2024 年网络安全协议期末考试详细回忆版

注：本试卷完全由笔者回忆得，如有差错敬请谅解。

一. 填空题（20 题 × 1 分=20 分）

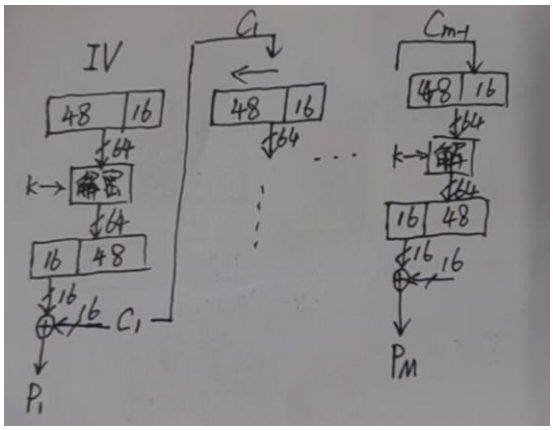
1. 请写出以下简写的英文全称或中文释义：
   DDOS(1)　　AAA(2)　　SET(3)　　SSL(4)
2. 中断针对的是(5)，窃听针对的是(6)，篡改针对的是(7)，伪造针对的是(8)（请填网络安全特征）
3. SSL 中 KDF 函数为了计算主密钥，除了需要输入预主密钥，还需要输入包括(9)，(10)，
4. IPSec 协议主要包含了 AH，(11)，(12)。
5. SA 三元组为协议，(13)，(14)。
6. AH 外出处理包括：自上而下检索(15)，从(16)查找对应多个(17)，构建 AH 载荷，添加 IP 头，其他。
7. PGP 基于 64 变换使得长度扩大了(18)%，目的是实现(19)功能。
8. 小王正在进行交易，PI，OI 表示支付与预购信息。K1，K2 为密钥，$E_k[x]$表示使用密钥 k 对内容 x 进行加密或签名。请给出小明的双数字签名(20)。

二. 不定项选择题。（前五题为单项选择题，后五题为不定项选择题，少答得 1 分。）（10 题 × 2 分=20 分）

1. SSL 认证算法的实现中，哪一项可能是一对公钥与私钥？
   A. 服务器侧写密钥&客户端侧写密钥
   B. 服务器侧读密钥&客户端侧写密钥
   C. 服务器侧写密钥&客户端侧读密钥
   D. 服务器侧读密钥&客户端侧读密钥
2. 在密钥交换协议中，接受方采用什么处理而得到会话密钥
   A. 发送者公钥　B. 发送者私钥　C. 接收者公钥　D.接收者私钥
3. 这个协议可以用于保护两个应用程序之间的通信安全，其是 Internet 上的工业标准。
   A. IPSEC
   B. PGP
   C. SSL
   D. SET
4. 小王收到一封邮件，邮件内容为提醒小明下载安装补丁，请问这是什么攻击？
   A. 爆破攻击
   B. 特洛伊木马攻击
   C. 钓鱼攻击
   D. 蠕虫病毒攻击
5. 内网与外网之间构建 DMZ，外路负责防止外部网络对 DMZ 的未授权访问，内路管理内网与 DMZ 访问。请问，这种配置最适合使用哪种类型的防火墙？
   A. 屏蔽主机型防火墙
   B. 双宿柱型防火墙
   C. 屏蔽子机型防火墙
   D. 包过滤型防火墙
6. 数字证书内容必须含有：
   A. 用户公钥
   B. CA 公钥
   C. 用户身份信息
   D. 用户权限
   E. 生效与失效日期
7. 下列关于 PKI 中，错误的是：
   A. 数字签名可以提供数据完整性，防止消息的否认
   B. MAC 可以提供数据完整性，防止消息的否认

C. PKI 中 CA 为双方分配共享密钥
D. PKI 中签名私钥不进行备份，存在周期长
E. PKI 中加密密钥不进行备份，存在周期长

8. 由一个 CA 和多个 RA 组成的系统中，CA 的作用有：
   A. 参与加密解密
   B. 签发数字证书
   C. 安全管理
   D. 维护 CRL
   E. 审查用户注册信息
9. 由我国自主研发的 WLAN 标准有：
   A. WPA
   B. WPA2
   C. 802.11i
   D. WAPI
   E. TD-SCPMA
10. 下列不是 DNSSec 功能的有：
    A. 源端认证
    B. 目的端认证
    C. 完整性检验
    D. 增加或修改 DNS 中的资源记录
    E. 验证域名与 IP 地址之间的正确映射关系



三. 简答题（12+6+6+6+6+12+12=60 分）

1. 左上方图为 CFB 解密过程。(1) 请按照解密过程，绘制出 CFB 加密过程图解（2）假如有 1bit 错误，请问他会传多远（3）在 CFB 中，IV 有什么作用?
2. 会话重用的目的是什么？在哪一个协议中?
3. A 需要对通信端进行认证以确认 B 的身份，设计一个基于数字签名的方案。注意，该方案需要具备抗重放攻击的能力。
4. IPSec AH/ESP，SSL/TLS 都不使用数字签名，请说明原因
5. A,B 都可以独立使用各种数据加密方法，但是 AB 之间没有可靠的密钥分配以及传输渠道，信道不安全。现在 A 想要向 B 发送消息，请问能否做到，如果能请详细解释。
6. PGP 是一种用于数据加密和签名的程序，它可以提供加密、认证、保护和压缩功能（1）请描述邮件发送端产生 PGP 消息的具体过程，包括使用密钥的情况，给定加密、认证和压缩的顺序及其理由。(2) 在通信过程中，一个用户可能拥有很多密钥，如何确定哪个密钥对应于接收到的消息。(3) 讨论存储私钥的安全手段。
7. NATPT 是 NAT 技术中的一种，它不仅转换源地址和目的地址，还结合了 IP 地址和传输层端口号的转换。如图涉及提供源地址转换和目的地址转换的功能。目的用户 A 尝试浏览地址为'http://202.38.75.11'的网页，并且能够访问到 C 服务（1）网关 B 执行的操作设置（2）在 Linux 中网层处理过程中，与防火墙和 NAT 相关的功能是由哪一个模块实现的，为什么是该模块？（3）给出在 web 页面请求过程中，用户 A、网关 B、服务器 C 上 IP 数据包地址字段的变化以及 NAT 模块的操作。