为前程添彩！

我能过软考

第3章 密码学基本理论3
(密码管理、安全协议、应用场景)

建群网培

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

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

手淘扫一扫

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

- 3.5.1 密码管理
- 3.5.2 数字证书

02

- 3.6.1 Diffie-Hellman 密钥交换协议

03

- 3.6.2 SSH

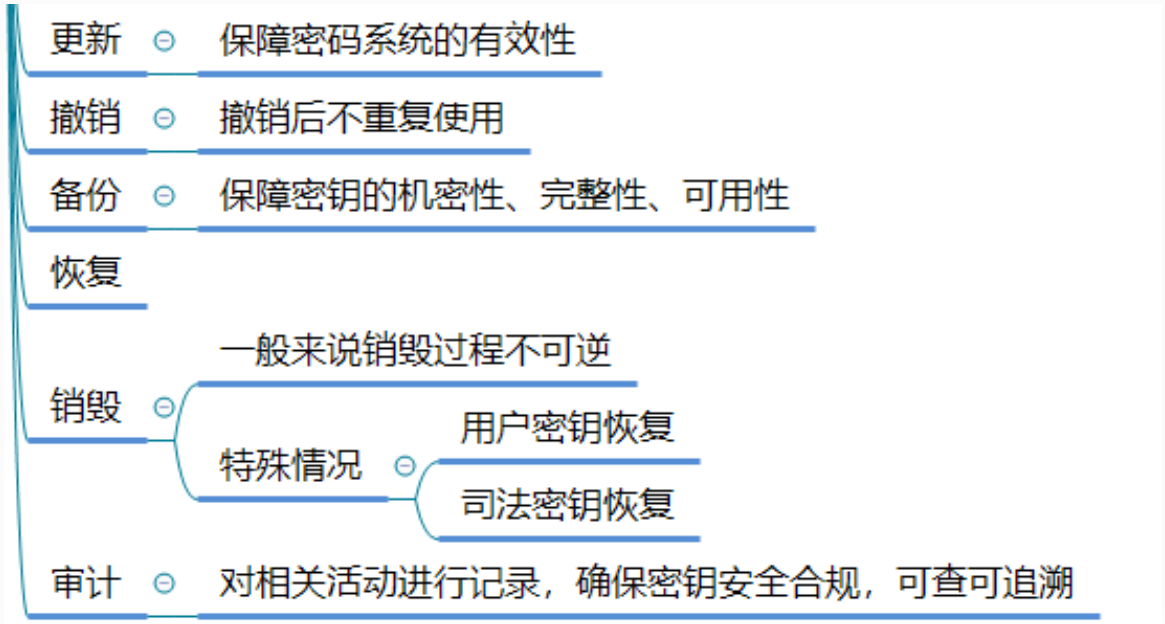
04

- 3.7 密码学网络安全应用

3.5.1 密码管理

版权所有：我能过软考

密码管理包括：密钥管理、密码管理政策、密码测评

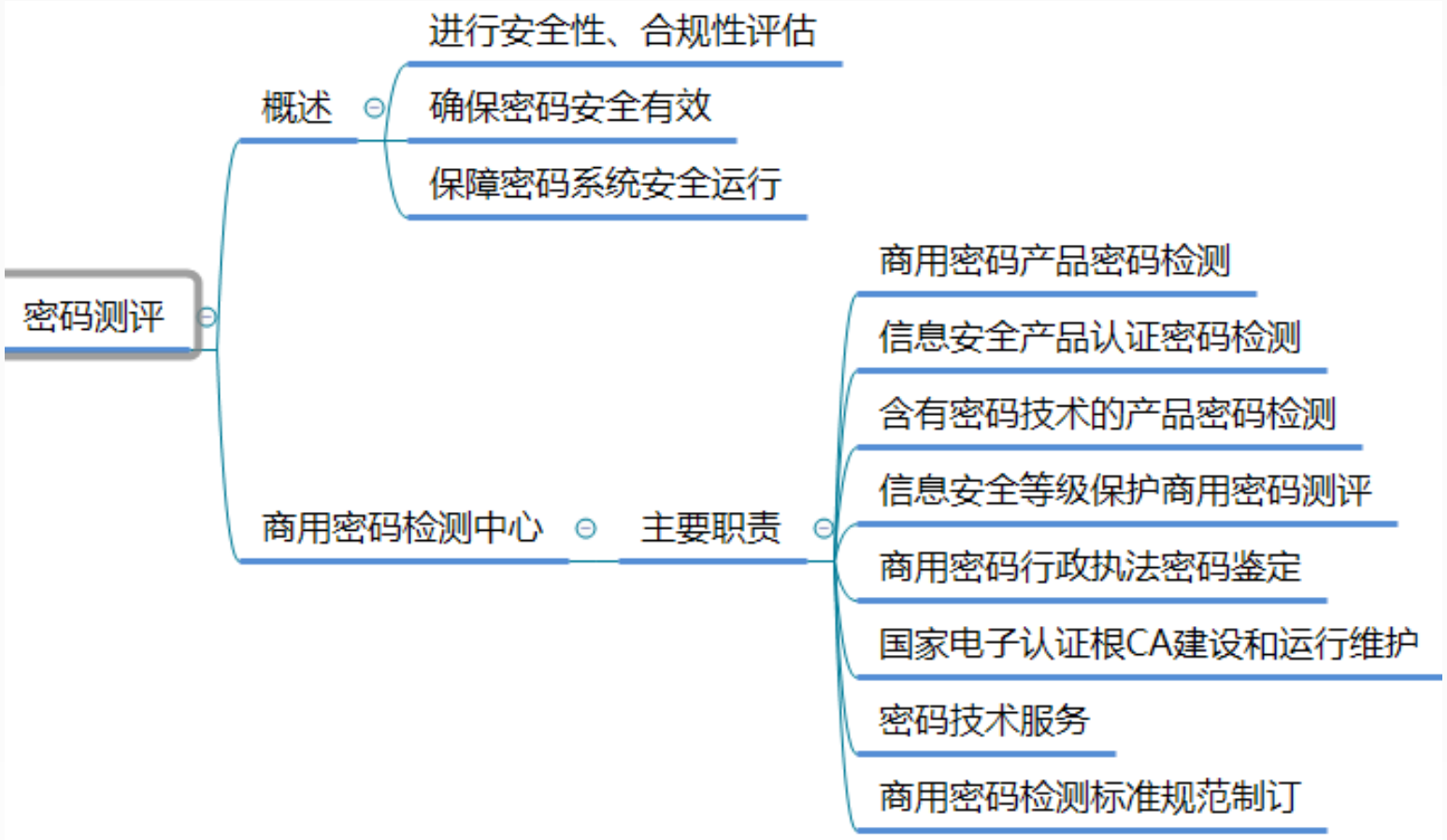


3.5.1 密码管理—密码管理政策

版权所有：我能过软考

3.5.1 密码管理—密码测评

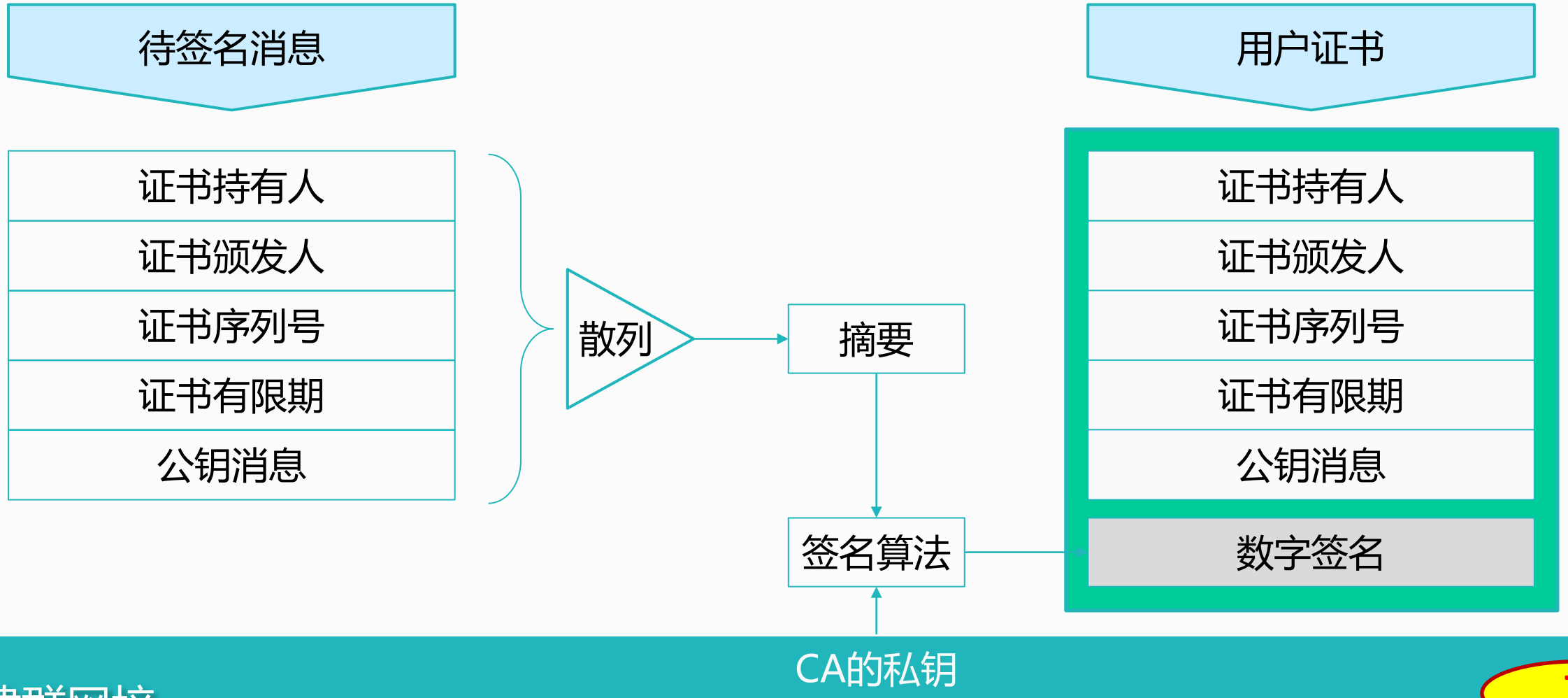
版权所有：我能过软考



3.5.2 数字证书

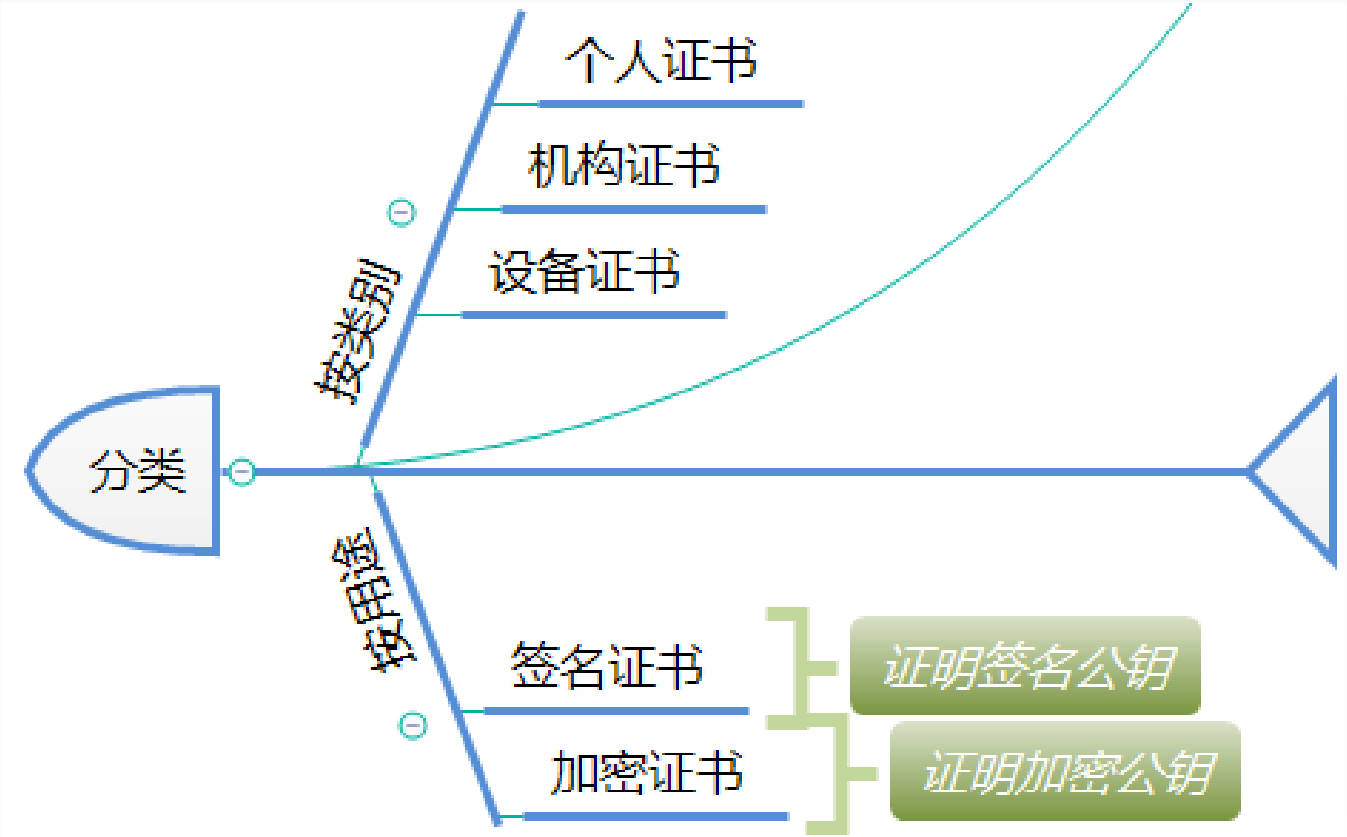
版权所有：我能过软考

数字证书 (Digital Certificate) 也称公钥证书，是由证书认证机构 (CA) 签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的 种数据结构。



数字证书：分类

版权所有：我能过软考



版权所有：我能过软考

1. 以下关于数字证书的叙述中，错误的是（）
A.证书通常由CA安全认证中心发放
B.证书携带持有者的公开密钥
C.证书的有效性可以通过验证持有者的签名获知
D.证书通常携带CA的公开密钥

2. 甲不但怀疑乙发给他的信遭人篡改，而且怀疑乙的公钥也是被人冒充的，为了消除甲的疑虑，甲和乙决定找一个双方都信任的第三方来签发数字证书，这个第三方是（）
A.国际电信联盟电信标准分部（ITU-T）
B.国家安全局（NSA）
C.认证中心（CA）
D.国际标准化组织(ISO)

3.6.1 Diffie-Hellman 密钥交换协议

版权所有：我能过软考

- D-H密钥交换协议
- 1976年提出的，最早的公钥技术之一。
- 基于求解离散对数问题的困难性
- 主要功能仅仅是完成两个用户之间的密钥协商，并不能完成加解密或者其他功能。

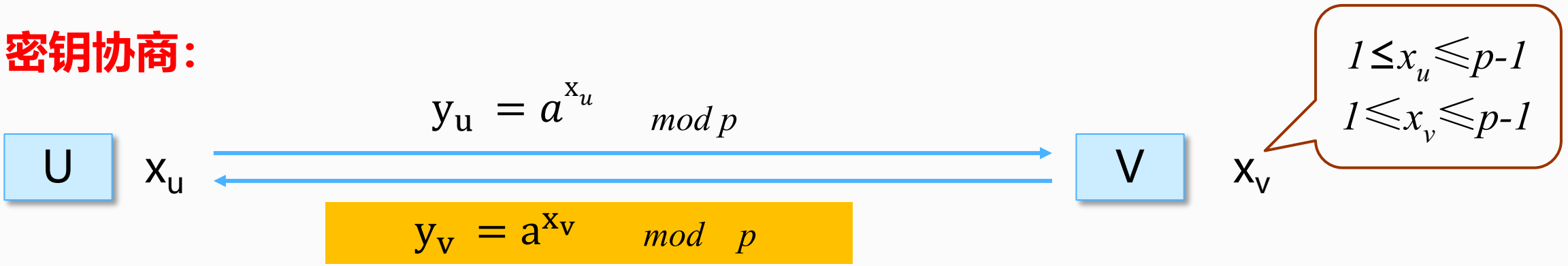
3.6.1 Diffie-Hellman 密钥交换协议

版权所有：我能过软考

◆ **参数选取：**

选取大素数p，再选择p的一个本原元a，并将p和a公开，全网公用。

◆ **密钥协商：**



$k = (y_v)^{x_u} \bmod p = a^{x_u x_v} \bmod p = k = (y_u)^{x_v} \bmod p$

➢ 将K作为双方协商的密钥，同时不再保留x_u和 x_v

D-H密钥交换协议的优缺点

版权所有：我能过软考

➢ **优点：**

1）任何两个人都可协商出会话密钥，不需事先拥有对方的公开或秘密的信息。

2）每次密钥交换后，不必再保留秘密信息，减少了保密的负担。

➢ **缺点：　容易受到中间人攻击。**

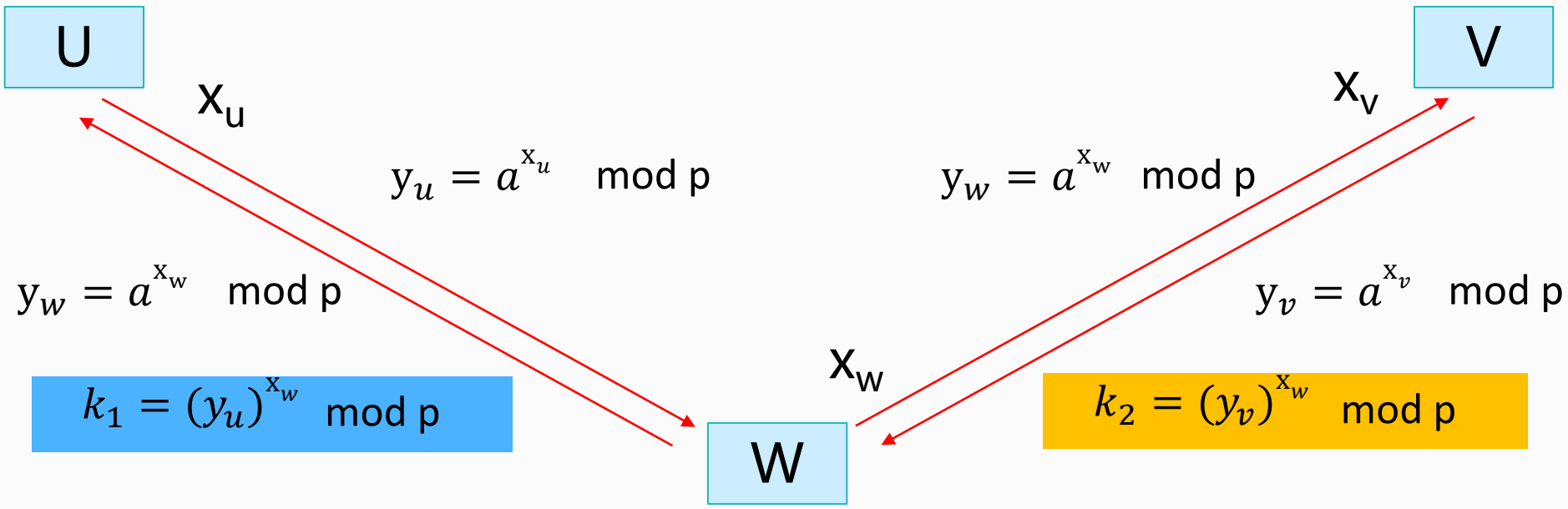
攻击者W在信道中间，假冒U，与V进行密钥交换；同时假冒V，与U进行密钥交换。致使看似U与V交换的密钥，实际上都是与攻击者交换的密钥。

D-H容易遭受中间人攻击

版权所有：我能过软考

$k_1 = (y_w)^{x_u} \bmod p$

$k_2 = (y_w)^{x_v} \bmod p$



原因： **D-H协议与双方的身份信息无关**

示例

版权所有：我能过软考

◆素数q=97,它的一个本原元a=5，A和B分别选择随机数X_A=36和X_B=58

- A 计算公开密钥：$Y_A=5^{36} \bmod 97=50 \bmod 97$
- B计算公开密钥：$Y_B=5^{58} \bmod 97=44 \bmod 97$
- A计算会话密钥：$K=(Y_B)^{X_A} \bmod p$

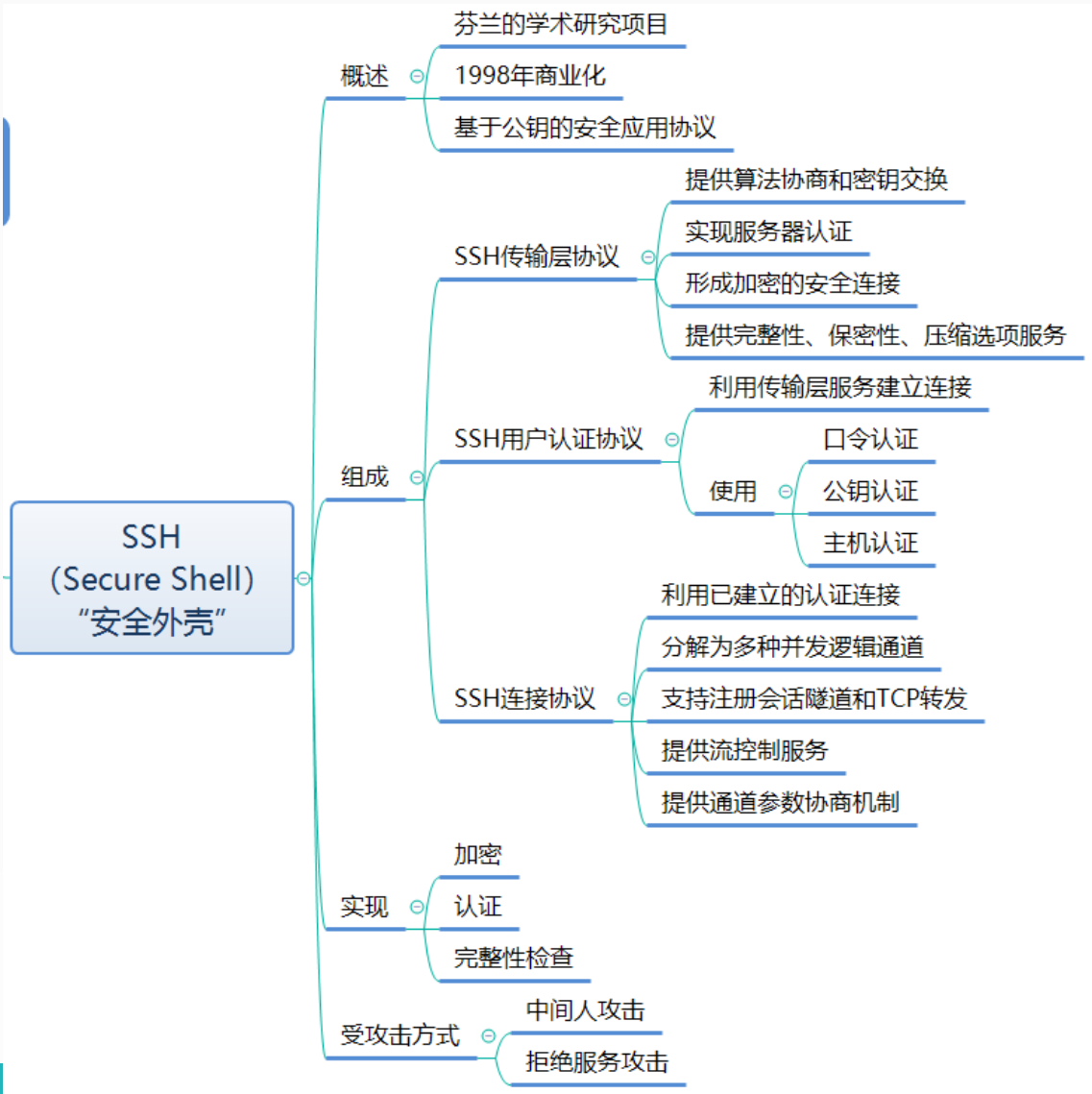
  $=44^{36} \bmod 97$

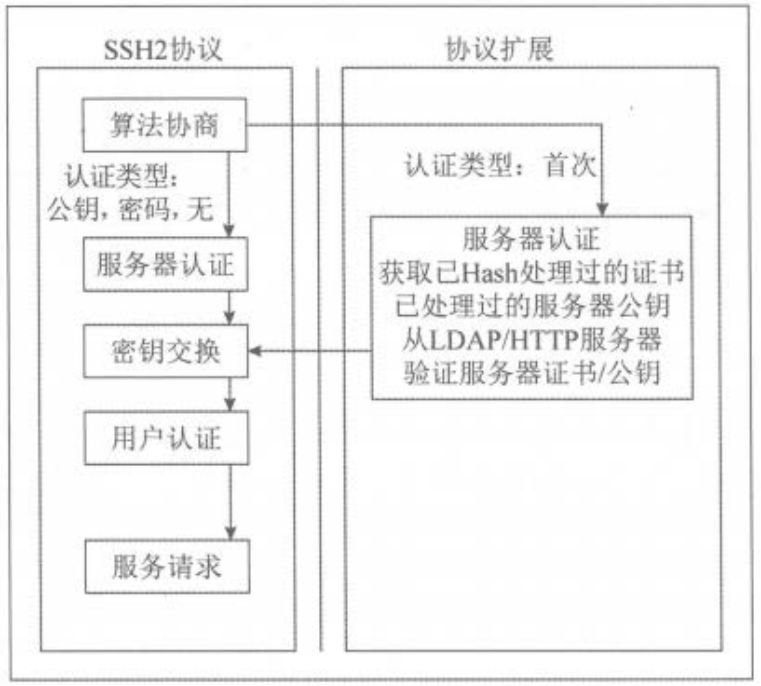
  $=75 \bmod 97$

- B计算会话密钥：$K=50^{58} \bmod 97=75 \bmod 97$

3.6.2 SSH

版权所有：我能过软考





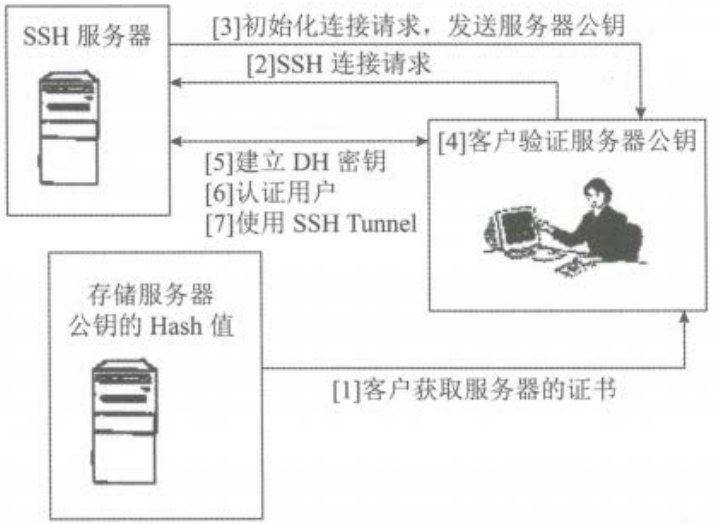
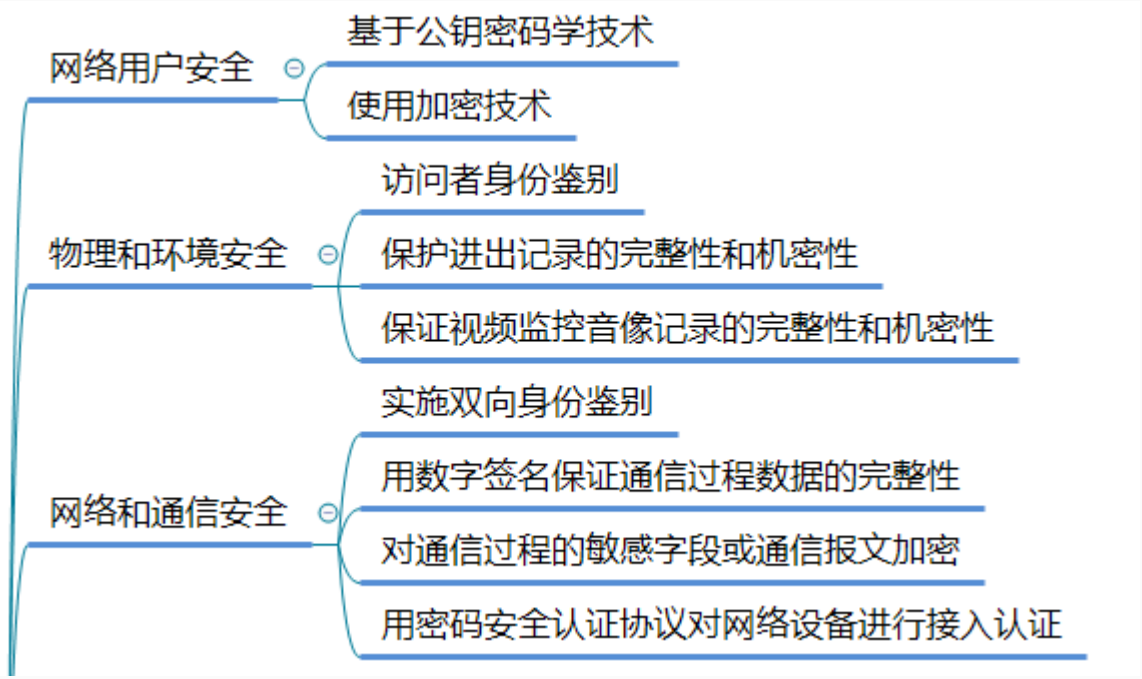


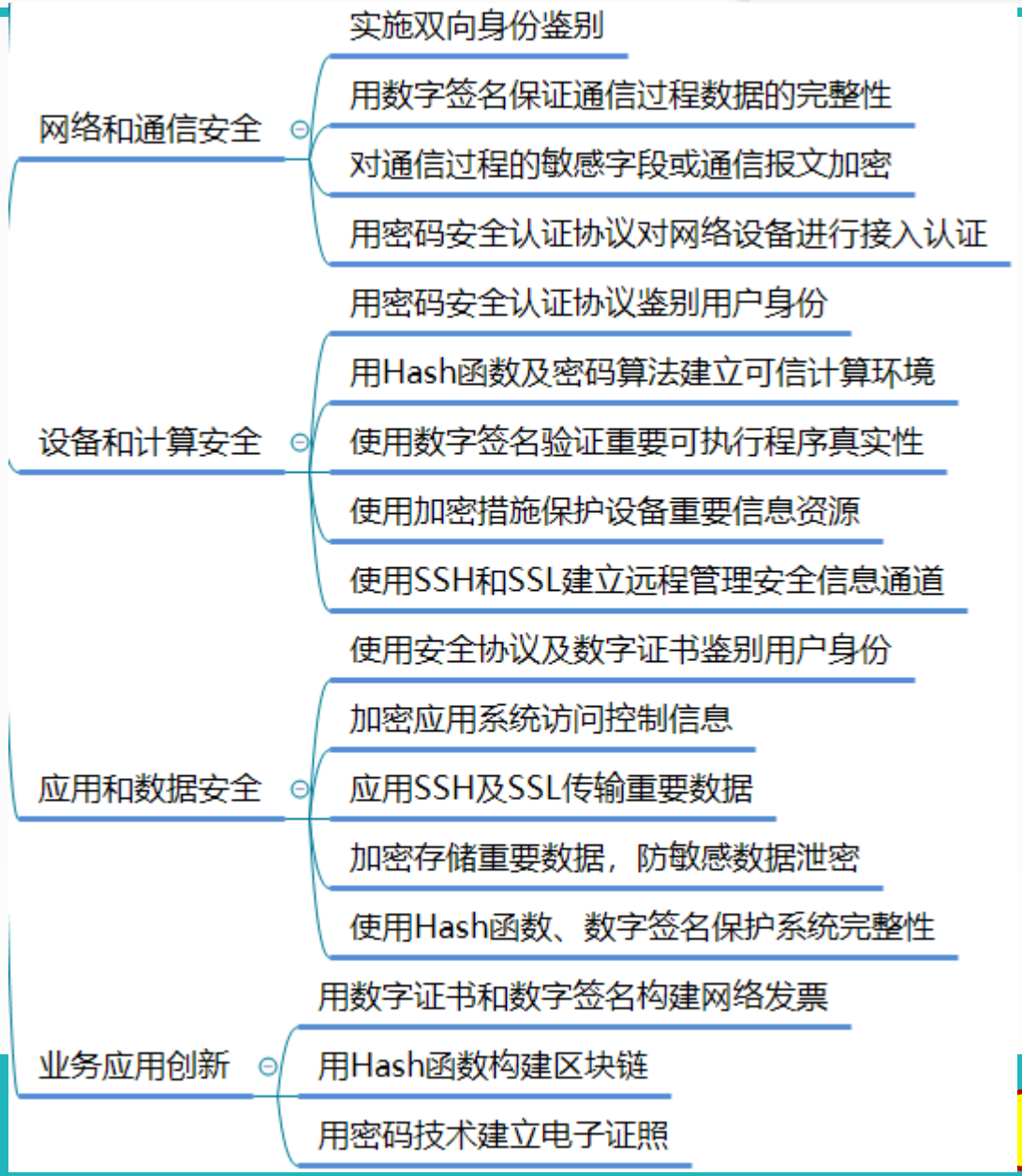
图 3-9　SSH 工作流程图

SSH 的服务进程端口通常为 22

3.7.1 密码技术常见应用场景类

版权所有：我能过软考





3.7.2 路由器安全应用参考

版权所有：我能过软考

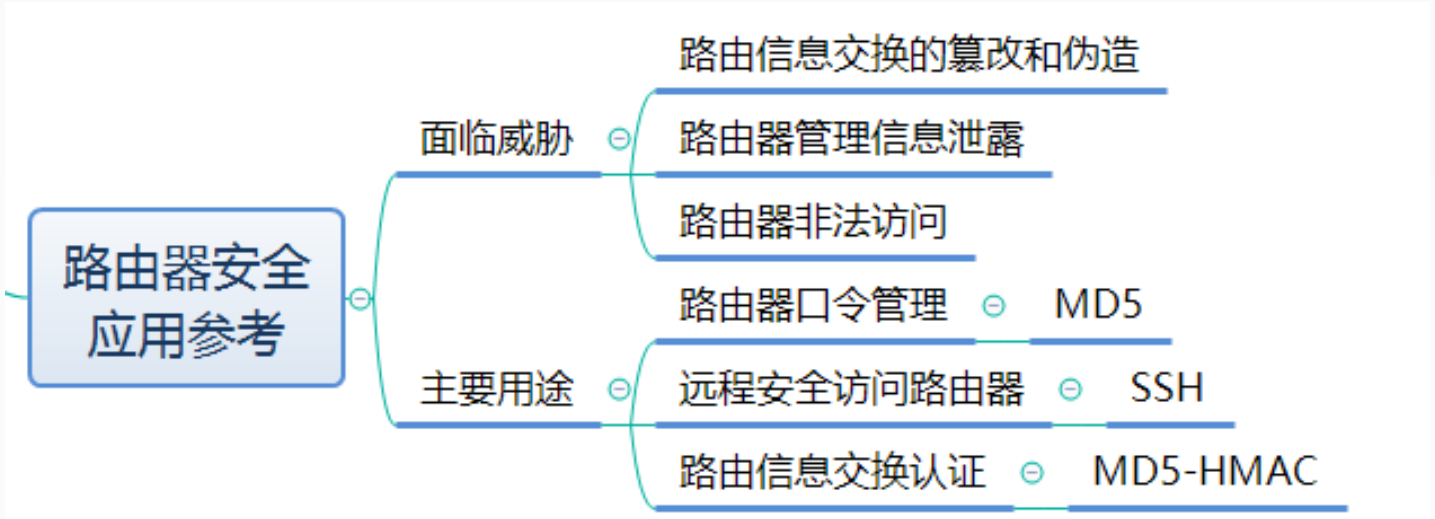
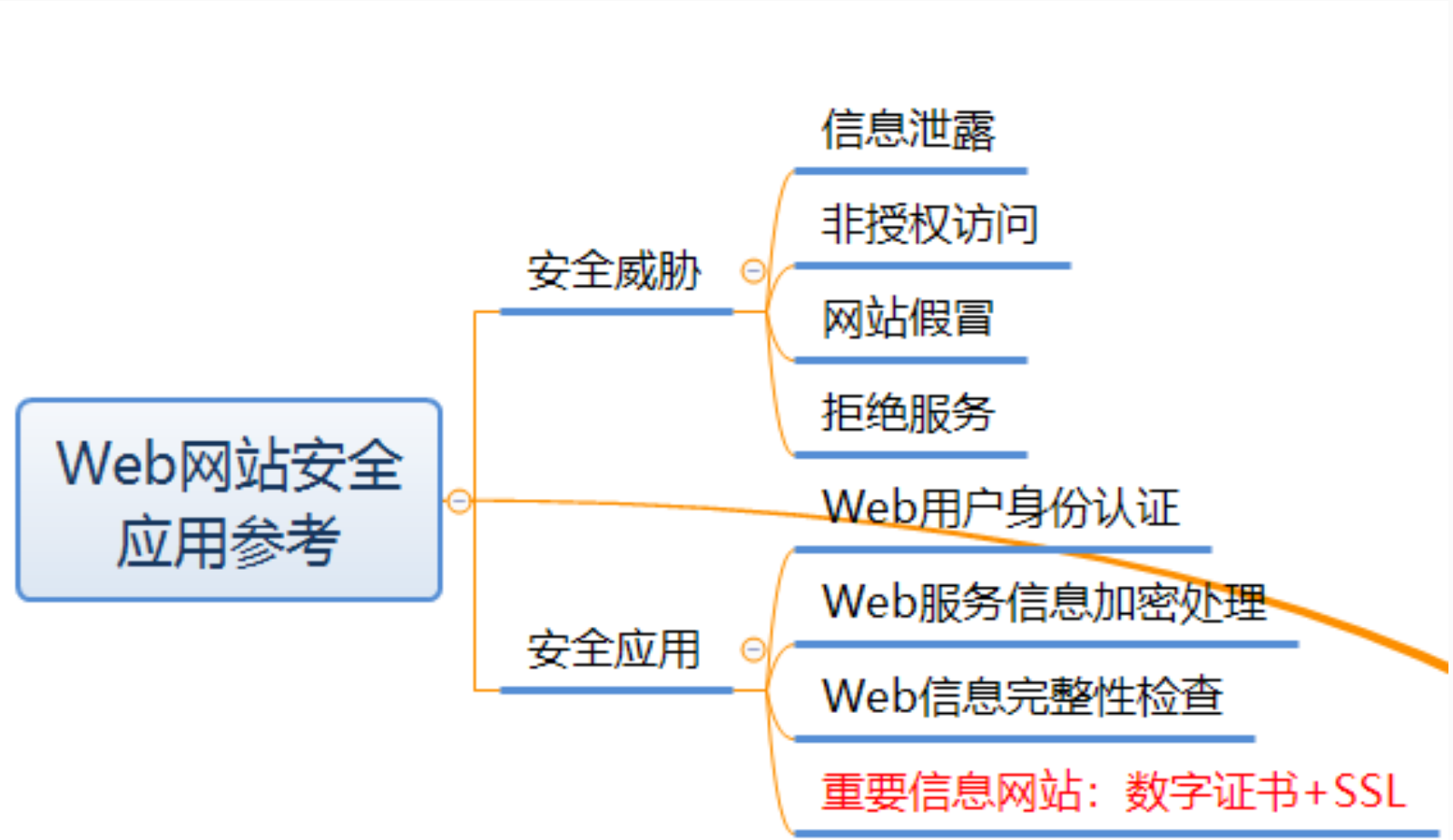


图 3-11　路由器信息交换认证示意图

3.7.3 Web 网站安全应用参考

版权所有：我能过软考



SSL补充

版权所有：我能过软考

◆ 安全套接层协议SSL（Security Socket Layer）

- 就是设计来保护网络传输信息的,它工作在传输层之上、应用层之下，其底层是基于传输层可靠的流传输协议（如TCP）
- 是一种国际标准的加密及身份认证通信协议，提供了两台机器间的安全连接。

◆ SSL提供的服务

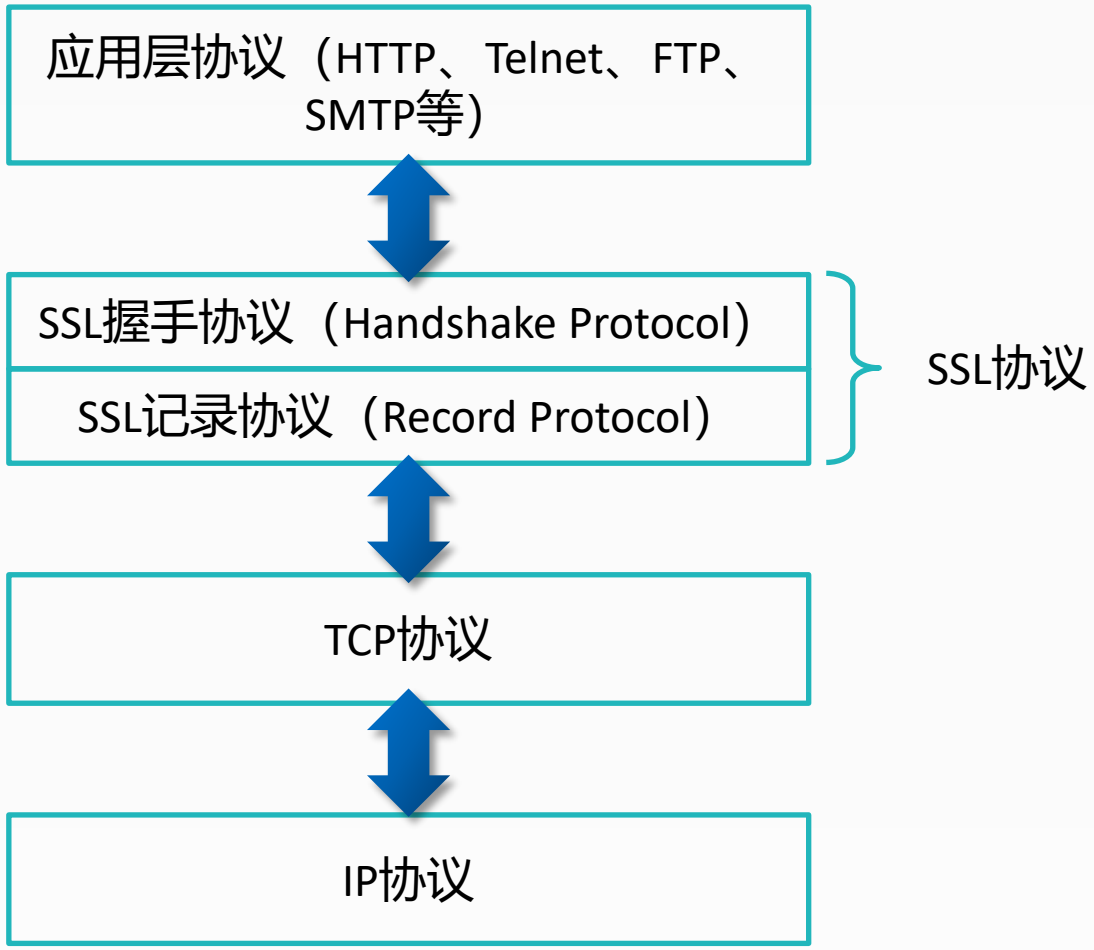
- 认证用户和服务器，确保数据发送到正确的客户机和服务器；（数字证书和公钥密钥技术）
- 加密数据以防止数据中途被窃取；（对称算法）
- 维护数据的完整性，确保数据在传输过程中不被改变。（MAC）

SSL不能提供对任何信息都实现抗抵赖性

SSL体系结构

版权所有：我能过软考

- 1）SSL的握手协议
  - SSL握手协议用于鉴别初始化和传输密钥，它使得服务器和客户能相互鉴别对方的身份，并保护在SSL记录中发送的数据。
- 2）SSL的记录协议
  - SSL从应用层取得的数据需要重定格式（分片、可选的压缩、应用MAC、加密等）后才能传给传输层进行发送。



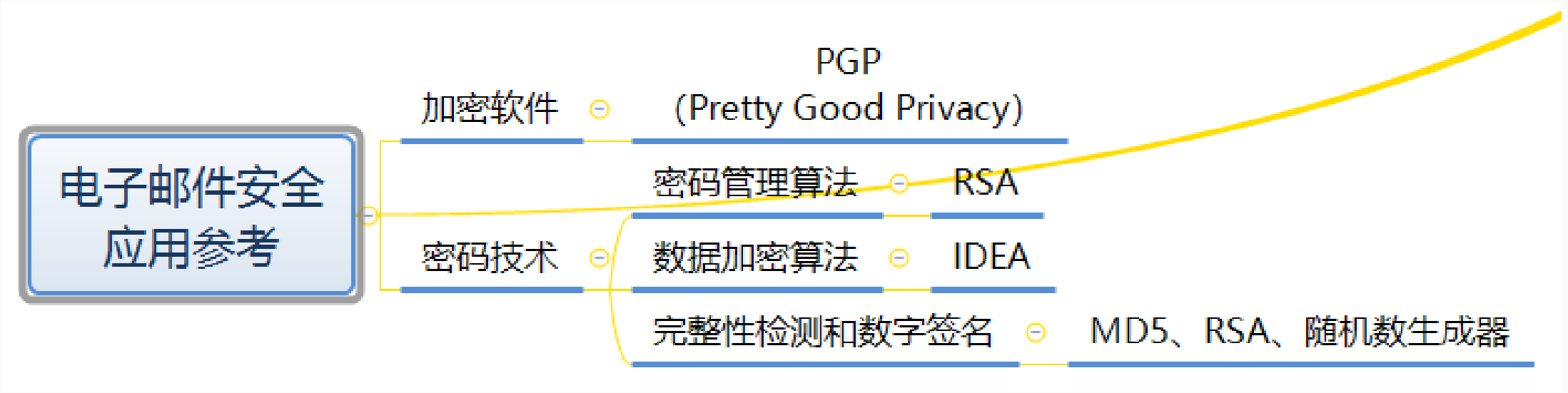
版权所有：我能过软考

3.以下关于安全套接字层协议(SSL)的叙述中，错误的是()
A.是一种应用层安全协议
B.为TCP/IP连接提供数据加密
C.为TCP/IP连接提供服务器认证
D.提供数据安全机制

4. SSL协议是对称密码和公钥密码技术相结合的协议，该协议不能提供的安全服务是（）
A.保密性
B.可用性
C.完整性
D.可认证性

3.7.4 电子邮件安全应用参考

版权所有：我能过软考



版权所有：我能过软考

- PGP - Pretty Good Privacy

– 作者：Phil Zimmermann
– 提供可用于电子邮件和文件存储应用的保密与鉴别服务。
– pgp已成为Internet 标准文档（RFC 3156）
– http://ietf.org/html.charters/openpgp-charter.html

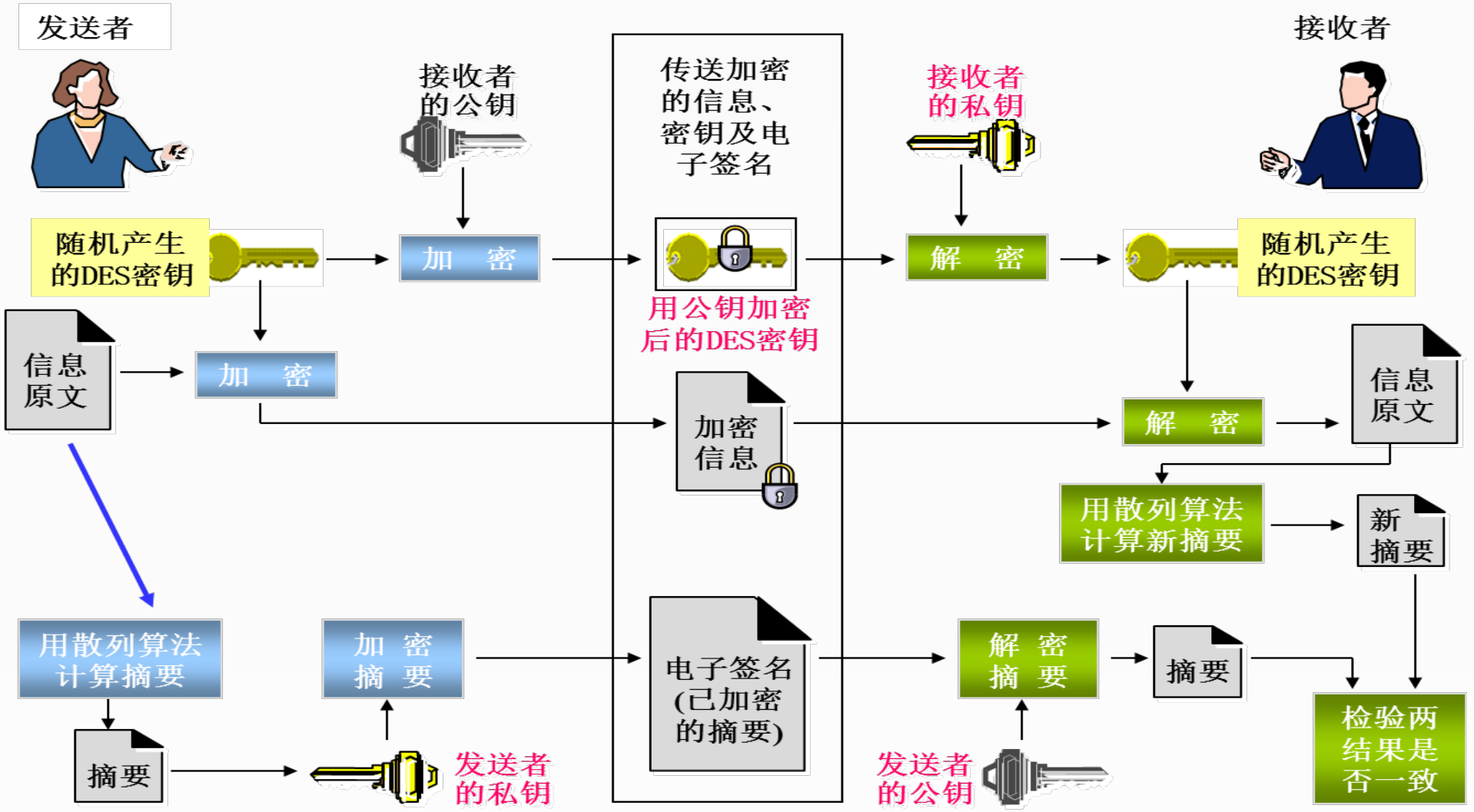
– 主要用于安全电子邮件，它可以对通过网络进行传输的数据创建和检验数字签名、加密、解密以及压缩。

PGP的功能

版权所有：我能过软考

功能	使用的算法	解释说明
保密性	IDEA、CAST或三重DES， Diffie-Hellman或RSA	发送者产生一次性会话密钥，用会话密钥以IDEA或CAST或三重DES加密消息，并用接收者的公钥以Diffie-Hellman或RSA加密会话密钥
签名	RSA或DSS，MD5或SHA	用MD5或SHA对消息散列并用发送者的私钥加密消息摘要
压缩	ZIP	使用ZIP压缩消息，以便于存储和传输
E-mail兼容性	Radix64交换	对E-mail应用提供透明性，将加密消息用Radix64变换成ASCII字符串
分段功能	-	为适应最大消息长度限制，PGP实行分段并重组

版权所有：我能过软考


发送者
接收者的公钥
传送加密的信息、密钥及电子签名
接收者的私钥
接收者
随机产生的DES密钥
加 密
用公钥加密后的DES密钥
解 密
随机产生的DES密钥
信息原文
加 密
加密信息
解 密
信息原文
用散列算法计算新摘要
新摘要
用散列算法计算摘要
加 密 摘 要
电子签名(已加密的摘要)
解 密 摘 要
摘要
检验两结果是否一致
摘要
发送者的私钥
发送者的公钥

版权所有：我能过软考

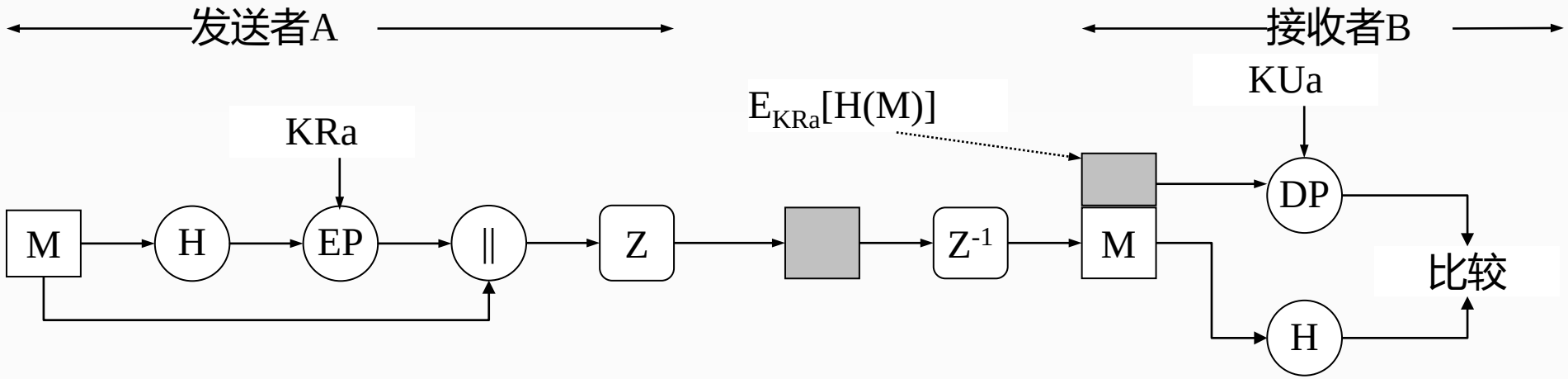


图7.15 （a） PGP的操作过程——只进行鉴别

其中，图7.15记号的含义为：

Ks: 会话密钥

Kra: 用户A的私钥

KUa: 用户A的公钥

H: 散列函数

||: 连接

R64:用radix64转换到ASCII格式

EP: 公钥加密

DP: 公钥解密

EC: 常规加密

DC: 常规解密

Z: 用ZIP算法进行数据压缩

Z^{-1}：解压缩

PGP鉴别的过程

版权所有：我能过软考

- PGP鉴别的过程
  - 发送者产生消息M；
  - 用SHA-1对M生成一个160位的散列码H；
  - H用发送者的私钥加密，并与M连接；
  - 接收者用发送者的公钥解密并恢复散列码H；
  - 对消息M生成一个新的散列码，与H比较。如果一致，则消息M被认证，即报文作为已鉴别的报文而接受。（提供DSS/SHA-1可选替代方案和签名与消息分离的支持。）

版权所有：我能过软考

- PGP提供的另一个基本服务是机密性，它是通过对将要传输的报文或者将要像文件一样存储在本地的报文进行加密来保证的（如图7.15(b)所示）。

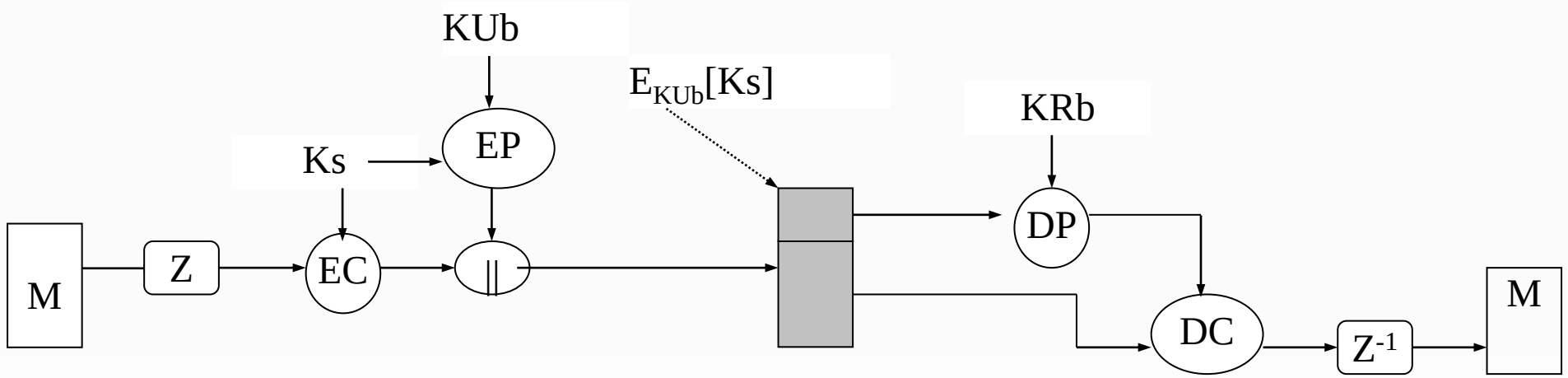


图7.15（b） PGP的操作过程——只保证机密性

版权所有：我能过软考

- PGP可以同时提供机密性与鉴别。当加密和认证这两种服务都需要时，发送者先用自己的私钥签名，然后用会话密钥加密，再用接收者的公钥加密会话密钥(如图7.15(c)所示)。

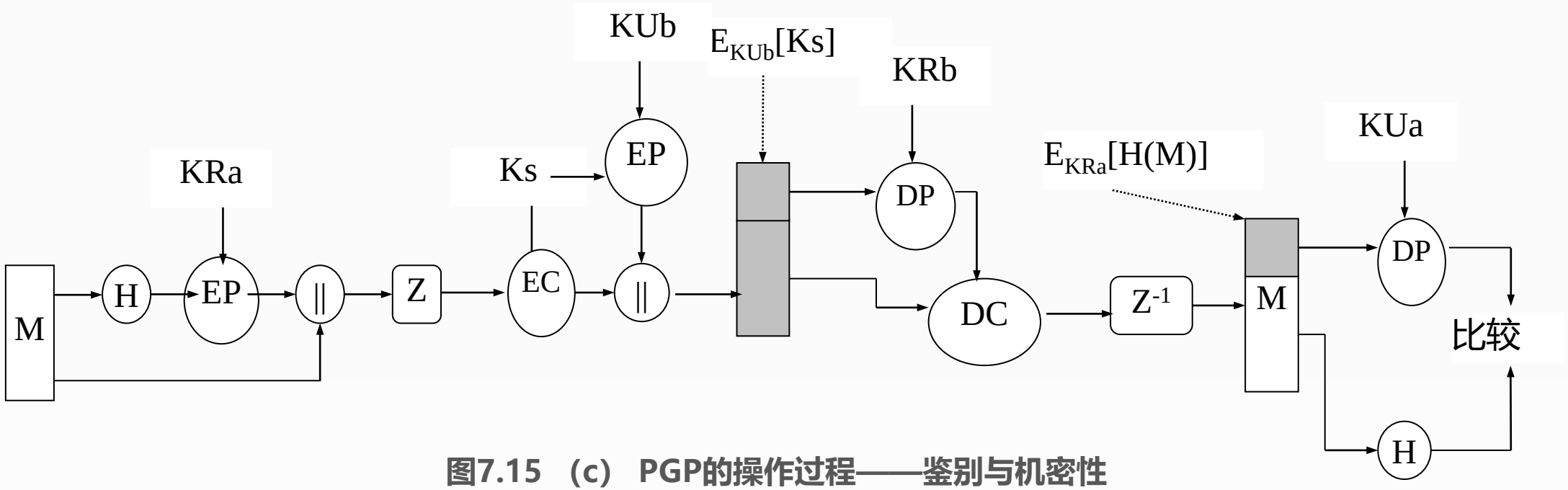


图7.15 （c） PGP的操作过程——鉴别与机密性

版权所有：我能过软考

- PGP对报文进行压缩，这有利于在电子邮件传输和文件存储时节省空间。但压缩算法的放置位置比较重要，在默认的情况下，放在签名之后加密之前。这是因为：
  - 对没有经过压缩的报文进行签名更好些。这样，为了将来的验证就只需要存储没压缩的报文和签名。如果对压缩文档签名，那么为了将来的验证就必须或者存储压缩过的报文、或者在需要验证时更新压缩报文；
  - 即使个人愿意在验证时动态生成重新压缩的报文，PGP的压缩算法也存在问题。算法不是固定的，算法的不同实现在运行速度和压缩比上进行不同的折衷，因此产生了不同的压缩形式。但是，这些不同的压缩算法是可以互操作的，因为任何版本的算法都可以正确地解压其他版本的输出。如果在压缩之后应用散列函数和签名，将约束所有的PGP实现都使用同样的压缩算法。
  - 在压缩之后对报文加密可以加强加密的强度。因为压缩过的报文比原始明文冗余更少，密码分析更加困难。


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

手淘扫一扫


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

建群网培