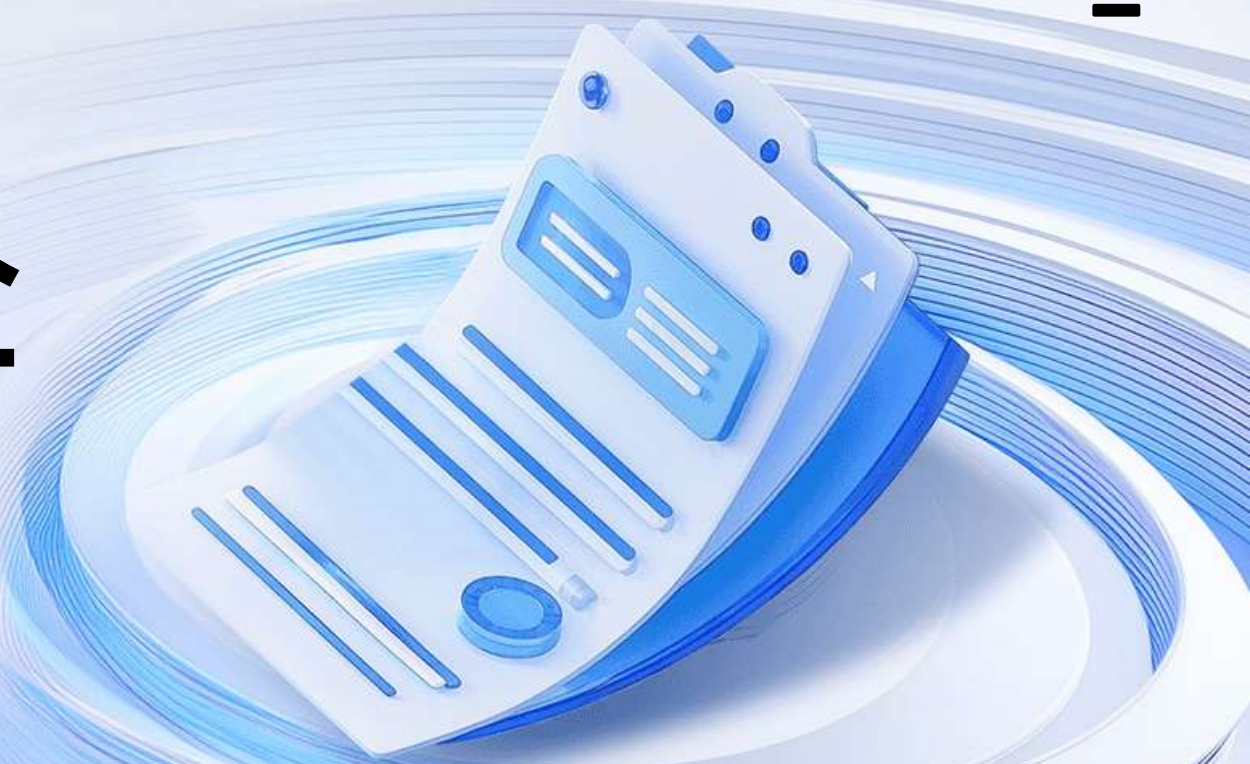
第7章 网络安全课后习题讲解



汇报人：林银蕊 甘芝清 黄慧雯

汇报日期：2025/12/03

目录

CONTENTS

/ 01. 书本习题题

书本习题

01

书本习题7-2：拒绝服务与分布式拒绝服务攻击的产生

拒绝服务 DoS（Denial of Service）和分布式拒绝服务 DDoS（Distributed DoS）这两种攻击是怎样产生的?

解答:

拒绝服务 DoS 的产生方式（常使用虚假 IP 地址）：

1. 向特定服务器快速发送大量任意分组，导致服务器过载瘫痪。
2. 发送大量 TCP SYN 报文段，耗尽服务器连接资源（SYN flooding）。
3. 重复建立 TCP 连接并发送无用报文段。
4. 发送不完整的 IP 数据报分片，使目的主机持续等待组装。
5. 向多个网络发送 ICMP 回送请求，引发大量响应导致网络拥塞（Smurf 攻击）。

分布式拒绝服务 DDoS 的产生方式：

1. 攻击者获取大量主机账号，秘密安装从属程序。
2. 攻击者通过主程序控制所有从属程序，同一时刻向目标主机发起 DoS 攻击，破坏性极强。

书本习题7-5：RSA 加密和解密示例

能否举一个实际的 RSA 加密和解密的例子?

解答:

举一个说明 RSA 工作原理的例子，选择 p=5，q=7，e=5，明文为英文字母 o，完成加密和解密过程。

1.密钥生成:

选择素数 p=5，q=7，计算 $n=p\times q=35$，$\Phi(n)=(p-1)(q-1)=24$。

选择 e=5（与 24 互素），由 $ed\equiv 1 \bmod 24$，解得 d=29（$5\times 29=145\equiv 1 \bmod 24$）。

公钥 PK=(5,35)，私钥 SK=(29,35)。

2.明文转换：英文字母 o 对应序号 15（X=15<35）（因 759375=21696×35+15）。

3.加密：$Y=X^e \bmod n=15^5 \bmod 35=759375 \bmod 35=15$，即密文 Y=15。

4.解密：$X=Y^d \bmod n=15^{29}$ ，mod 35=15，还原为字母 o。

THANK YOU FOR READING!

感谢您的观看

汇报人：林银蕊 甘芝清 黄慧雯

汇报日期：2025/12/03