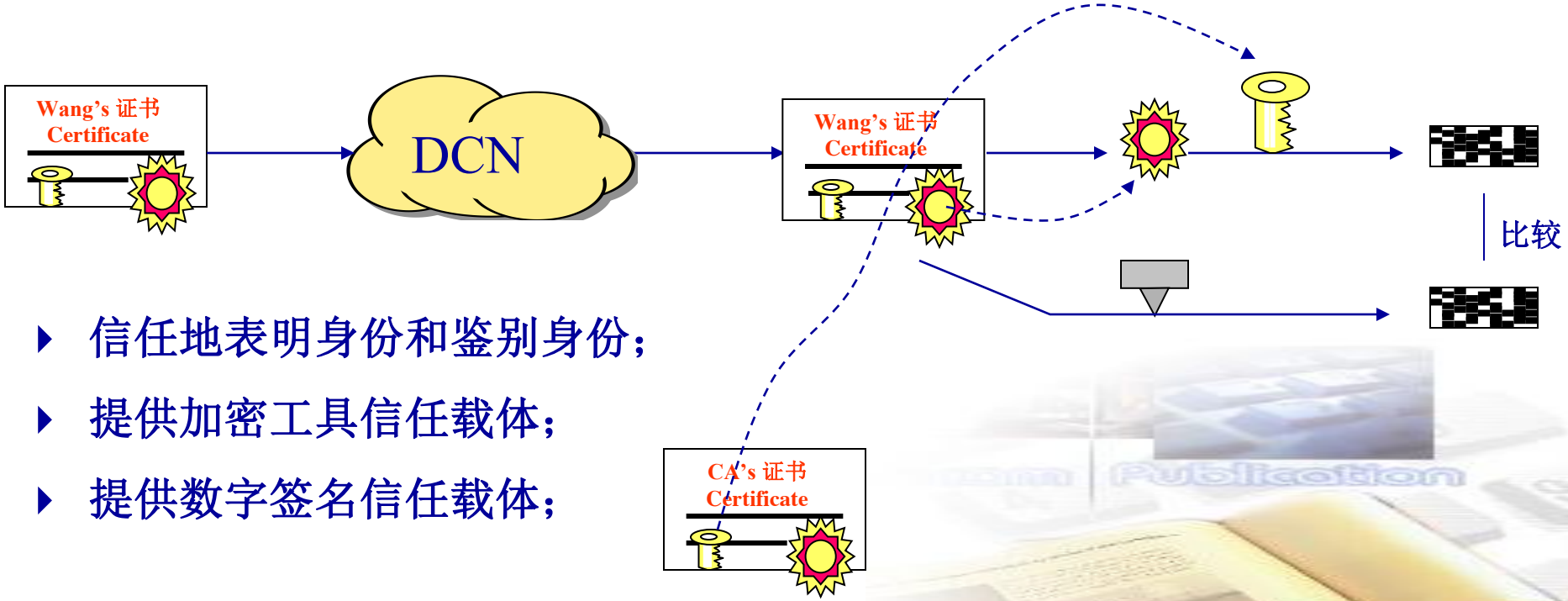
一对是签名密钥对，一对是加解密密钥对。

签名私钥个人保管，

解密私钥CA备份托管。

PKI基础





- 信任地表明身份和鉴别身份；
- 提供加密工具信任载体；
- 提供数字签名信任载体；

PKCS 标准（一）

PKCS1 公开密钥算法加密和签名机制

补位规则 例子，1024bit 00 + 01|02 + PAD + 00 + DATA

同样的数据，同一个公钥，生成的密文是否相同？

PKCS2

PKCS3 定义 Diffie-Hellman密钥交换协议 TLS/SSL https

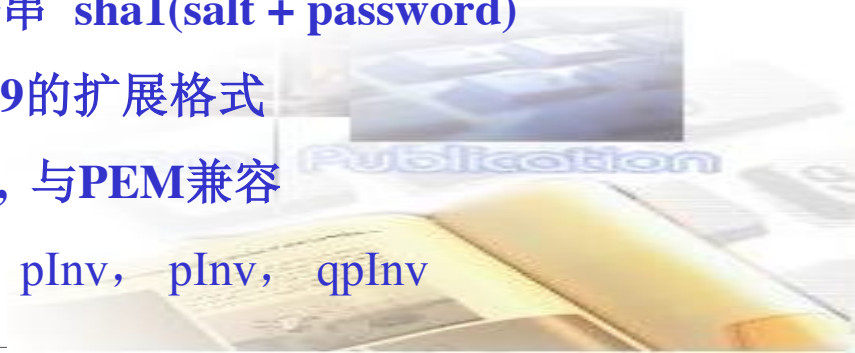
PKCS4

PKCS5 从口令派生出来的安全密钥加密字符串 sha1(salt + password)

PKCS6 公钥证书的标准语法，主要描述X.509的扩展格式

PKCS7 数据标准 Data，Digest，SignData ，与PEM兼容

PKCS8 私有密钥信息格式 n，e，d， p，q， pInv， pInv， qpInv



PKCS 标准（二）

PKCS9　属性证书

PKCS10　证书请求语法

PKCS11　一套接口　类似 微软 CSP+CERTMGR，　CFCA SCSP

PKCS12　个人信息交换　　.p12，　　.pfx

PKCS13　椭圆曲线密码 体制标准

PKCS14　伪随机数

PKCS15　密码令牌

编码标准及工具源码

- ASN1 DER 是密码，数字证书方面最重要基础。

  我能见到的格式文件 .cer .der， p7。

  对于公钥，私钥，证书请求， 数字证书，以及PKCS标准多使用这个编码标准进行描述。

- BASE64

  我能见到的格式文件 .pem

- 非常好用的工具

  OpenSSL Crypto

- 各位如有需要，我这里有SM2，SM3，SM4源代码，C版和Java版。

CFCA

设计手机端私钥保护方案

1 软私钥， 软证书=（证书+私钥）

2 客户端对证书加密，其实是对私钥加密，防止CA证书链替换

3 证书请求和下载

4 数字签名

5 查验证书　证书没有被篡改（验证书链），没有过期，没有吊销（苏宁自建SDC，信息安全标准OCSP，信息安全标准CRL）

6 验证签名数据。

实践

设计手机端私钥保护方案

【支付密码加密私钥，不能解开时用备用数据解开私钥再用支付密码加密】

1 目标保护客户端私钥(如何保护？加密！，使用什么算法)

PVK私钥，K1 支付密码，K2 备用密码，服务密钥SK，密钥导出函数DFK

存放客户端加密私钥 EK1 = f(DFK(K1),PVK)

存放客户端加密私钥 EK2 = f(DFK(K2),PVK)

存放服务端 K1变更校验码 VK = MAC(SK,DFK(K1))

校验 客户端发送 VD = DFK(K1)， 服务端验证 VK ?= MAC(SK,VD)

2 客户端发送DFK(K1),服务端校验VD，如校验成功，K1打开PVK。

3 校验不成功，采用手机短信保护，将K2发送给客户端，用K2打开PVK，同时用K1加密PVK，替换EK1，然后进入步骤2.

问答列表

1 PBE的原理怎么样的？为什么会有PBE？

2 密钥相同，明文相同，密文 就一样了吗？（密钥相同，密文不同，解密后的明文有可能相同吗）

3 一次一密和一次两密的应用？

问答环节

1 PBE的原理怎么样的？为什么会有PBE？

SK = KDF(password, salt)　　MD5/SHA1/…　　128bit, 256bit

C = E(SK, data)

Why　SK = MD(password) ？　C=(MD(password),data)

（26+26+10）^6 = 62^6　约 2^36 约 64*(10^3)^3=640亿

假如 1ms完成一次解密，6400万秒即 1.8万小时，750天。

增加破解时间？理论上可行，时间上不可行.

选择适当的 salt，

问答环节

2 密钥相同，明文相同，密文 就一样了吗？（密钥相同，密文不同，解密后的明文有可能相同吗）

对称　　data+||+random

ECB　　data<16　　abc00000x13　　16字节

非对称

1024bit　　00 + 01|02 + PAD + 00 + DATA

加密　02..17

问答环节

3 一次一密和一次两密的应用？

客户端 eke = E(pubkey, sk), cipher1= E(sk, request)

服务端 sk = D(pvkkey, eke), request = D(sk, cipher1)

cipher2 = E(sk, response)

客户端 respone = D(sk, cipher2)

几乎全内存操作

谢谢各位！

上研中心　　朱成敏