网络安全实习概论

第二章. 8

(1) Alice公钥为 (n, e) 即 $(p \times q, e) \Rightarrow (437, 13)$

(2) $\phi(n) = 18 \times 22 = 396$

$de = 1 \pmod{396} = 13d$

$396 = 30 \times 13 + 6$

$13 = 2 \times 6 + 1$

$\therefore 1 = 13 - 2 \times 6$

$= 13 - 2 \times (396 - 30 \times 13)$

$= 13 + 60 \times 13 - 2 \times 396$

$= 61 \times 13 - 2 \times 396$

$\therefore d = 61$

由于没有Bob的公钥信息，这里姑且不考虑安全性，仅叙述用Alice的p. q及e对"10"进行加解密的过程：

加密：

密文 $C = M^e \pmod{n} = 10^{13} \pmod{437} = 222$

$13 = 1 + 4 + 8$

$10^1 \pmod{437} = 386 = -51$

$10^4 \pmod{437} = 416 = -21$

$10^{13} \pmod{437} = (10 \times -51 \times -21) \pmod{437}$

$= 222$

解密：

明文 $M' = c^d \pmod{n} = 222^{61} \pmod{437} = 10$

No.

Date

第三章.2

机密性：确保信息不会泄露给不应知情的人（未授权的实体）
认证性：验证数据来源的真实性，即确认信息确实来源于声称的发送者
完整性：确保信息在传输中保持准确、完整，未被破坏
不可抵赖性：确保信息交换的参与方不能否认其行为，有据可查

第五章.3

① 传输层：TCP并发连接数、最大TCP连接建立速率
② 网络层：吞吐量、时延、丢包率、背压背缓冲
③ 应用层：HTTP传输速率、最大HTTP事务处理速率

第六章.4

CIDF主要由4个部分组成：CIDF的体系结构、通信机制、描述语言和API

体系结构：① 事件产生器：从系统之外的环境收集事件并发送其它组件
② 事件分析器：分析其它组件的GIDO并经过更新的GIDO
③ 事件数据库：用于存储GIDO
④ 响应单元：处理收到的GIDO，采取措施

通信机制：① GIDO定义事件表示方法
② 消息层负责将数据从发送方传到接收方
③ 体系传输层定义各个组件间的传输机制

描述语言：CISL：用S表达式编组，对各种事件和分析结果编码，封装在得到GIDO

API作为：负责创建GIDO编码、解码与传递

第九章

6. 拒绝服务攻击：攻击者设法使目标主机停止服务。由单个攻击源出发，利用网络协议的缺陷，采用耗尽目标主机的通信、存储或计算资源的方式以迫使目标主机暂停服务甚至系统崩溃。

分布式拒绝服务攻击：在攻击的DoS行为发起前，多个攻击源联合起来攻击一个主机，操纵大量傀儡主机中的代理程序以攻击，流量更大。

7. ① 缓冲区溢出攻击是利用缓冲区溢出漏洞所进行的攻击行为。
攻击者通过向目标程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序堆栈，使程序转而执行其指令，以达到攻击的目的。

② 1) 通过OS控制使接收数据的缓冲区不可执行，从而阻止攻击者植入代码
2) 要求编写正确的代码，拒绝存在溢出风险的函数
3) 利用编译器的边界检查实现缓冲区的保护，使溢出不能发生，但代价较大。