46、数字签名的原理及使用

答：①、发送方将消息散列，并用自己的私钥加密这个散列值，即为数字签名。②、将这个散列值与消息一并发送给接收方。③、接收方对该消息进行散列，并用发送方公钥对原始报文的数字签名进行解密，对比两者散列值，相同则报文完整。

47、数字证书的原理及使用

答：①、A 示证方向 CA 申请数字证书。②、CA 颁发经过 CA 私钥签名的数字证书，该证书包含 A 的身份信息和 A 的公钥，其他人无法伪造。③、A 使用私钥签名信息，连同数字证书一起发给验证方 B。④、B 使用 CA 公钥验证 A 的证书，通过后获取 A 公钥验证 A 签名的信息。

【注：注意上面两者的区别，加以理解。】

48、X.509 数字证书在 PKI 中的作用

答：X.509 数字证书在网络中证实了实体所声明的身份与其公钥的匹配关系。数字证书是非对称密钥管理的媒介，密钥的分发传送是通过数字证书来实现的。数字证书提供身份认证功能，识别完整性、保密性、不可否认性。

49、消息编码认证的基本思想

答：思想源于消息通信中的差错校验码。通过引入冗余度，是传送的可能序列集（M）大于消息集（S）。发送方从 M 中选出代表消息的序列 L 对消息编码。接收方按此规则进行解码。攻击者不知道选定的编码规则，伪造的假消息多为禁用序列，能通过消息编码检测出来篡改。

【注：考这个的可能性不大，不算太重点的知识，理解原理即可。】

50、AH 协议与 ESP 协议都支持认证功能，两者有什么区别。

答：AH 的认证作用域是整个 IP 数据包，包括 IP 头和承载数据，ESP 的作用域只是承载数据，不包括 IP 头，理论上，AH 的认证安全性高于 ESP 认证服务。

【注：注意区分 AH 与 ESP 认证服务、加密服务的作用域。】

51、安全关联 SA 的工作原理。

答：见书本 P136~137。结合文字与图作答。

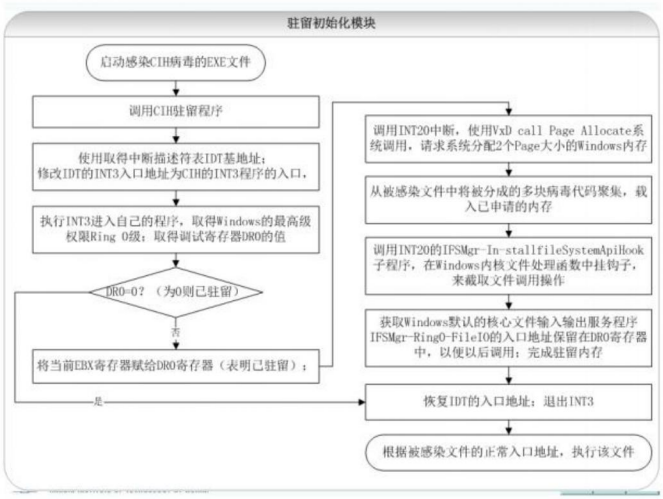
52、在 DES 加密算法中，ECB、CBC、CFB、OFB 模式下，假设传输时一个比特出错，对接收方解密有什么影响？

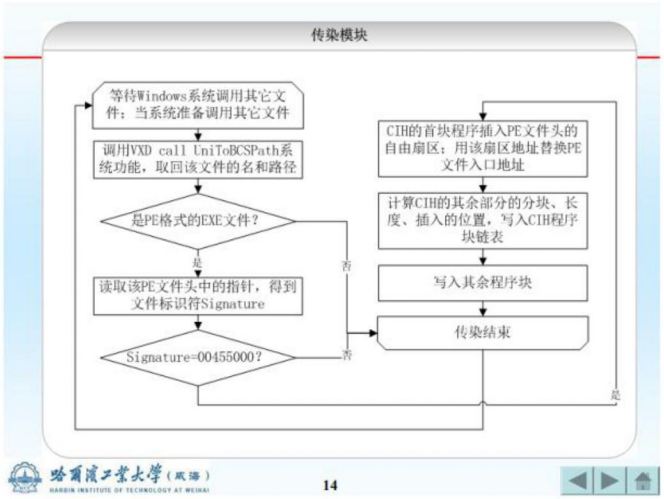
答：ECB：对应密文块无法解密。CBC：涉及两块密文块无法解密。CFB：涉及两块密文块无法解密。OFB：只有对应一个密文块无法解密。

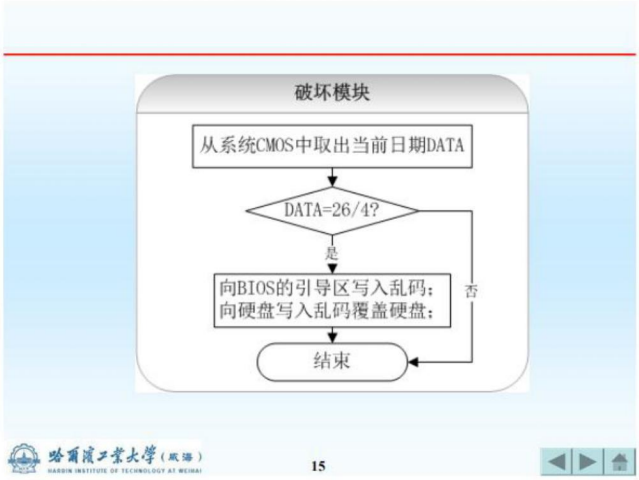
【注：与前面加密时比特出错对照理解。】

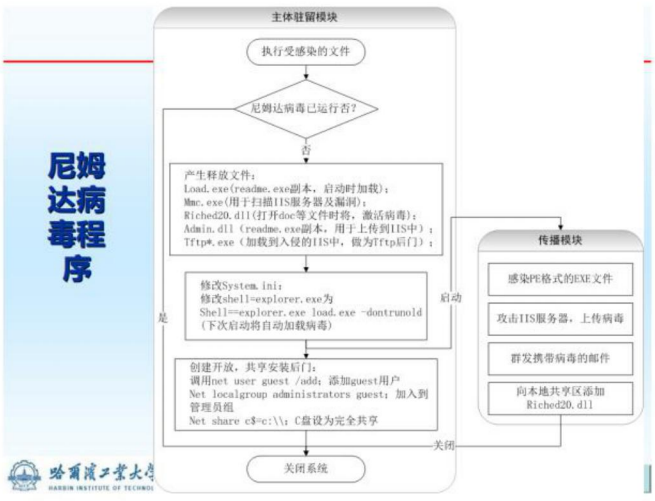
53、简述 CIH、尼姆达、灰鸽子的实现原理

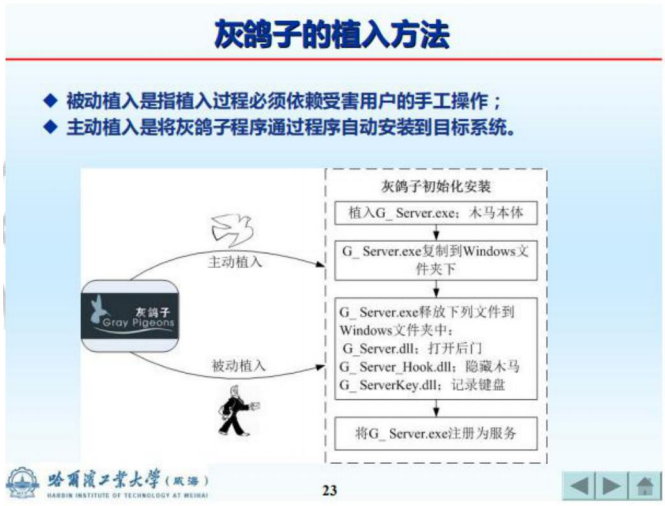
答：











【注：理解模块，过程即可，不需要过于深入了解其中内容，不太可能考。】

54、试推导哈希碰撞概率公式

答：设有 n 次试验，d 为输出取值空间，则不发生碰撞概率为：

$$P(n)=1*(1-\frac{1}{d})*(1-\frac{2}{d})\ldots\ldots(1-\frac{n-1}{d})$$

则发生碰撞概率为：

$$1-p(n)$$

便于计算可用泰勒公式近似表示：

$$e^x=1+x+\frac{x^2}{2}\ldots\ldots\frac{x^n}{n},x\to 0$$

$$e^x\approx 1+x$$

则：

$$e^{-\frac{i}{d}}\approx 1-\frac{i}{d}$$

故，哈希碰撞概率公式为：

$$p(n,d)=1-p(n)=1-e^{-\frac{n(n-1)}{2d}}$$

【注：了解即可】

55、简述数字证书撤销的原因

答：①、数字证书持有者报告该证书对应的私钥被盗。②、CA 发现签发证书出错。③、证书持有者离职，证书再起在职期间签发。

【注：了解即可。】