习题课答疑

第一次作业

思考题 1.2&1.3

被动攻击和主动攻击之间有什么不同

列出并简要定义主动攻击和被动攻击的分类

- **主动攻击(active attack):**

更改数据流，或伪造假的数据流。可以划分为：假冒、重放、改写消息、拒绝服务

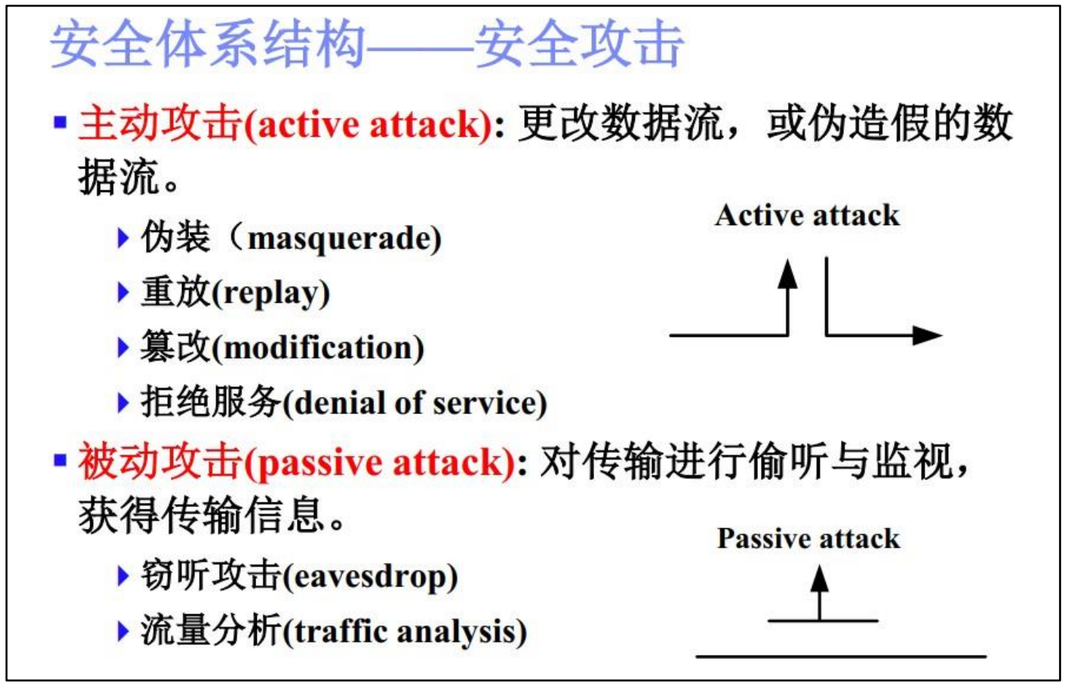
主动攻击难以防范，但是容易被检测并可以恢复

- **被动攻击(passive attack):**

对传输进行偷听与监视，获得传输信息。

主要形式包括：消息内容泄露攻击、流量分析攻击

被动攻击难以检测，重点在于防范



思考题2.4

分组密码和流密码的区别是什么？

- **序列密码**（stream cipher)： 序列密码按**位或字节**加密，也可以称为流密码，序列密码是手工和机械密码时代的主流。
- **分组密码**(block cipher)： 分组密码将明文分成固定长度的组，用同一密钥和算法对**每一块**加密，输出也是固定长度的密文。

分组密码一次处理一个输入元素分组，产生与该输入分组对应的一个输出分组。**流密码**连续处理输入元素，每次产生一个输出元素。

思考题2.8

为什么3DES的中间部分是解密而不是加密？

为了与单次DES兼容。

思考题 2.7

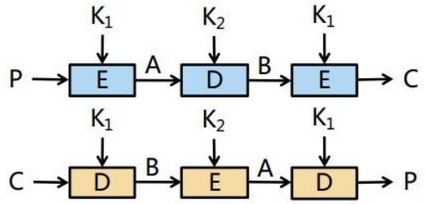
什么是三重加密？

使用三个密钥对数据块进行三次DES操作，三重DES有四种模型：

- DES-EEE3 使用三个不同密钥顺序进行三次加密变换
- DES-EDE3 使用三个不同密钥依次进行加密-解密-加密变换 (3DES标准)
- DES-EEE2 其中密钥K1=K3 顺序进行三次加密变换
- DES-EDE2 其中密钥K1=K3 依次进行加密-解密-加密变换

2、3DES（TDEA）

- 使用两个密钥的算法：
  - $C=E(K_1,D(K_2,E(K_1,P)))$
  - $P=D(K_1,E(K_2,D(K_1,C)))$



- 加密、解密交替使用，仅仅为了与单次DES兼容

习题2.11

Alice和Bob同意使用RC4通过E-mail秘密通信，但是他们想要避免在每次传输的过程中使用新的密钥。Alice和Bob私下同意使用128比特的密钥K。为了对一串比特的信息m进行加密，使用下列流程：

1.选择一个80比特的值v。

2.生成密文c=RC4（v||k）⊕m。

3.发送比特流(v||c).

（a）假设Alice用这个流程来给Bob发送信息，描述bob怎样能利用k从(v||c)中恢复信息m。

（b）如果攻击者观察到Alice和Bob之间传输的数值(v1||c1)，(v2||c2).....他怎样决定什么时候相同的密钥流已经被用来加密两个信息？

（a） $m = RC4(v||k) \oplus c$

$= RC4(v||k) \oplus RC4(v||k) \oplus m$

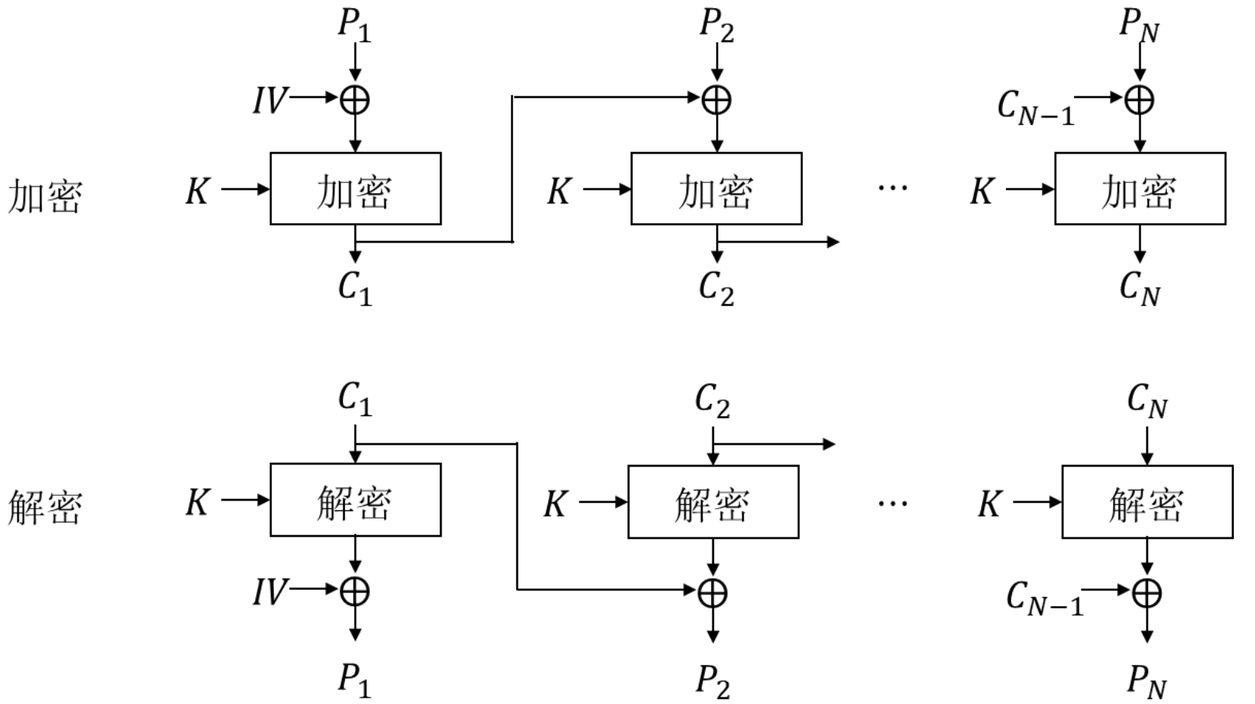
（b） $v_i = v_j,\ i \neq j$

习题2.12

什么是ECB(电码本)模式，如果传输密文的一个分组出错，只有对应的明文分组受影响。但是利用CBC(密文分组链接)模式，会传播错误。例如在图2.9中，传输的C1中的错误显然会破坏P1和P2.

a. 除P2之外，还有其他分组受影响 吗？ 无影响

b. 假设在P1的源版本中会有1比特错误。此错误会传播多少密文分组？接收端所受的影响是什么？传播所有密文分组；接收端除p1出错外无影响。



CBC模式操作过程

习题2.14

假设在使用CBC传输的密文块中发生错误，对恢复的明文块产生什么影响？

会影响当前分组和下一分组，对其他分组则没有影响

习题2.15

CBC-Pad是RC5分组密码使用的分组密码操作模式，但是它能在任何分组密码中使用。CBC-Pad处理任何长度的明文，密文最多比明文长一个分组。填充字节用来保证明文输入是分组长度的倍数。这假设了原始明文是整数个字节。明文在末尾添加的字节数可以为1到bb，其中bb等于以字节表示的分组的大小。填充的字节都相等并设为一个代表填充字节数的字节。例如，如果添加了8个字节，每个字节的比特表示为00001000。为什么不允许添加0字节？即如果原始明文是分组大小的整数倍，为什么不会避免进行填充。

如果允许添加0字节，当明文正好是整数个字节的话，可能会产生歧义。例如最后一个字节是00000001，会被认为是填充了一个字节。

习题 2.18

如果以8比特CFB模式传输密文字符时发生了1比特的错误，错误会传播多远？

s=8, b=64

一旦某位数据出错,会影响目前和其后64/8=8个分组的数据，总计影响9个分组。

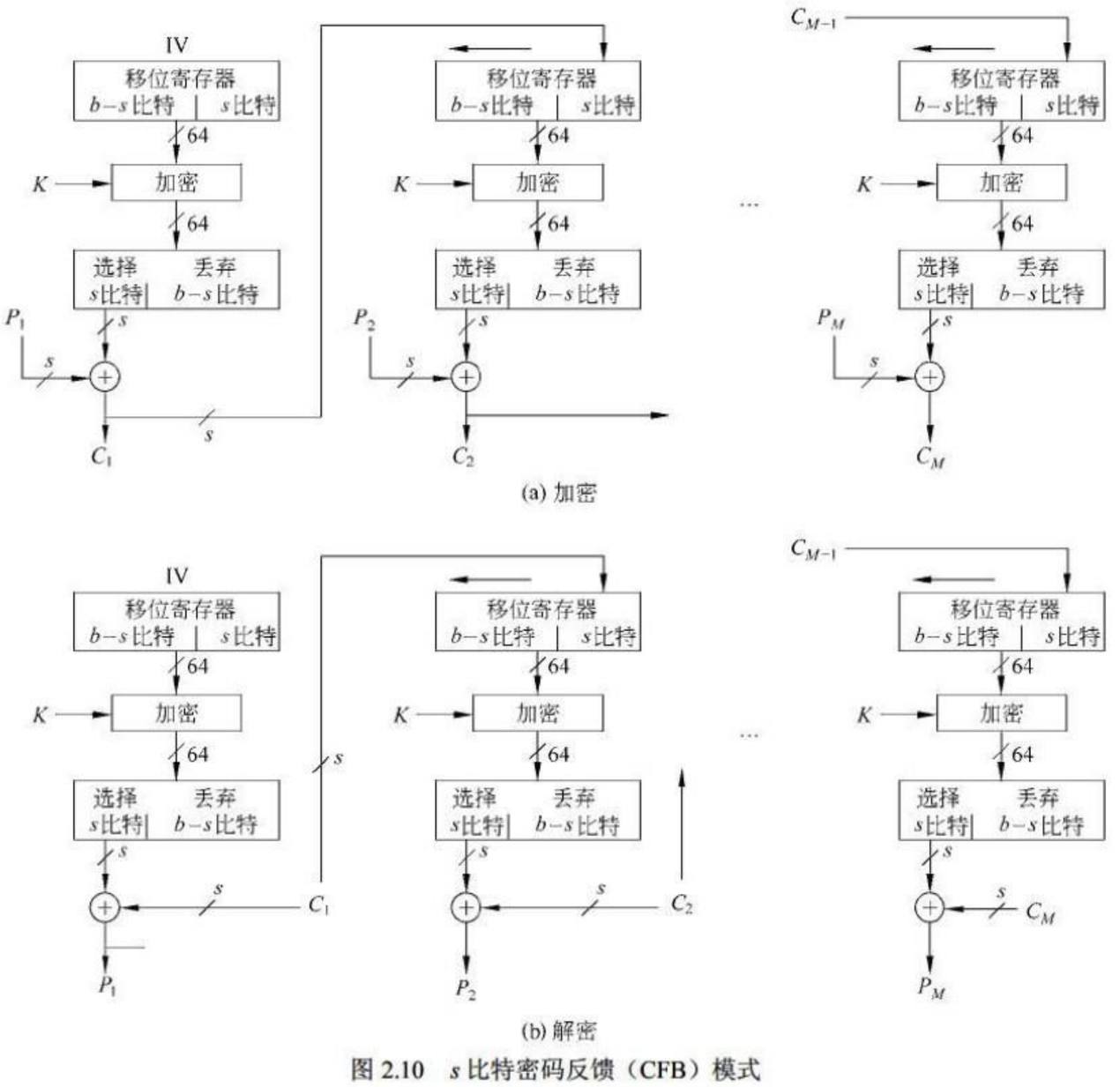


图 2.10 s 比特密码反馈（CFB）模式

补充题

给出PPT中分组密码的5种工作模式的解密数学表示方法：

ECB、CBC、CFB、OFB、CTR

ECB解密 输入：$C_1, C_2, \cdots, C_N$；输出：$P_1, P_2, \cdots, P_N$

$$P_i = \mathrm{D}(K, C_i), i = 1,2, \cdots, N$$

CBC解密 输入：$IV, C_1, C_2, \cdots, C_N$；输出：$P_1, P_2, \cdots, P_N$

$$C_0 = IV$$

$$P_i = C_{i-1} \oplus \mathrm{D}(K, C_i), i = 1,2, \cdots, N$$

CFB解密 输入：$IV, C_1, C_2, \cdots, C_N$；输出：$P_1, P_2, \cdots, P_N$

$$I_1 = IV$$

$$I_i = \mathrm{LSB}_{b-s}(I_{i-1}) || C_{i-1}, \quad i = 2, \cdots, N$$

$$O_i = \mathrm{E}(K, I_i), \quad i = 1,2, \cdots, N$$

$$P_i = C_i \oplus \mathrm{MSB}_s(O_i), \quad i = 1,2, \cdots, N$$

OFB解密 输入：$IV, C_1, C_2, \cdots, C_N$；输出：$P_1, P_2, \cdots, P_N$

$$I_1 = IV$$

$$I_i = \mathrm{LSB}_{b-s}(I_{i-1}) || \mathrm{MSB}_s(O_i), \quad i = 2, \cdots, N$$

$$O_i = \mathrm{E}(K, I_i), \quad i = 1,2, \cdots, N$$

$$P_i = C_i \oplus \mathrm{MSB}_s(O_i), \quad i = 1,2, \cdots, N$$

CTR解密 输入：$Ctr_1, C_1, C_2, \cdots, C_N$；输出：$P_1, P_2, \cdots, P_N$

$$P_i = C_i \oplus \mathrm{E}(K, Ctr_i), \quad i = 1,2, \cdots, N$$

思考题3.1

列举消息认证的几种方法

- 可用来做认证的函数有三类：
  - (1) 加密函数
    - 用对称密钥加密，信息的完整作为对信息的认证
    - 用公钥密码中的私钥加密，但加密速度太慢，并且很多情况下，消息并不需要加密。
  - (2) 消息认证码MAC (Message Authentication Code)

    是对信源消息的一个编码函数,以消息和密钥作为输入，定长输出
  - (3) 散列函数 (Hash Function)

    是一个公开的函数它将任意长的信息映射成一个固定长度的信息，需要结合公钥签名一起使用。

思考题3.9

什么是数字签名

公钥密码学的一个重要应用就是数字签名，数字签名就是利用私钥生成签名，而用公钥验证签名。

- 一个数字签名方案时是由签名算法和验证算法组成
  - 签名算法利用私钥生成签名，称消息m的签名为sig（m），然后将（m，sig（m））发给接收方
  - 验证算法利用签名者的公钥对sig（m）进行解密，如果解密输出与m一致，则为合法数据。
- 由于无法识别数字签名与其拷贝之间的差异，所以，在数字签名前应加上时间戳。
- 数字签名标准（DSS）
  - DSA（数字签名算法，是Elgamal公钥算法的一种变体）
  - RSA

习题3.5

a. 考虑下面的散列函数。消息是一列十进制数字：M=$(a_1,a_2,\ldots,a_t)$。对于某一预先定义的值n，计算散列值h：$\left(\sum_{i=1}^{t} a_i\right) \bmod n$。该散列函数能满足3.4节列出的关于散列函数的一些要求吗？

b. 散列函数为$h = \left(\sum_{i=1}^{t} (a_i)^2\right) \bmod n$时，重做(a)

c. 当M=(189,632,900,722,349)和n=989时，计算(b)的散列函数

a.满足前三个要求,不满足后三个要求
b.满足前三个要求,不满足后三个要求
c. 229

（1）H可适用于任意长度的数据块。

（2）H能生成固定长度的输出。

（3）对于任意给定的x，计算$H(x)$相对容易，并且可以用软/硬件方式实现。

（4）对于任意给定值h，找到满足$H(x)=h$的x在计算上不可行。满足这一特性的散列函数称为具有**单向性**，或具有**抗原像攻击性**[3]。

（5）对于任意给定的数据块x，找到满足$H(y)=H(x)$的$y \neq x$在计算上是不可行的。满足这一特性的散列函数被称为具有**抗第二原像攻击性**，有时也称为具有**抗弱碰撞攻击性**。

（6）找到满足$H(x)=H(y)$的任意一对(x, y)在计算上是不可行的。满足这一特性的散列函数被称为**抗碰撞性**，有时也被称为**抗强碰撞性**。

习题3.14

对下列值使用RSA算法进行加密和解密：

a. p=3, q=11, e=7, M=5;
b. p=5, q=11, e=3, M=9;
c. p=7, q=11, e=17, M=8;
d. p=11, q=13, e=11, M=7;
e. p=17, q=31, e=7, M=2。

（a）C=14，M=5；
（b）C=14，M=9；
（c）C=57，M=8；
（d）C=106，M=7；
（e）C=128，M=2

- **A. 密钥的生成**
  - 选择p, q， p, q为互异素数，计算n=p*q, φ(n)=(p-1)(q-1), 选择整数e与φ(n)互素，即gcd(φ(n),e)=1,1<e<φ (n) 计算d,使d=e^{-1}(modφ (n)),公钥Pk={e, n}; 私钥Sk={d, n}
- **B. 加密 (用e, n)，**
  - 明文是以分组方式加密的，每一个分组的比特数应小于n的二进制表示，即每一个分组的长度应小于$\log_2 n$
  - 明文M<n， 密文C=M^e(mod n).
- **C. 解密 (用d, n)**
  - 密文C， 明文M=C^d（mod n)

习题3.15

在使用RSA的公钥系统中，你可截获发送给用户的密文C=10，并且已知它的公钥是e=5,n=35。明文M是什么？

M=5

习题 3.16

对于RSA系统，某用户的公钥为：e=31, n=3599。该用户的私钥是什么？

n=3599=59*61， d=3031

习题 3.17

假设有一使用RSA算法编码的数据块集合，但是没有私钥。设n=pq, e是公钥。假设某人告诉我们这些明文块之一与n有公共因子。这对我们有帮助吗？

有帮助。对这些明文块与n求最大公因子。N=pq只有两个因子，那么其最大公因子就是p、q中的一个。求出最大公因子p后，就能求出另一个因子q。 继而求出私钥。

$$\varphi(n) = (p-1)(q-1)$$
$$ed \equiv 1 \bmod \varphi(n)$$
$$d = e^{-1}$$

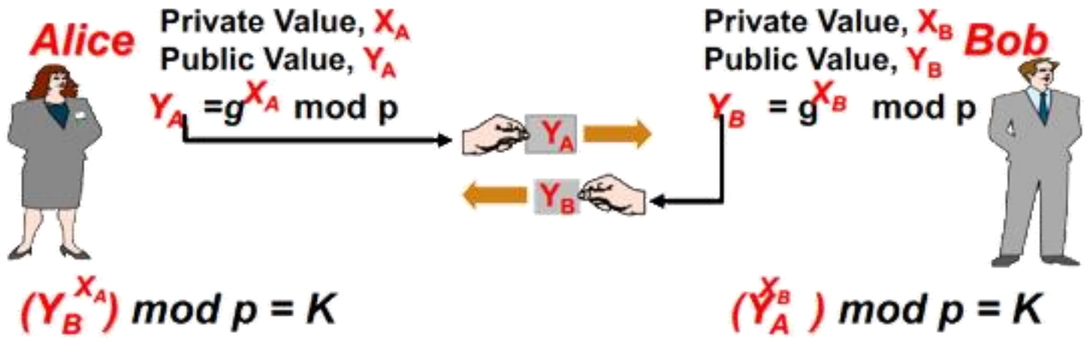
公钥： n：两个大素数 p 与 q 的乘积 e：与 $\Phi(n) = (p-1)(q-1)$ 互素 私钥： d：$d = e^{-1} \pmod{\Phi(n)}$	加密算法： $c = m^e \pmod{n}$ 解密算法： $m = c^d \pmod{n}$

习题 3.20

假设Bob用模n很大的RSA加密系统。该模值在合理的时间内不能进行因式分解。假设Alice给Bob发送一条把每个数字对应成0~25整数（A→0，…，Z→25）的消息，然后再用具有大的的e、n值的RSA分别加密每个数。这种方法安全吗？如果不安全，给出对这种加密方法最有效的攻击。

相当于单表代换加密：将每个明文字母替换为一个数字

可以通过字频统计攻击破解



习题 3.21

考虑公共素数q=11和本原根$\alpha = 2$的Diffie-Hellman方案。

a. 如果用户A有公钥$Y_A = 9$，请问A的私钥X_A是什么？ 由 $Y_A = \alpha^{X_A}$可得 X_A=6

b. 如果用户B有公钥$Y_B = 3$，请问共享的秘钥K是什么？ $K = (\alpha^{X_B})^{X_A} \bmod q = Y_B^{X_A} \bmod q = 3$

第二次作业

如何在通信双方间协商一个会话密钥

- 基于对称加密：通过选择一个密钥分发中心，为通信双方提供一个会话密钥。如Kerberos认证协议
- 基于非对称加密：包括Diffie-Hellman密钥交换，数字信封

什么是随机数？基于已学课程大致描述随机数的作用？

- 一种统计上独立且无偏的二进制数字序列
- 作为分组密码技术中的密钥
- 作为流密码技术中的密钥或密钥流
- 用于产生公钥密钥算法中的大素数、私钥等，如RSA中p和q的选取
- 用于认证协议中防止重放攻击

思考题4.8

与密钥分发有关的公钥密码的两个不同用处是什么？

1.公钥的分发（公钥证书）

2.使用公钥加密分发私钥（数字信封，D-H密钥交换）

思考题4.10

什么是公钥证书？

公钥证书由公钥、公钥所有者的主体身份信息、可信第三方的签名这样的整个数据块组成。

思考题4.12

X.509标准的目的是什么？

X.509：是ISO和CCITT/ITU-T的X.500标准系列中的一部分，为了**解决X.500目录中的身份鉴别和访问控制问题**而设计的。同时本身也采用目录的形式进行管理和访问。在X.509中采用了大量的篇幅来定义证书和CRL的数据格式。

思考题4.14

怎样撤销X.509证书

撤销阶段：密钥/证书生命周期管理以撤销阶段来结束。

此阶段包括如下内容：

- 证书过期——证书生命周期的自然结束
- 证书撤销——证书在过期之前被撤销。比如私钥泄露、关系终止、CA签名私钥泄露或者变更等
- 存档——维持一个CRL和有关历史证书的记录（一般是关于终端实体的），以便被过期的密钥资料所加密的数据能够被解密
- 审计信息——出于对密钥历史恢复、审计和解决争议的考虑所进行的密钥资料的安全第三方长期储存

习题4.5

为了给公钥证书提供一种标准格式，X.509 中规范了一种认证协议。X.509 的原始版本包含了一个安全流程。这个协议的实质如下：

$A \rightarrow B:$ $A\{t_A, r_A, ID_B\}$ 发起

$B \rightarrow A:$ $B\{t_B, r_B, ID_A, r_A\}$ B向A证明身份

$A \rightarrow B:$ $A\{r_B\}$ A向B证明身份

这里，t_A 和 t_B 表示邮戳，r_A 和 r_B 是随机数，而符号 X{Y}表示消息 Y 通过 X 签名、加密和传输。

X.509 的内容指出：在三向认证中，检查时间戳 t_A 和 t_B 是可选的。但是考虑以下的例子：假定 A 和 B 在以前使用上面的协议，然后攻击者 C 截获了前面的三条消息。另外，假定时间戳未被使用而均被设定为 0。最后，假定 C 希望对 B 假扮 A。C 首先向 B 发送第一条被截获的消息：

$C \rightarrow B:$ $A\{0, r_A, ID_B\}$

B 做出应答，以为它在与 A 对话，而实际上是与 C 对话：

$B \rightarrow C:$ $B\{0, r'_B, ID_A, r_A\}$

C 其间通过某种方式使得 A 发起 C 的认证。结果，A 向 C 发送：

$A \rightarrow C:$ $A\{0, r'_A, ID_C\}$

C 使用与 B 提供给 C 相同的随机数应答 A：

$C \rightarrow A:$ $C\{0, r'_B, ID_A, r'_A\}$

A 应答：

伪造身份

$A \rightarrow C:$ $A\{r'_B\}$

这正是 C 需要使 B 确认它在与 A 进行对话的信息，所以 C 现在将此到来的消息重发给 B：

$C \rightarrow B:$ $A\{r'_B\}$

所以 B 将确信它正在与 A 对话，而实际上它是在与 C 对话。提出一种对于这个问题的简单解决方案，在这个方案中不要使用时间戳。 攻击结果：C伪装A与B对话

思路：在最后一步使A应该发给B和C的是不同的内容，则C无法伪装成A

方案：在认证的最后一步加上关于B的信息

$$A->B: A\{0, r_a, ID_B\};$$

$$B->A: B\{0, r_B, ID_A, r_A\};$$

$$A->B: A\{E(PU_B, r_B)\}$$

$$A->C: A\{E(PU_C, r_B)\}$$

$$C->B: A\{E(PU_B, r_B)\}$$

无法计算，因为C没有A的私钥

习题4.6

考虑基于非对称加密技术的单向认证：

$A \rightarrow B: ID_A$

$B \rightarrow A: R_1$

$A \rightarrow B: E(PR_a, R_1)$

a.解释协议。

b.协议易受什么类型的攻击？

a. A向B认证自己的身份：

- A向B表明自己的ID是ID_A；
- B给A一个随机数；
- A用自己的私钥签名随机数，表明自己的身份；

b. 容易受到中间人攻击；C向B假冒A。

习题4.7

考虑基于非对称加密技术的单向认证：

$A \rightarrow B: ID_A$

$B \rightarrow A: E(PU_a, R_2)$

$A \rightarrow B: R_2$

a.解释协议。

b.协议易受什么类型的攻击？

a. A向B认证自己的身份：

- A向B证明自己的ID是ID_A
- B用A的公钥加密随机数R2给A
- A用自己私钥解密得到R2发送给B证明自己的身份

b.中间人攻击；C向B假冒A。

习题4.15

考虑下列协议，它让 A 和 B 决定一个新鲜共享的对话密钥 K'_{AB}，假设它们已经共享了一个长期密钥 K_{AB}：

（1）A→B: A, N_A A发送随机数

（2）B→A: E(K_{AB},[N_A, K'_{AB}] B产生新密钥并发送

（3）A→B: E(K'_{AB}, N_A) A向B确认新密钥

a. 我们首先要理解协议设计者的理由：

- 为什么 A 和 B 认为他们可以通过这个协议和对方共享 K'_{AB}。
- 为什么他们相信共享的密钥是新鲜的。

在两种情况中，你应该对 A 和 B 都进行解释，从而使你的回答可以完成下列句子

A 认为她和 B 共享是 K'_{AB} 因为……

B 认为她和 A 共享是 K'_{AB} 因为……

A 认为 K'_{AB} 是新鲜的因为……

B 认为 K'_{AB} 是新鲜的因为……

b. 假设 A 开始和 B 使用这个协议，然而通信被 C 截获。说明 C 如何利用反射开始新的协议，使得 A 认为她已经同意了和 B 使用新鲜的密钥（尽管实际上她只是和 C 进行了通信），从而使得 a 中的理由是错误的。

c. 提出一个改进的协议使得其可以避免这种攻击。

a. 1) 因为A用旧密钥K_{AB}解密B发送的消息得到了新密钥K'_{AB}

2) 因为B收到A用新密钥加密的N_A

3) 因为B在应答(2)中包含了A给B的随机数，并且使用共享密钥 K_{AB} 加密；

4) 新密钥是由B指定的，B使用新密钥解密(3)可得到N_A

b. $\alpha : A -> C : A, N_A$

$\beta : C -> A : B, N_A$

$\beta : A -> C : E\{K_{AB}, [N_A, K_{AB}']\}$

$\alpha : C -> A : E\{K_{AB}, [N_A, K_{AB}']\}$

$\alpha : A -> C : E\{K_{AB}', N_A\}$

$\beta : C -> A : E\{K_{AB}', N_A\}$

c. 解决方案：加一个ID在(2)中。

$B -> A : E\{K_{AB}, [ID_A, N_A, K_{AB}']\}$

有同学回答说从第一步开始加密，但是这种情况B无法判断使用和谁通信的秘钥来解密消息

习题4.16

PKI的核心部分是什么？简要描述每个部分(P100， PPT 9-10)

认证中心CA（Certificate Authority） 证书的签发机构，它是PKI的核心构件，是PKI应用中权威的、可信任的、公正的第三方机构。

注册机构RA（Registration Authority）注册功能也可以由CA直接实现，但随着用户的增加，多个RA可以分担CA的功能，作为CA的延展，可以增强可扩展性。按照特定的政策和管理规范对用户的资格进行审查，并执行是否同意给该申请人发放证书。撤销证书等操作，应注意的是RA不容许直接颁发证书或CRL。

证书库（Certification Library）CA颁发证书和证书撤销列表CRL的集中存放地，提供公众查询，常用目录服务器提供服务，采用LDAP（Lightweight Directory Access Protocol）目录访问协议。

习题4.18

考虑如下协议

A→KDC:	$ID_A \| ID_B \| N_1$
KDC→A:	$E(K_a, [K_S \| ID_B \| N_1 \| E(K_b, [K_S \| ID_A])$
A→B:	$E(K_b, [K_S \| ID_A])$
B→A:	$E(K_S, N_2)$
A→B:	$E(K_S, f(N_2))$

a. 解释这个协议。
b. 你能给出可能的攻击吗？解释他是如何完成的。
c. 提出一种可能的技术躲开那种攻击，不需要详细描述，只需说明基本思路。

a. A向KDC请求与B协商会话密钥K_S：

- A向可信第三方提交与B通信的请求。并附上一个随机数N_1；
- 可信第三方用与A协商好的密钥K_a加密临时会话密钥K_S，B的ID和随机数N_1，并用与B的私钥K_b加密临时会话密钥和A的ID。然后发送给A
- A将可信第三方给予的用K_a加密的消息部分给B；
- B解密后得到会话密钥K_S，并用其加密随机数N_2给A（为了确认A有会话密钥）
- A用会话密钥解密N_2并加密$f(N_2)$证明自己有K_S且会话密钥是K_S.(确认会话密钥有效)

b. 可能的攻击：旧会话密钥泄露攻击，攻击者C获取了以前的某次会话密钥K_S^*并保存$E(K_b,[K_s^* \| ID_A])$ B会以为与A建立了安全通道。

$$(3) C->B: E(K_b,[K_s^* \| ID_A])$$

$$(4) B->C: E(K_s^*, N_2)$$

$$(5) C->B: E(K_s^*, f(N_2))$$

c. 解决方法：$E(K_b,[K_s^* \| ID_A])$ 中加时间戳，B收到后解密验证时间的有效性。

答案合理即可。

Kerberos相关（第六版书P86）

版本4，C→V：$\text{Ticket}_V || \text{Authenticator}_C$

$$\text{Ticket}_V = E(K_V, [K_{C,V} || ID_C || AD_C || ID_V || TS || Lifetime])$$

V→C：$E(K_{C,V}, [TS + 1])$

习题4.8　Bob收到Alice发送的票，他如何确定真伪？

Ticket_B用K_B加密，K_B只由Bob和TGS知道。

习题4.9　Bob收到Alice发送的票，他如何确定票来自Alice？

Ticket_B有ID_A和AD_A

习题4.10 Alice接收到回复，如何确定来自Bob？

时间戳使用$K_{A,B}$加密

习题4.11 票的什么信息能够保证两人的秘密通信？

K_B加密的共享的会话密钥$K_{A,B}$

第三次作业

思考题 9.2

IPSec提供哪些服务？（写书上RFC 4301列举的也可以）

AH协议提供无连接的数据完整性、数据源认证和抗重放保护服务

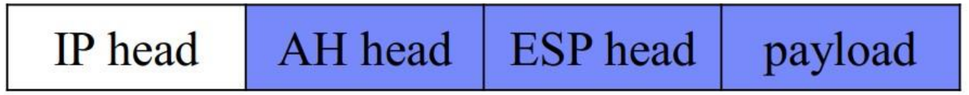
ESP提供数据保密、无连接完整性（可选，不覆盖IP头标）、数据源认证、抗重放攻击

思考题 9.4

传输模式和隧道模式有何区别？

传输模式主要为上层协议提供保护；隧道模式对整个IP包提供保护

- 传输模式



  - 在传输模式中，AH和ESP头标被插在IP头标及其他选项（或扩展头标）之后，但在传输层协议之前。它保护净荷的完整性和机密性。

- 隧道模式

  - 在隧道模式下，AH或ESP头标插在IP头标之前，另外生成一个新的IP头放在前面，隧道的起点和终点的网关地址就是新IP头的源/目的IP地址。
  - 保护整个IP分组

思考题9.5

什么是重放攻击，在IPSec AH和ESP中怎么防止重放攻击？

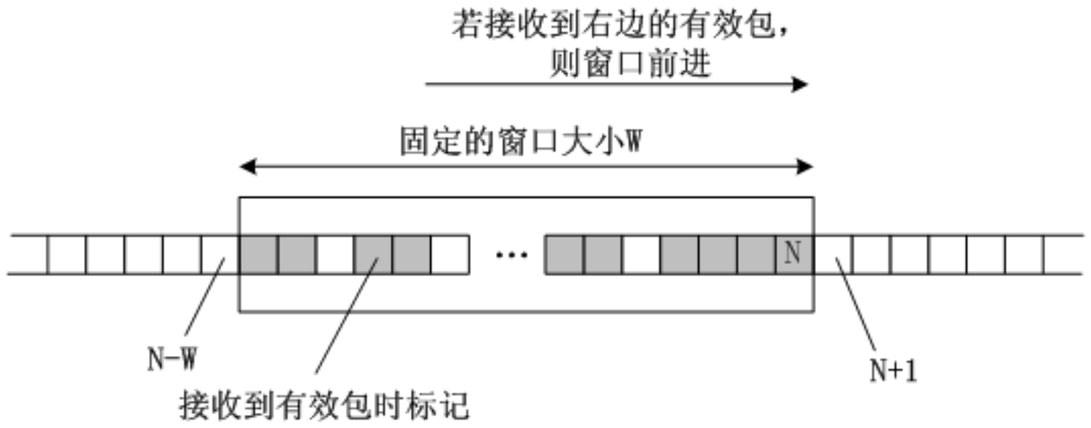
1)重放攻击是一个攻击者得到了一个经过认证的包的副本，稍后又将其传送到其希 望被传送到的目的站点的攻击

2)防止：在IPSec中发送方**为每一个包附上一个序号**；接收方实现一个大小为W的窗

口，窗口的右端代表最大的序列号N，记录目前收到的合法包的最大序列号，序列号在（N-W+1）~N的包被接收并再相应位置标记。

接收方具体操作：

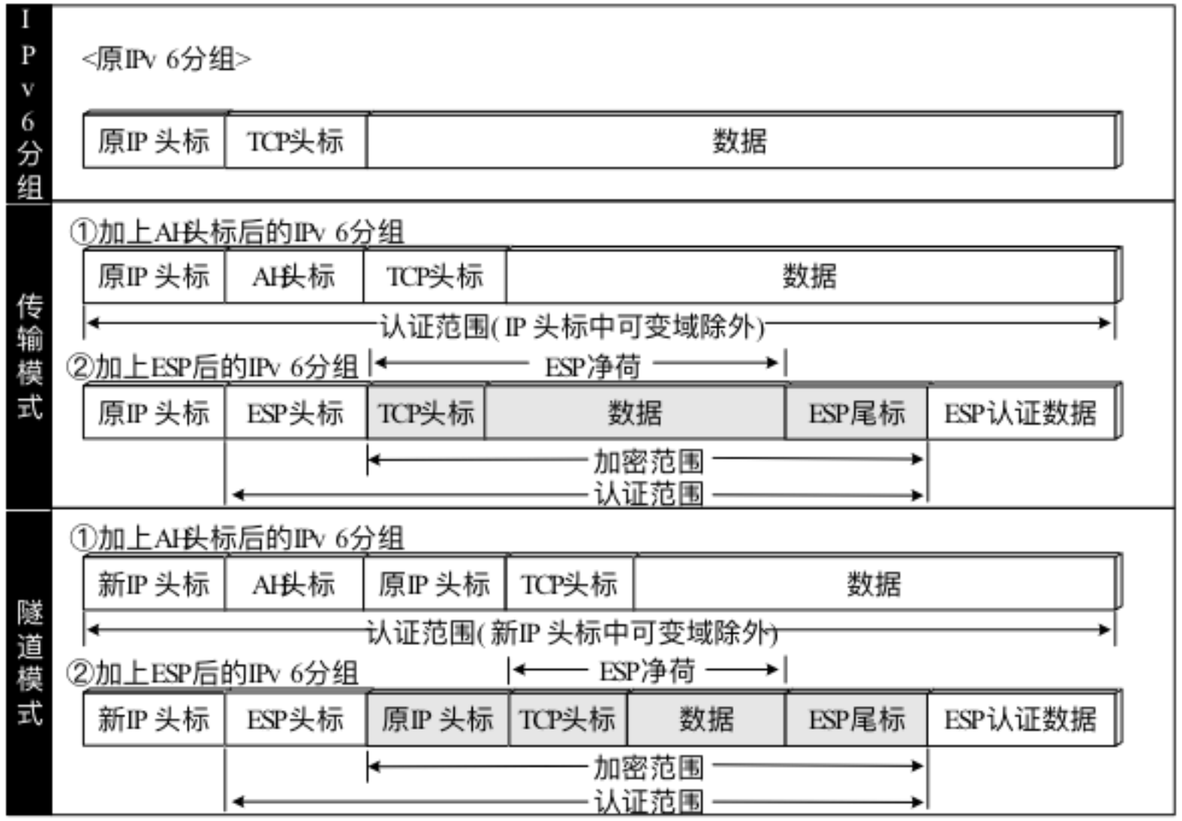
- 接收到包含在窗口中的新包，且验证通过，则直接进行标记；
- 接收包超过了窗口右边界，且验证通过，则窗口右移，使得新包成为右边界；
- 接收包超过了左边界或者没有通过验证，丢弃该包。



思考题 9.6 为什么ESP包含一个填充域？(PPT P34)

（1）加密算法要求明文为某个数目字节的整数倍；
（2）32位对齐；
（3）隐藏实际载荷长度，提供流量保密性

习题9.2 对AH画一个类似于图9.8的图



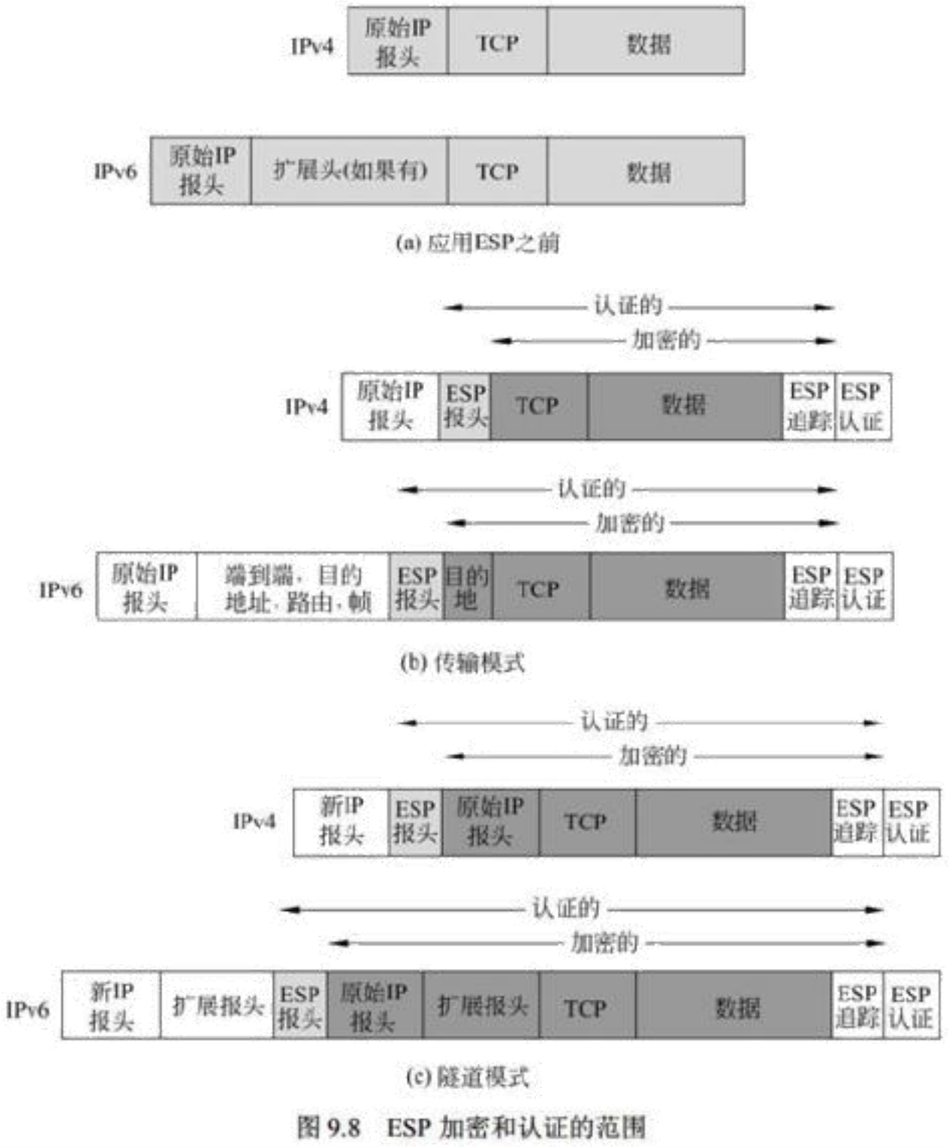


图 9.8 ESP 加密和认证的范围

习题 9.3

分别列出AH和ESP提供的主要安全服务。

- AH协议提供无连接的完整性、数据源认证和抗重放保护服务
- 不提供保密性服务
- AH使用消息认证码（MAC）对IP进行认证

- ESP提供数据保密、无连接完整性、抗重播服务
- ESP大都采用对称密码体制加密数据
- ESP使用消息认证码（MAC）提供认证和完整性保护服务

习题 9.4b

指明在IPv6报头的所有域中，哪些是不可变的，哪些是可变但可预测的，哪些是可变的(0优先级ICV计算)？

不可变:：Version, Payload Length, Next Header (This should be the value for AH.), Source Address, Destination Address (without Routing Extension Header)
可变但可预测：Destination Address (with Routing Extension Header)
可变：Class, Flow Label, Hop Limit

习题9.5

假设当前的重放窗口由120扩展到530：

a.如果下一个进来的已认证包有序列号105，则接收 者需如何处理该包？处理后的窗口参数是什么？

b.如果下一个进来的已认证包有序列号是440，则接 收者又当如何处理？处理后的窗口参数又是什么？

c.如果下一个进来的已认证包有序列号是540，则接 收者又当如何处理？处理后的窗口参数又是什么？

a.丢弃；窗口不变；

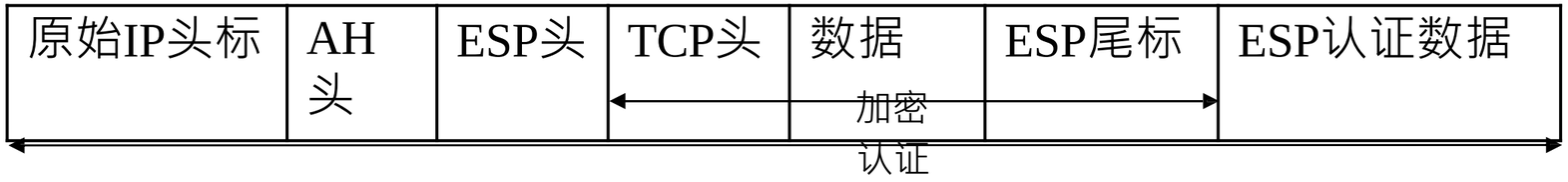
b.标记，窗口不变

c.接受，窗口右移。参数130~540

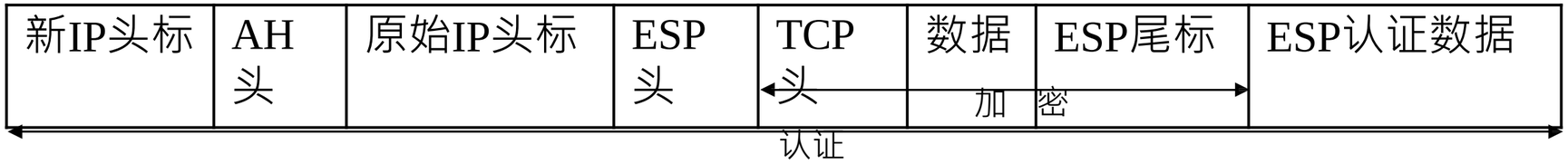
习题 9.7

在两个主机之间需要实现端对端加密和认证，请画出示意图说明：

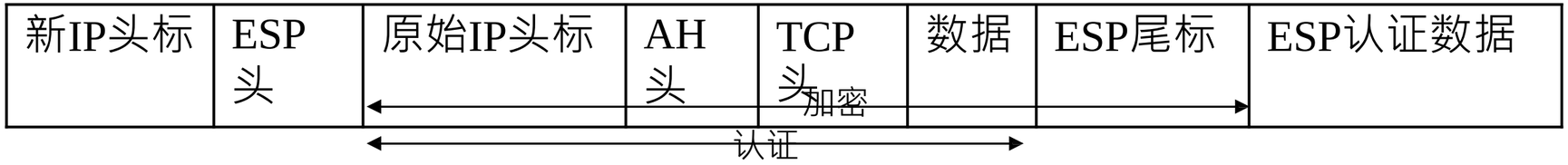
a.传输邻接，先加密后认证



b.一个隧道SA中有一个传输SA，先加密后认证



c.一个隧道SA中有一个传输SA，先认证后加密



习题9.8

IPSec的体系结构文档规定：当两个传输模式的SA被捆绑在一起以允许AH协议和ESP协议可以在同一个端对端流中实现时，仅有一个顺序看起来是较为合理的-----先执行ESP协议再执行AH协议。请问：为什么推荐这种顺序而不是先认证后加密？

在解密前对包进行筛选，减少计算开销

网络安全协议习题课
第 5 至 9 章

黄轩博

2021 年 6 月

第六章思考题

Q 思考题6.1: 图 6.1 三种方案各有什么优点？ P135

1. **网络层（IPSec）**：对用户和应用程序是透明的，且提供了广泛的安全性。
2. **传输层（TLS）**：可以充分利用 TCP 协议可靠到达和流控制机制。更加灵活。
3. **应用层（Kerberos、S/MIME）**：可以满足不同应用和应用场景自身的需要。

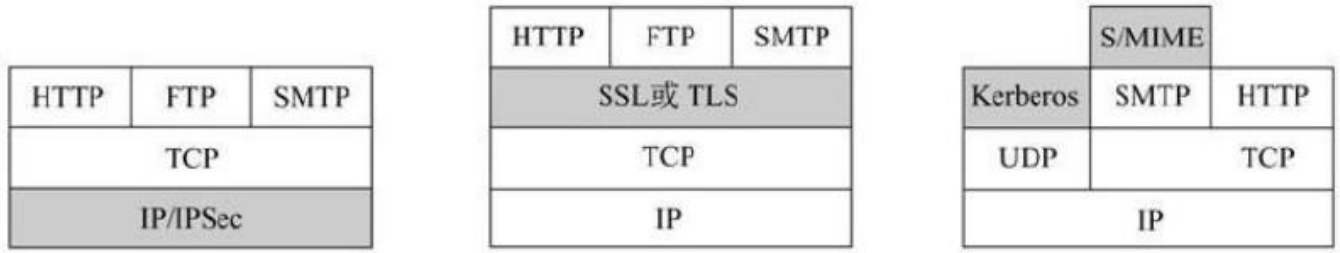


图 6.1 TCP/IP 协议栈中的安全设施的相对位置

Q 思考题6.2: SSL 协议由那些协议组成？ P136

- Record Protocol
- Handshake Protocol
- Change Cipher Spec Protocol
- Alert Protocol
- (Application Data)

Q 思考题6.3: SSL 连接和 SSL 会话直接的区别？ P136

连接：一种提供合适服务类型的传输。对于 SSL 来说这种点对点连接是短暂的。每一条连接都与一条会话相关联。

会话：是客户端和服务器之间的一种关联。通过握手协议相关联，并定义了密码安全参数关联。这些参数在多个连接中共享。通过使用会话重用机制来减少多次连接中协商密码学参数的额外开销。

Q 思考题6.6: SSL 记录协议提供哪些功能？ P137

SSL 记录协议为SSL 连接提供如下两种服务：

1. 机密性：握手协议定义一个用于加密上层载荷的加密秘钥
2. 完整性：握手协议定义一个提供完整性保护的完整性秘钥

Q 思考题6.7: SSL 记录协议执行了那些过程？ P137

1. 分段（将上层消息分割为不大于 2^14-byte 的块
2. 压缩（默认为空算法）
3. 添加 MAC（完整性保护）
4. 加密（机密性保护）
5. 添加 SSL 记录协议头

第六章习题

Q 习题6.3:考虑下面 Web 威胁，并说明 SSL协议是如何提供保护的?

Web 安全威胁	对应提供保护的 SSL 特性
穷举密码攻击	使用秘钥空间更大的加密算法和消息验证码，最新的 TLSv1.3 中，最低的加密秘钥空间是 128 bit（TLS_AES_128_GCM_SHA256）。
已知明文字典攻击	加密算法使用 IV 初始向量，使得同样的明文和秘钥能够产生不同的密文。
重放攻击	握手协议中包括了随机数 N 和时间戳。
中间人攻击	在 Key Exchange 的基础上，需要对双方或者单方进行身份认证（通常是 X.509 证书认证)
口令窃听	对载荷数据进行了加密，防止窃听 HTTP 报文中的口令
IP 地址假冒	TCP 协议需要进行三次握手来建立连接，可以防止原地址冒充攻击
IP 劫持	TLS 在进行认证的基础上，协商出了秘钥，防止 IP 劫持攻击
SYN 泛滥	TLS 协议不提供该保护

Q 习题6.4: SSL 能对接受到的无序 SSL 记录协议进行重排吗?

不行，SSL 依赖与 TCP 协调提供的可靠传输，自身不提供流控制和重排技术。

补充题：在可出口的 SSLv3 中，有流程是将 40 bit 短秘钥、结合两个随机值进行 hash 运算得到 128 bit 的秘钥（见 PPT 24 页）。这种方法具有什么优点？破解单个会话需要多少个秘钥?

这种方案的好处是保证了兼容性，使得SSL 协议无需很大改变，就能用于出口。
注意随机数是在 client_hello 和 server_hello 报文中明文传输的，此时秘钥空间依旧是 2^40。也就是需要 2^40 次尝试进行破解。

第七章思考题

Q 思考题12.4: 包过滤防火墙有哪些弱点？ P305

1. 不能检查更高层数据，不能阻止利用了特定应用漏洞的攻击
2. 可利用的信息有限，日志记录功能业有限
3. 不支持高级的用户认证功能
4. 对利用 TCP/IP 协议栈的攻击，不能很好的防御（比如 IP 原地址冒充）
5. 不恰当的设置可能导致安全性容易受到威胁

Q 思考题12.5: 包过滤防火墙和状态监测防火墙的区别是什么？ P307

状态监测防火墙和包过滤防火墙检查的信息相同，通时还记录了有关 TCP 连接的相关信息。

Q 思考题12.6: 什么是应用层网关?

也称为代理服务器，起到了应用层流量缓冲的作用，通常情况下，网关进行身份认证并建立与远程主机直接的连接。

Q 思考题12.7: 什么是链路层网关?

也称为链路层代理，此网关建立两个 TCP 连接。一个典型的例子是 SOCKSv5 协议。

Q 思考题12.11: 什么是 DMZ 网关?

位于外部防火墙和内部防火墙之间的区域，对外提供可接入但是需要保护的系统。

Q 思考题12.12: 内部防火墙和外部防火墙的区别是什么?

外部防火墙连在WAN上，内部防火墙保护企业内网

Q 习题12.4: 描述表 12.3 中的规则

1. 允许放行发往 192.168.1.0 大于 1023 端口的报文
2. 拒绝 192.168.1.1 发出的全部报文
3. 拒绝发往 192.168.1.1 的全部报文
4. 放行从 192.168.1.0 发出的全部报文
5. 允许发往 192.169.1.2 25 端口的 TCP 报文
6. 允许发往 192.168.1.3 80 端口的 TCP 报文
7. 拒绝其他不匹配的报文

表 12.3 包过滤规则集

	源地址	源端口	目的地址	目的端口	动 作
1	任意	任意	192.168.1.0	>1023	允许
2	192.168.1.1	任意	任意	任意	拒绝
3	任意	任意	192.168.1.1	任意	拒绝
4	192.168.1.0	任意	任意	任意	允许
5	任意	任意	192.168.1.2	SMTP	允许
6	任意	任意	192.168.1.3	HTTP	允许
7	任意	任意	任意	任意	拒绝

Q 习题12.5 (a): 描述每条规则的作用

1. A、B 允许发往内网的 SMTP 连接
2. C、D 允许发往外网的 SMTP 连接
3. E 拒绝其他任意连接

规则	方向	源地址	目的地址	协议	目的端口	动作
A	进	外部	内部	TCP	25	允许
B	出	内部	外部	TCP	>1023	允许
C	出	内部	外部	TCP	25	允许
D	进	外部	内部	TCP	>1023	允许
E	进或出	任意	任意	任意	任意	拒绝

Q 习题12.5 (b): 下面报文是否放行?

全部放行

包	方向	源地址	目的地址	协议	目的端口	动作
1	进	192.168.3.4	172.16.1.1	TCP	25	?
2	出	172.16.1.1	192.168.3.4	TCP	1024	?
3	出	172.16.1.1	192.168.3.4	TCP	25	?
4	进	192.168.3.4	172.16.1.1	TCP	1357	?

习题12.5 (C): 下面报文是否放行?

全部放行，规则 B 和 规则 D 放行了全部 1023 端口以上的进出流

包	方向	源地址	目的地址	协议	目的端口	动作
5	进	10.1.2.3	172.16.3.4	TCP	8080	?
6	出	172.16.3.4	10.1.2.3	TCP	5150	?

Q 习题12.6 (a) :为了提供更多的保护，将上题规则改动如下，描述规则的变化?

加入了对于源端口 25 的限制。

Q 习题12.6 (b) :此时上述 6 个包是否放行?

1-4 包允许放行；5-6 包拒绝访问

规则	方向	源地址	目的地址	协议	源端口	目的端口	动作
A	进	外部	内部	TCP	>1023	25	允许
B	出	内部	外部	TCP	25	>1023	允许
C	出	内部	外部	TCP	>1023	25	允许
D	进	外部	内部	TCP	25	>1023	允许
E	进或出	任意	任意	任意	任意	任意	拒绝

12.7 一名黑客使用端口 25 作为他或她的用户端口，想要开通一个连接到你的网络代理服务器。

a. 可能产生以下的包：

包	方向	源地址	目的地址	协议	源端口	目的端口	动作
7	进	10.1.2.3	172.16.3.4	TCP	25	8080	?
8	出	172.16.3.4	10.1.2.3	TCP	8080	25	?

解释一下利用上一题的规则集，攻击为什么会成功。

b. 当一个 TCP 连接刚建立时，在 TCP 头的 ACK 没有设置。随后，所有通过 TCP 连接发送的 TCP 头的 ACK 比特被设置。使用该信息改变上一题的规则集，使得刚刚描述的攻击不成功。

Q 习题12.7 (a) :

包 7允许放行，由 12.6 题中的规则 D 放行

包 8允许放行，由 12.6 题中的规则 C 放行

Q 习题12.7 (b):

ACK 被设置代表该 TCP 报文不是首个连接的报文。在规则中添加一列 ACK Set:

A、C、E：any；B、D：ACK 设置为 true

12.10 给你如下防火墙规则细节，可以由图 12.3 的防火墙执行：

（1）E-mail 通过防火墙在两个方向上使用 SMTP 进行发送，但必须经过 DMZ 信件网关的中继来进行头清理和内容过滤。外部 E-mail 必须指定给 DMZ 信件服务器。

（2）内部用户可以使用 POP3 或者 POP3S 从 DMZ 信件网关重获 E-mail，并认证自身。

（3）内部用户只能使用安全 POP3 协议从 DMZ 信件网关重获 E-mail，并认证自身。

（4）来自内部用户的网络请求（安全的和不安全的）允许通过防火墙，但必须通过 DMZ 网络代理以进行内容过滤（注意，对于安全请求是不可能的），用户必须用代理认证以便登录。

（5）来自因特网任意地方的网络请求（安全的和不安全的）允许到 DMZ 网络服务器。

（6）内部用户的 DNS 查询请求允许通过 DMZ DNS 服务器，向因特网查询。

（7）外部 DNS 请求由 DMZ DNS 服务器提供。

（8）DMZ 服务器上信息的管理和更新允许使用内部相关授权用户的安全连接（每个系统可能有不同的用户集）。

（9）从内部管理主机到防火墙的 SNMP 管理请求被允许，并且防火墙被允许发送管理陷阱到管理主机。

设计能够在外部防火墙和内部防火墙执行，并满足上述规则要求的合理的包过滤规则集（同表 12.1 相似）。

Q 习题12.10 外部网络

action	src	port	dest	port	flags	comment
permit	DMZ mail gateway	any	any	SMTP (25)		header sanitize
permit	any	any	DMZ mail gateway	SMTP (25)		content filtered
permit	any	any	DMZ mail gateway	POP3S (995)		user auth
permit	DMZ web proxy	any	any	HTTP/S (80,443)		content filtered, user auth
permit	DMZ DNS server	DNS (53)	any	DNS (53)		TCP & UDP
permit	any	DNS (53)	DMZ DNS server	DNS (53)		TCP & UDP
permit	any	any	any DMZ server	any	estab-lished	return traffic flow
deny	any	any	any	any		block all else

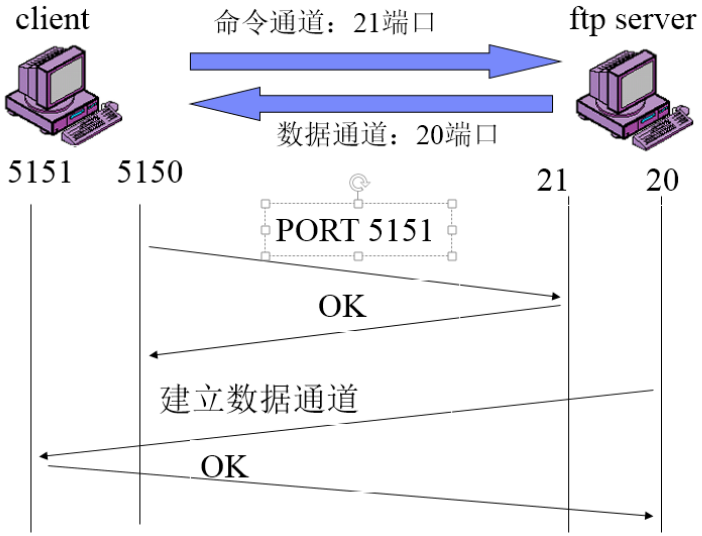
Q 习题12.10 内部网络防火墙

action	src	port	dest	port	flags	comment
permit	any internal	any	DMZ mail gateway	SMTP (25)		
permit	any internal	any	DMZ mail gateway	POP3/S (110,995)		user auth
permit	any internal	any	DMZ web proxy	HTTP/S (80,443)		content filtered, user auth
permit	any internal	DNS (53)	DMZ DNS server	DNS (53)		UDP lookup
permit	DMZ DNS server	DNS (53)	any internal	DNS (53)		UDP lookup
permit	any internal	any	any DMZ server	SSH (22)		user auth on server
permit	mgmt user hosts	any	any DMZ server	SNMP (161)		
permit	any DMZ server	any	mgmt user hosts	SNMP TRAP (162)		
permit	any DMZ server	any	any internal	any	estab-lished	return traffic flow
deny	any	any	any	any		block all else

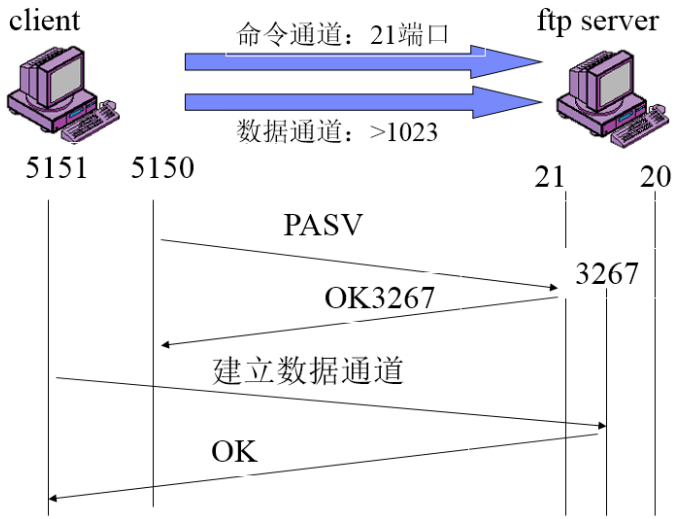
Q 补充题：FTP 在主动模式和被动模式下，经过状态监测防火墙的行为?

1. 主动模式：需要允许 in 方向的 x 端口的 TCP SYN 报文放行，需要防火墙与 FTP 服务器交换端口信息
2. 被动模式：只需要允许 out 方向建立连接的 TCP 报文放行即可

ftp文件传输协议（主动模式）



ftp文件传输协议(被动模式)



第八章思考题

Q 思考题8.3: MIME的内容类型和其传输编码之间的区别?

内容类型用于描述信息的表述方法，传输编码是内容使用的编码方案

Q 思考题8.4: 什么是 Base64 变换?

一种将二进制数据转化为 ASCII 字符的变换

Q 思考题8.5:为什么邮件要使用 Base64 变换?

由于如果使用加密或者签名，那么得到的原始输出是二进制数据。但是邮件协议只能传输 ASCII 字符。

第八章习题

8.2 POP3和IMAP是什么?

Post Office Protocol 3 和 Internet Mail Access Protocol 都能够让客户端下载服务器上的邮件。

8.3 无损压缩算法（zip）用于S/MIME，为什么在压缩前签名会更好?

签名后再压缩是为了方便保存未压缩的报文和签名，为了以后存储方便

8.7 PGP体制中，前一次会话密钥生成后，希望生成多少会话密钥?

8.8 具有N个公钥的用户至少有一个重复密钥ID的几率是多少?

密钥不重复的概率

$$P(N) = \frac{2^{64}}{2^{64}} * \frac{2^{64}-1}{2^{64}} * \frac{2^{64}-2}{2^{64}} \cdots * \frac{2^{64}-(N-1)}{2^{64}} = \frac{2^{64}!}{(2^{64})^N * (2^{64}-N)!}$$

至少一个重复的概率

$$1 - P(N)$$

第八章习题

8.9 PGP签名消息摘要中的前16bit是以明文的方式存在的，这能使得接收方通过比较这个明文的前两字节和解密后的摘要的前两字节来确定是否使用了正确的公钥解密消息摘要。

a. 这对散列算法的安全性带来了多大的威胁?

没有威胁

b. 这对其设计功能有多少帮助?

只需要验证前两个字节就可以知道是否使用了正确的公钥来解密消息。

使用错误的公钥但可以得到正确的两字节的概率等于2^{-16}

第九章思考题

Q 思考题7.7: 简要描述 802.11i 的四个阶段

1. 发现阶段：站点和网络接入点确认身份，协商安全参数、建立连接
2. 认证阶段：站点和分布式系统中的认证服务器进行相互认知
3. 秘钥管理阶段：产生一系列秘钥并分配秘钥到站点
4. 保密数据传输阶段：使用 TKIP 或者 CCMP 提供安全加密的传输

Q 思考题7.8: TKIP 和 CCMP 的区别:

加密算法、认证算法等不同。TKIP 只设计软件变更，为了给传统 WEP WiFi 设备提供兼容性。CCMP 安全性更强。

Q 习题 7.1：基于 MAC 地址的黑白名单的优势和安全性不足?

1. 优势：方案构建简单、可以防止非授权的节点接入
2. 安全性不足：要求节点诚实地工作。无法防止伪造 MAC 攻击。

Q 习题 7.2：

a) WEB 认证实体方案的优势?

方案简单，挑战应答机制可以证明 STA 拥有 PSK

b) 认证是否完整?

认证是单项的 STA 也需要知道 AP 是否拥有 PSK。

可以添加面向 AP 的挑战应答

c) 方案的缺陷是什么?

提供了广泛的明文密文对进行密码分析和一直明文攻击。

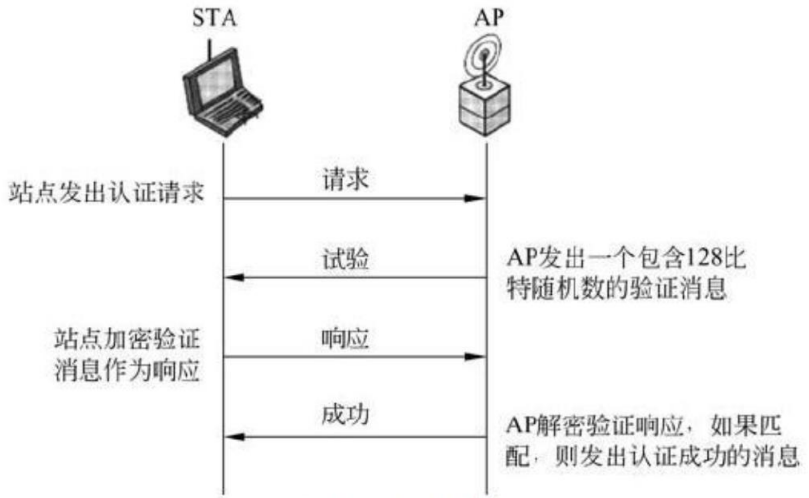


图 7.12 WEP 认证

Q 习题 7.3：

7.3 在 WEP 中，数据完整性和机密性都是由 RC4 流加密算法完成的。MPDU 的传输由以下步骤组成（通常被称为封装）。

（1）发射机选择初始矢量值（IV）。

（2）初始矢量值通过使用共享的 WEP 密钥连接成 RC4 的种子或输入密钥。

（3）32 位的 CRC 被用来计算 MAC 数据域的所有位并将其结果添加到数据域。CRC 是数据连接控制协议中一种通用的错误发现机制。在该例中，CRC 用来进行完整性验证。

（4）第（3）步的结果通过 RC4 加密形成密文块。

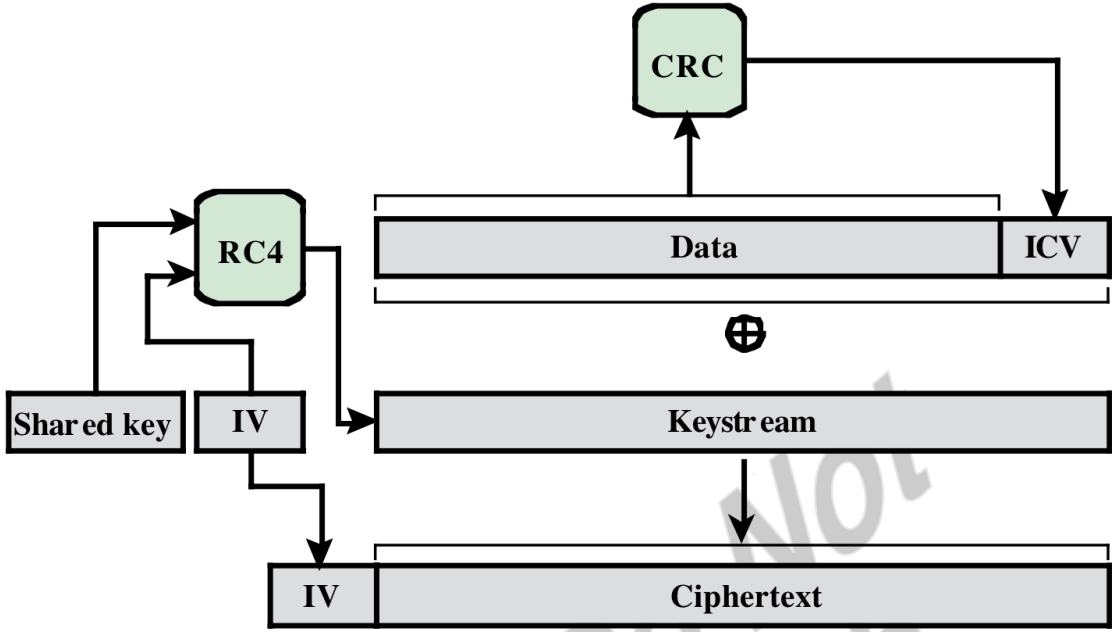
（5）明文 IV 被掩饰为密文块来形成封装的 MPDU 并用来进行传输。

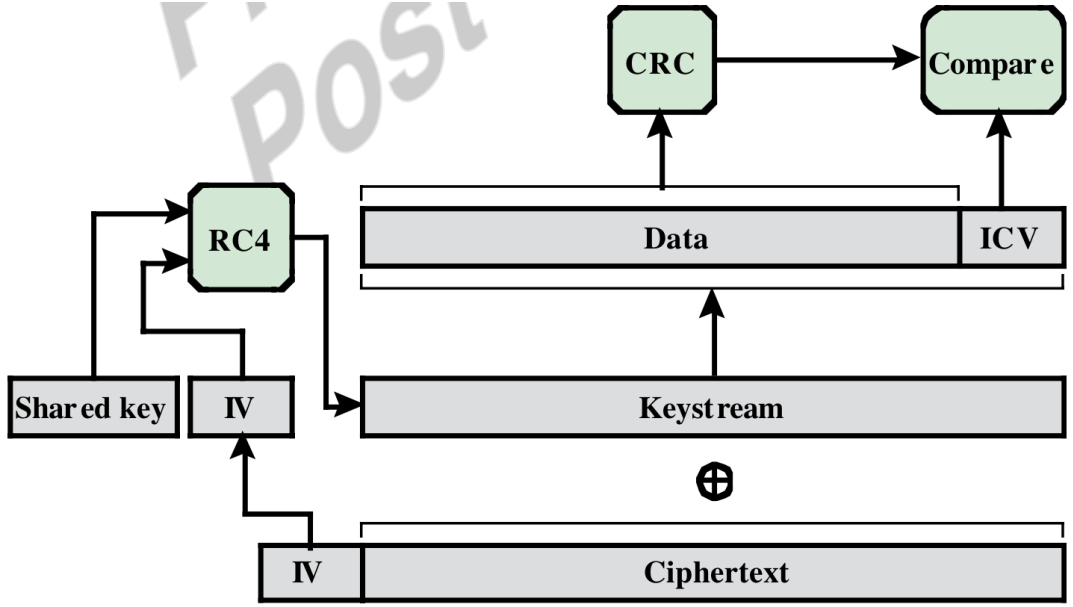
a. 画出封装过程的结构图。

b. 描述接收端如何恢复明文和如何进行完整性验证。

c. 画出 b 的结构图。

1. 首先 从消息截取出 IV
2. 由 PSK 和 IV 通过 RC 4 得到秘钥流 keystream
3. 解密出数据和 ICV
4. 对数据进行 CRC 认证





Q 习题 7.4：ICV 能否抵御比特反转攻击?

不能抵御，基于异或操作的流加密依然是线性变换。