《密码学导论》中俄双语对照复习资料

Вопросы по курсу «Введение в криптографию»

《密码学导论》课程详细答案（中俄双语对照版）

Автор / 作者: Лапонина О.Р.
Программа / 项目: Магистратура, РКТ

Оглавление / 目录

21. 第三方认证协议
22. Kerberos协议
23. PKI与X.509证书
24. 证书撤销方式
25. TLS协议
26. 防火墙分类与包过滤
27. 应用层防火墙
28. 防火墙策略
29. NAT防火墙
30. DMZ网络拓扑

1. 信息安全基本概念

Основные понятия информационной безопасности

定义 / Определения

中文	Русский	说明 / Описание
攻击 (Атака)	Атака	利用系统漏洞破坏安全策略的行为或一系列相关行为。/ Действие, использующее уязвимости системы и приводящее к нарушению политики безопасности.
漏洞 (Уязвимость)	Уязвимость	系统中可被利用来实施攻击的弱点。/ Слабое место в системе, которое может быть использовано для атаки.
风险 (Риск)	Риск	利用特定漏洞实施特定攻击的概率。/ Вероятность осуществления конкретной атаки с использованием конкретной уязвимости.
安全策略 (Политика безопасности)	Политика безопасности	定义系统正确行为的规则、指令和实践。/ Правила, директивы и практики, определяющие правильное поведение системы.
安全机制 (Механизм безопасности)	Механизм безопасности	检测和/或阻止攻击的软硬件。/ Программное и/или аппаратное средство для определения и предотвращения атак.
安全服务 (Сервис безопасности)	Сервис безопасности	确保系统和数据安全的服务，使用一个或多个安全机制。/ Сервис, обеспечивающий безопасность систем и данных.

攻击分类 / Классификация атак

类型 / Тип	中文	Русский
被动攻击	攻击者只能查看传输流量（如流量分析）	Пассивная атака — противник может просматривать передаваемый трафик
主动攻击	攻击者可以修改传输的消息	Активная атака — противник может изменять передаваемые сообщения

主动攻击类型 / Типы активных атак

攻击类型	中文说明	Русское описание
DoS（拒绝服务）	使服务不可用，通常通过资源耗尽实现	Отказ в обслуживании — клиент не может получить доступ к ресурсу
MitM（中间人攻击）	攻击者位于通信双方之间，修改传输流量	Man in the Middle — противник модифицирует передаваемый трафик
数据伪造	攻击者冒充其他客户端获取机密信息	Фальсификация данных — противник представляется другим клиентом
重放攻击	攻击者截获数据后重新发送给服务器	Replay атака — противник перехватывает данные и повторно отправляет

2. 主要安全服务和机制

Основные сервисы и механизмы безопасности

安全服务 / Сервисы безопасности

服务 / Сервис	中文	Русский
机密性 (Конфиденциальность)	防止被动攻击，保护传输或存储的数据	Предотвращение пассивных атак для передаваемых или хранимых данных
认证 (Аутентификация)	确认信息来自合法来源，接收者是预期的	Подтверждение того, что информация получена из законного источника
完整性 (Целостность)	接收者可以确定信息在传输或存储过程中未被修改	Возможность определить, что информация не изменилась
不可否认性 (Невозможность отказа)	发送者和接收者都不能否认传输的事实	Невозможность отказаться от факта передачи
访问控制 (Контроль доступа)	限制和控制对系统和应用程序的访问	Возможность ограничить и контролировать доступ к системам
可用性 (Доступность)	最小化DoS攻击的可能性	Минимизация возможности осуществления DoS-атак

安全机制 / Механизмы безопасности

机制 / Механизм	中文	Русский
对称加密 (Симметричное шифрование)	加密和解密使用同一个密钥	Один и тот же ключ для шифрования и расшифрования
非对称加密 (Асимметричное шифрование)	使用公钥和私钥两个不同的密钥	Два разных ключа — открытый и закрытый
哈希函数 (Хеш-функции)	输入任意长度消息，输出固定长度消息	Входное значение произвольной длины, выход фиксированной длины

3. 对称加密算法

Алгоритмы симметричного шифрования

基本概念 / Основные понятия

中文： 对称加密的主要目的是保证机密性。加密和解密使用同一个密钥。

Русский: Основное назначение — обеспечивать конфиденциальность. Для шифрования и расшифрования используется один и тот же ключ.

加密流程 / Процесс шифрования

$$\text{明文} \xrightarrow{\text{加密算法 + 密钥}} \text{密文} \xrightarrow{\text{解密算法 + 密钥}} \text{明文}$$

加密方式 / Способы шифрования

方式 / Способ	中文	Русский
分组加密	对固定大小的数据块进行加密	Шифрование блоками
流加密	逐位或逐字节加密	Шифрование потоком

安全性要求 / Требования к безопасности

1. **中文：** 算法必须足够强大，没有密钥无法解密 **Русский:** Алгоритм должен быть достаточно сильным
2. **中文：** 安全性应依赖于密钥的保密性，而非算法的保密性 **Русский:** Безопасность должна зависеть от секретности ключа, а не алгоритма
3. **中文：** 即使知道很多明文–密文对，也无法推断出密钥 **Русский:** Даже зная много пар (зашифрованное, незашифрованное), нельзя узнать ключ

基本操作 / Основные операции

操作 / Операция	中文	Русский
表替换 (S-box)	一组比特映射到另一组比特	Группа битов → другая группа битов
置换 (P-box)	重新排列消息的比特	Переупорядочивание битов сообщения
异或 (XOR)	模2加法	Сложение по модулю 2
模加法	模 2^{32} 或 2^{16} 加法	Сложение по модулю 2^{32} или 2^{16}
循环移位	比特循环移动	Циклический сдвиг

算法强度描述 / Описание стойкости алгоритма

特性 / Свойство	中文	Русский
扩散 (Диффузия)	明文每个元素的值影响密文的多个元素	Значение каждого элемента открытого текста влияет на многие элементы шифротекста
混淆 (Конфузия)	消除密文与密钥之间的统计关系	Уничтожение статистической взаимосвязи между шифротекстом и ключом
雪崩效应 (Лавинный эффект)	输入消息改变一位导致输出平均一半位改变	Изменение одного бита входа приводит к изменению половины бит выхода

---

4. Feistel网络与SP网络

Сеть Фейстеля и SP-сеть

Feistel网络 / Сеть Фейстеля

中文： – 输入块分成两个等长的子块（左L和右R） – 每轮对一个分支应用函数F，并与另一分支进行XOR – 加密和解密使用相同的结构，只是密钥顺序相反 – **主要优点：** 即使函数F不可逆，网络也是可逆的

Русский: – Входной блок делится на две части равной длины (L и R) – Каждый раунд состоит из вычисления функции F для одной ветви и XOR с другой – Для расшифрования используется тот же алгоритм, но ключи в обратном порядке – **Главный плюс:** Сеть обратима даже если функция F не является таковой

单轮计算 / Вычисление одного раунда

$$L_{i+1} = R_i \quad R_{i+1} = L_i \oplus F(R_i, K_i)$$

SP网络 / SP-сеть

中文： – 由替换层（S层）和置换层（P层）交替组成 – 所有变换必须可逆 – AES就是基于SP网络的算法

Русский: – Состоит из чередующихся слоев подстановки (S) и перестановки (P) – Все преобразования должны быть обратимы – AES основан на SP-сети

S-box与P-box / S-box и P-box

组件 / Компонент	中文	Русский
S-box	将小块输入位替换为另一块输出位（非线性变换）	Замена маленького блока входных бит на другой блок (нелинейное преобразование)
P-box	重新排列所有位的位置	Перестановка всех бит

5. DES与三重DES

Алгоритмы DES и тройной DES

DES参数 / Параметры DES

参数 / Параметр	值 / Значение
块大小 / Размер блока	64 бит
密钥长度 / Длина ключа	56 бит
轮数 / Число раундов	16
基础结构 / Основа	Сеть Фейстеля

DES缺点 / Недостатки DES

中文： 密钥太短（56位），1995年在竞赛中3小时被破解。

Русский: Слишком маленький ключ (56 бит). В 1995 году был взломан за 3 часа.

中间相遇攻击 / Атака “встреча посередине”

中文： 这就是为什么不使用双重DES的原因。攻击者可以： 1. 用所有密钥（2^{56}个）加密明文 2. 用所有密钥解密密文 3. 寻找匹配，复杂度约为 2^{57} 而非 2^{112}

Русский: Поэтому не используется двойной DES. Злоумышленник: 1. Шифрует plain_text всеми ключами (2^{56}) 2. Расшифровывает cipher_text всеми ключами 3. Ищет совпадения. Сложность порядка 2^{57} вместо 2^{112}

三重DES / Тройной DES

中文： 使用三次DES操作：加密–解密–加密 (EDE)

Русский: Используется троекратное применение DES: Encrypt–Decrypt–Encrypt

模式 / Режим	密钥 / Ключи	密码强度 / Криптостойкость
2个密钥	K1, K2, K1	2^{112}
3个密钥	K1, K2, K3	2^{168}

---

6. Blowfish, IDEA, GOST 28147

Алгоритмы Blowfish, IDEA, ГОСТ 28147

Blowfish

特性 / Характеристика	值 / Значение
块大小 / Размер блока	64 бит
密钥长度 / Длина ключа	可变，最长448 бит
结构 / Структура	Сеть Фейстеля
操作 / Операции	XOR, подстановка, сложение

IDEA

特性 / Характеристика	值 / Значение
块大小 / Размер блока	64 бит
密钥长度 / Длина ключа	128 бит
轮数 / Раундов	8 + 输出变换
操作 / Операции	模 2^{16} 加法, 模 2^{16}+1 乘法, XOR

GOST 28147-89 / ГОСТ 28147-89

特性 / Характеристика	值 / Значение
块大小 / Размер блока	64 бит
密钥长度 / Длина ключа	256 бит
轮数 / Раундов	32
结构 / Структура	Сеть Фейстеля

7. Rijndael (AES)算法

Алгоритм Rijndael (AES)

参数 / Параметры

参数 / Параметр	值 / Значение
块大小 / Размер блока	128 бит
密钥长度 / Длина ключа	128/192/256 бит
轮数 / Число раундов	10/12/14 (取决于密钥长度)

轮变换 / Преобразования раунда

```
Round(State, RoundKey) {
    ByteSub(State);      // 字节替换 / замена байт
    ShiftRow(State);     // 行移位 / сдвиг строк
    MixColumn(State);    // 列混淆 / замешивание столбцов
    AddRoundKey(State, RoundKey);  // 轮密钥加 / добавление ключа
}
```

变换 / Преобразование	中文	Русский
ByteSub	非线性字节替换（S-box）	Нелинейная замена байт через S-блоки
ShiftRow	行循环左移	Циклический сдвиг строк влево
MixColumn	列混合（GF(2^8)上的多项式乘法）	Умножение столбцов как многочленов над GF(2^8)
AddRoundKey	与轮密钥XOR	XOR с раундовым ключом

8. GOST 34.12-2015 “草蜢”

Алгоритм ГОСТ 34.12-2015 «Кузнечик»

参数 / Параметры

参数 / Параметр	值 / Значение
块大小 / Размер блока	128 бит
密钥长度 / Длина ключа	256 бит
轮数 / Число раундов	10
结构 / Структура	SP-сеть

轮变换 / Преобразования раунда

1. **与轮密钥相加** — 128位向量与轮密钥按位异或
2. **非线性变换** — 对每个8位子向量应用固定替换
3. **线性变换** — 可通过LFSR（线性反馈移位寄存器）实现

Русский: 1. **Сложение с раундовым ключом** — побитовое XOR 2. **Нелинейное преобразование** — применение фиксированной подстановки к каждому 8-битному подвектору 3. **Линейное преобразование** — реализуется с помощью РСЛОС

---

9. 流加密算法 Salsa20/ChaCha20

Поточные алгоритмы Salsa20 и ChaCha20

流加密原理 / Принцип поточного шифрования

中文： 逐位或逐字节加密，使用伽马序列与明文进行XOR。

Русский: Шифрование каждого бита или байта с использованием гаммирования (XOR с гамма-последовательностью).

Salsa20

特性 / Характеристика	值 / Значение
内部状态 / Внутреннее состояние	16个32位字 (4×4矩阵)
操作 / Операции	ARX (加法、循环移位、XOR)
轮数 / Раундов	20

核心函数 / Основные функции

- **quarterround(y)** — 对4个字进行变换
- **rowround(y)** — 对矩阵的每行应用quarterround
- **columnround(y)** — 对矩阵的每列应用quarterround
- **doubleround(y)** — columnround后接rowround

ChaCha20

中文： Salsa20的改进版本，目标是每轮提供更好的混合和更高的密码强度。

Русский: Разновидность Salsa20 с улучшенным перемешиванием данных за один раунд.

区别 / Отличия: – 每个字在变换中被修改两次而非一次 – 初始状态布局不同

---

10. 对称加密工作模式

Режимы выполнения симметричного шифрования

ECB (电子密码本模式) / Режим электронной кодовой книги

$C_i = E_K(P_i)$

优点 / Преимущества	缺点 / Недостатки
可并行处理 / Возможно распараллеливание	保留明文统计特性 / Сохранение статистических особенностей
块独立加密 / Блоки независимы	相同明文块产生相同密文块 / Одинаковые блоки → одинаковый шифротекст

CBC (密码块链接模式) / Режим сцепления блоков

$C_i = E_K(P_i \oplus C_{i-1}), \quad C_0 = IV$

优点 / Преимущества	缺点 / Недостатки
隐藏统计特性 / Скрытие статистических особенностей	不能并行加密 / Невозможность распараллеливания шифрования

CTR (计数器模式) / Режим счётчика

$C_i = P_i \oplus E_K(\text{Counter}_i)$

优点 / Преимущества	缺点 / Недостатки
可并行处理 / Возможно распараллеливание	计数器值必须唯一 / Значения счётчика должны быть уникальными
可预计算 / Можно вычислять заранее	

CFB (密文反馈模式) / Режим обратной связи по шифротексту

中文： 前一个密文块作为算法输入，输出与明文XOR。

Русский: Предыдущий зашифрованный блок используется как вход в алгоритм.

OFB (输出反馈模式) / Режим обратной связи по выходу

中文： 类似CFB，但输入是前一次加密的输出，而非密文。

Русский: Аналогичен CFB, но на вход подается результат шифрования предыдущего блока.

GCM (伽罗瓦计数器模式) / Режим Galois/Counter Mode

中文： CTR模式的安全增强版，提供认证加密（AEAD）。

Русский: Более безопасная модификация CTR, предоставляющая аутентифицированное шифрование (AEAD).

---

11. 伪随机数生成

Способы создания псевдослучайных чисел

应用场景 / Применение

应用 / Применение	说明 / Описание
Nonce	防止重放攻击 / Предотвращение replay-атак
会话密钥	KDC生成的临时密钥 / Ключ сессии от KDC

要求 / Требования

要求 / Требование	中文	Русский
随机性	均匀分布、独立	Однородное распределение, независимость
不可预测性	无法从已知元素预测下一个	Нельзя предугадать следующие элементы

生成方法 / Методы генерации

1. **循环加密** — 用主密钥加密计数器值
2. **OFB模式DES** — 使用DES的OFB模式
3. **ANSI X9.17** — 使用三重DES，输入为当前时间和种子值

---

12. 哈希函数要求

Требования к криптографическим хеш-функциям

基本公式 / Основная формула

$h = H(M)$

其中 M 是任意长度的消息，h 是固定长度的哈希码。

六大要求 / Шесть требований

#	中文	Русский
1	适用于任意长度的数据块	Применяется к блоку данных любой длины
2	产生固定长度的输出	Создает выход фиксированной длины
3	容易计算（多项式时间）	Легко вычисляется (за полиномиальное время)
4	**单向性**：给定h，难以找到M使H(M)=h	**Односторонность**: невозможно найти M по h
5	**弱抗碰撞**：给定x，难以找到y≠x使H(y)=H(x)	**Слабая устойчивость к коллизиям**
6	**强抗碰撞**：难以找到任意(x,y)使H(x)=H(y)	**Сильная устойчивость к коллизиям**

生日悖论 / Парадокс дня рождения

中文： 如果哈希码长度为m位，则只需约 2^{m/2} 次尝试就能找到碰撞。因此哈希码长度应约100位以上。

Русский: Если хеш-код имеет длину m бит, то достаточно примерно 2^{m/2} попыток для нахождения коллизии. Поэтому хеш должен быть длинным (порядка 100 бит).

---

13. Merkle–Damgård结构

Структура Меркла — Дамгора

原理 / Принцип

中文： 将任意长度的输入消息分成固定长度的块，通过压缩函数依次处理。

Русский: Разбиение входных сообщений на блоки фиксированной длины и работа с ними по очереди с помощью функции сжатия.

流程 / Процесс

1. 使用初始化向量（IV）
2. 对每个消息块应用压缩函数f

3. 每次的输出作为下一次的输入
4. 最后一块添加填充和长度信息
5. 可选的最终化函数

基于此结构的算法 / Алгоритмы на основе этой структуры

算法 / Алгоритм	输出长度 / Длина выхода	状态 / Статус
MD5	128 бит	不安全 / Небезопасен
SHA–1	160 бит	不安全 / Небезопасен
SHA–256	256 бит	安全 / Безопасен
SHA–512	512 бит	安全 / Безопасен
ГОСТ 3411	256 бит	俄罗斯标准

14. SHA–3哈希函数

Хеш–функция SHA–3

海绵结构 / Конструкция «губки»

中文： SHA–3使用海绵结构，分为”吸收”和”挤出”两个阶段。

Русский: SHA–3 использует конструкцию криптографической губки с этапами «впитывания» и «отжимания».

参数 / Параметры

参数 / Параметр	说明 / Описание
状态大小	5×5×64 = 1600 бит
速率 r	决定速度，r越大越快
容量 c	决定安全性，c越大越安全
关系	r + c = 1600

五个变换步骤 / Пять шагов преобразования

函数f由五个步骤组成：**θ, ρ, π, χ, ι**

其中 **χ** 是唯一的非线性变换。

---

15. 消息认证码MAC

Коды аутентификации сообщений (MAC)

定义 / Определение

中文： MAC是使用密钥计算的认证器，用于验证消息的完整性和来源。

Русский: MAC — это аутентификатор, вычисляемый с помощью ключа для проверки целостности и источника сообщения.

MAC = C_K(M)

MAC的属性 / Свойства MAC

1. 知道M和C_K(M)，难以找到M’使C_K(M) = C_K(M')
2. C_K(M)的值应均匀分布
3. 任意两个消息的MAC相等的概率为2^{–n}（n为MAC长度）

实现方式 / Способы реализации

方式 / Способ	说明 / Описание
基于对称加密	使用CBC模式DES，最后一块作为MAC
基于哈希函数	HMAC — 将密钥与消息结合后哈希

HMAC公式 / Формула HMAC

HMAC = H((K^+ \oplus opad) \| H((K^+ \oplus ipad) \| M))

---

16. 公钥密码学基础

Криптография с открытым ключом

基本概念 / Основные понятия

术语 / Термин	中文	Русский
公钥 (KU)	可公开的密钥	Открытый ключ
私钥 (KR)	必须保密的密钥	Закрытый ключ

要求 / Требования

1. 容易生成密钥对(KU, KR)
2. 用公钥加密容易：C = E_{KU}(M)
3. 用私钥解密容易：M = D_{KR}(C)
4. 从公钥推导私钥在计算上不可行
5. 从公钥和密文恢复明文在计算上不可行
6. （可选）加密和解密顺序可交换

三种主要用途 / Три основных способа использования

用途 / Назначение	中文	Русский
加密/解密	用接收者公钥加密，私钥解密	Шифрование открытым ключом получателя
数字签名	用发送者私钥签名，公钥验证	Подпись закрытым ключом отправителя
密钥交换	协商共享的会话密钥	Обмен сеансовым ключом

常用算法 / Популярные алгоритмы

算法 / Алгоритм	加密	签名	密钥交换
RSA	✓	✓	✓
DSS	✗	✓	✗
Diffie–Hellman	✗	✗	✓
椭圆曲线	✓	✓	✓

---

17. RSA算法

Алгоритм RSA

数学基础 / Математическая основа

中文： 基于大整数分解的困难性。

Русский: Основан на вычислительной сложности задачи факторизации больших целых чисел.

密钥生成 / Генерация ключей

步骤 / Шаг	操作 / Операция
1	选择两个大素数 p 和 q
2	计算 $n = p \times q$
3	计算 $\varphi(n) = (p-1)(q-1)$
4	选择 e，满足 $1 < e < \varphi(n)$，$\gcd(e, \varphi(n)) = 1$
5	计算 d，满足 $d \times e \equiv 1 \pmod{\varphi(n)}$
6	**公钥：(e, n)，私钥：(d, n)**

加密与解密 / Шифрование и расшифрование

操作 / Операция	公式 / Формула
加密	C = M^e \mod n
解密	M = C^d \mod n

数字签名 / Цифровая подпись

操作 / Операция	公式 / Формула
签名	S = M^d \mod n
验证	M = S^e \mod n

---

18. Diffie–Hellman算法

Алгоритм Диффи–Хеллмана

目的 / Цель

中文： 允许两方在不安全信道上安全交换密钥。

Русский: Позволяет двум участникам безопасно обменяться ключом по незащищённому каналу.

协议流程 / Процесс протокола

步骤 / Шаг	操作 / Операция
1	公开参数：素数 p 和 生成元 g
2	Alice选择私钥 a，计算 A = g^a \mod p
3	Bob选择私钥 b，计算 B = g^b \mod p
4	交换 A 和 B
5	Alice计算 K = B^a \mod p
6	Bob计算 K = A^b \mod p
7	**共享密钥：** K = g^{ab} \mod p

安全性 / Безопасность

中文： 基于离散对数问题的困难性。

Русский: Основан на сложности задачи дискретного логарифмирования.

缺点 / Недостаток

中文： 易受中间人攻击，需要配合认证机制使用。

Русский: Уязвим для атаки «Man-in-the-middle», требует дополнительной аутентификации.

---

19. 数字签名标准

Стандарты цифровой подписи

数字签名要求 / Требования к цифровой подписи

1. 签名必须依赖于被签名的消息
2. 签名必须使用发送者的唯一信息
3. 创建签名应相对容易
4. 验证签名应相对容易
5. 伪造签名在计算上不可行

6. 签名应足够紧凑

DSS (数字签名标准) / Digital Signature Standard

中文： 专门设计用于数字签名，不能用于加密或密钥交换。

Русский: Разработан специально для цифровой подписи, нельзя использовать для шифрования.

GOST 3410 / ГОСТ 3410

中文： 俄罗斯数字签名标准，算法与DSS类似。

Русский: Российский стандарт цифровой подписи, алгоритм схож с DSS.

签名类型 / Типы подписей

类型 / Тип	特点 / Особенность
随机化签名 (DSS, GOST)	每次签名不同（使用随机数k）
确定性签名 (RSA)	相同消息和密钥产生相同签名

---

20. 椭圆曲线密码学

Криптография на эллиптических кривых (ECC)

椭圆曲线方程 / Уравнение эллиптической кривой

$$y^2 = x^3 + ax + b \pmod{p}$$

点的加法 / Сложение точек

中文： 1. 存在无穷远点 O 作为零元素 2. 两点之和：过两点作直线，与曲线交于第三点，取其关于x轴的对称点 3. 点与自身相加：用切线代替割线

Русский: 1. Существует бесконечно удалённая точка O как нулевой элемент 2. Сумма двух точек: проводим прямую через две точки, находим третью точку пересечения, берём симметричную относительно оси x

单向函数 / Односторонняя функция

中文： 点的倍乘 kP 容易计算，但从 kP 和 P 求 k 非常困难。

Русский: Умножение точки на число kP легко вычислить, но найти k из kP и P очень сложно.

ECC优势 / Преимущества ECC

中文： 相同安全强度下，密钥长度更短，效率更高。

Русский: Обеспечивает ту же защиту при меньшей длине ключа.

RSA密钥长度	ECC密钥长度
1024 бит	160 бит
2048 бит	224 бит
3072 бит	256 бит

21. 第三方认证协议

Протоколы аутентификации с третьей доверенной стороной

密钥分发中心 (KDC) / Центр распределения ключей

中文： KDC负责为参与者分发会话密钥，每个参与者与KDC共享一个主密钥。

Русский: KDC отвечает за распределение ключей сессии, каждый участник разделяет мастер-ключ с KDC.

防止重放攻击 / Защита от replay-атак

方法 / Метод	中文	Русский
序列号	每条消息添加序列号	Добавление sequence number
时间戳	消息包含当前时间	Отметки времени
Nonce	发送随机数，验证响应	Запрос/ответ с случайным числом

Needham–Schroeder协议 / Протокол Нидхэма–Шредера

1. A → KDC: ID_A \| ID_B \| N_1
2. KDC → A: E_{K_A}[K_S \| ID_B \| N_1 \| E_{K_B}[K_S \| ID_A]]
3. A → B: E_{K_B}[K_S \| ID_A]
4. B → A: E_{K_S}[N_2]
5. A → B: E_{K_S}[f(N_2)]

---

22. Kerberos协议

Протокол Kerberos

组件 / Компоненты

组件 / Компонент	中文	Русский
AS	认证服务器	Сервер аутентификации
TGS	票据授予服务器	Сервер выдачи разрешений
Client	客户端	Клиент
Server	服务器	Сервер

工作流程 / Процесс работы

1. **客户端 → AS：** 请求TGT（票据授予票据）
2. **AS → 客户端：** 返回TGT（用用户密钥加密）
3. **客户端 → TGS：** 使用TGT请求服务票据
4. **TGS → 客户端：** 返回服务票据
5. **客户端 → 服务器：** 使用服务票据认证

特点 / Особенности

- 使用对称加密
- 使用”票据”机制
- 单点登录（SSO）
- 时间戳防止重放攻击

23. PKI与X.509证书

Инфраструктура открытого ключа и сертификаты X.509

PKI组件 / Компоненты PKI

组件 / Компонент	中文	Русский
CA	证书机构，签发和撤销证书	Сертификационный центр
RA	注册机构，验证身份	Регистрационный центр
Repository	存储证书和CRL	Репозиторий сертификатов

X.509证书内容 / Содержимое сертификата X.509

- 版本号
- 序列号
- 签名算法
- 颁发者名称
- 有效期
- 主体名称
- 主体公钥
- 扩展字段
- CA签名

证书链 / Цепочка сертификатов

$$CA_1 \langle\langle CA_2 \rangle\rangle \quad CA_2 \langle\langle B \rangle\rangle$$

24. 证书撤销方式

Способы отмены сертификатов

CRL (证书撤销列表) / Список отозванных сертификатов

中文： CA定期发布包含已撤销证书序列号的签名列表。

Русский: CA периодически выпускает подписанный список отозванных сертификатов.

优点 / Преимущества	缺点 / Недостатки
可通过不安全信道分发	撤销信息有延迟

OCSP (在线证书状态协议) / Online Certificate Status Protocol

中文： 实时在线查询证书状态。

Русский: Онлайн протокол для определения текущего статуса сертификата.

优点 / Преимущества	缺点 / Недостатки
实时获取状态	需要信任在线服务

---

25. TLS协议

Протокол TLS

主要任务 / Основные задачи

1. **密码安全** — 建立安全连接
2. **互操作性** — 不同实现可以互相通信
3. **可扩展性** — 可添加新算法
4. **相对高效** — 使用会话缓存减少计算

协议组成 / Состав протокола

协议 / Протокол	功能 / Функция
记录协议	数据传输，提供机密性和完整性
握手协议	协商参数，认证，交换密钥

握手流程 / Процесс рукопожатия

1. ClientHello
2. ServerHello
3. Certificate (服务器)
4. ServerKeyExchange (可选)
5. CertificateRequest (可选)
6. ServerHelloDone
7. Certificate (客户端，可选)
8. ClientKeyExchange
9. CertificateVerify (可选)
10. ChangeCipherSpec
11. Finished

---

26. 防火墙分类与包过滤

Классификация межсетевых экранов

防火墙功能 / Функции межсетевого экрана

- 根据策略允许或禁止流量
- 分析一个或多个TCP/IP层

包过滤器类型 / Типы пакетных фильтров

类型 / Тип	中文	Русский
无状态	只检查单个包的IP/端口	Без анализа состояния
有状态	跟踪连接状态	С анализом состояния

无状态包过滤 / Пакетные фильтры без состояния

优点 / Преимущества	缺点 / Недостатки
速度快	不能防止应用层攻击
高吞吐量	不支持用户认证
	易受地址欺骗攻击

有状态包过滤 / Пакетные фильтры с состоянием

- 使用状态表跟踪每个连接
- 三种状态：建立中、使用中、已结束
- 只允许已建立连接的流量

---

27. 应用层防火墙

Межсетевые экраны прикладного уровня

功能 / Функции

- 分析应用层协议
- 检测协议异常行为
- 检查命令序列和输入数据

代理网关 / Прокси-шлюзы

中文： 在客户端和服务器之间建立两个独立连接，不允许直接通信。

Русский: Устанавливает два отдельных соединения, не допускает прямого соединения клиента и сервера.

优点 / Преимущества	缺点 / Недостатки
支持用户认证	速度慢
分析完整数据包	功能受限
详细日志	

---

28. 防火墙策略

Политики межсетевого экрана

默认拒绝原则 / Принцип «deny by default»

中文： 拒绝所有不符合策略的流量，只允许明确需要的流量。

Русский: Весь трафик, не соответствующий политикам, отклоняется — разрешено только то, что явно не запрещено.

基于IP和协议的策略 / Политики на основе IP и протоколов

- 只允许必要的协议（TCP, UDP, IPsec）
- 阻止无效的源/目标地址
- 阻止广播地址流量
- 检查路由表验证请求

---

29. NAT防火墙

Межсетевые экраны с возможностями NAT

NAT定义 / Определение NAT

中文： 网络地址转换，将内部私有地址转换为外部公共地址。

Русский: Network Address Translation — преобразование частных IP-адресов во внешние.

NAT类型 / Типы NAT

类型 / Тип	中文	Русский
基本NAT	只转换IP地址	Преобразование только IP-адресов
NAPT	转换IP地址和端口号	Преобразование IP-адресов и портов

NAT池类型 / Типы NAT-пулов

类型 / Тип	特点 / Особенность
有状态	维护状态表，同一内部主机使用相同外部地址
无状态	每次连接可能使用不同外部地址
固定	一对一映射，通过哈希实现

---

30. DMZ网络拓扑

Топология сети DMZ

DMZ定义 / Определение DMZ

中文： 非军事区，是内外网之间的中间区域，存放对外开放的服务器。

Русский: Demilitarized Zone — сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных.

DMZ目的 / Цель DMZ

- 添加额外的安全层
- 即使公共服务被攻破，也能保护内部网络
- 最小化攻击造成的损害

防火墙在DMZ中的规则 / Правила МЭ в DMZ

规则 / Правило	原因 / Причина
禁止内网→DMZ流量	防止攻击者通过DMZ攻击内网
禁止DMZ→外网流量	防止数据泄露

构建原则 / Принципы построения

1. **简单性** — 越简单越安全
2. **按用途使用设备** — 不混用功能
3. **纵深防御** — 多层防护
4. **关注内部威胁** — 不只防外部攻击

重要公式总结 / Важные формулы

RSA

操作 / Операция	公式 / Формула
模数	$n = p \times q$
欧拉函数	$\varphi(n) = (p-1)(q-1)$
加密	$C = M^e \mod n$
解密	$M = C^d \mod n$
密钥关系	$d \times e \equiv 1 \pmod{\varphi(n)}$

Diffie–Hellman

操作 / Операция	公式 / Формула
Alice公钥	A = g^a \mod p
Bob公钥	B = g^b \mod p
共享密钥	K = g^{ab} \mod p

哈希函数 / Хеш-функции

属性 / Свойство	要求 / Требование
抗碰撞	难以找到 H(x) = H(y)
单向性	从 h 难以找到 m 使 H(m) = h

祝考试顺利！📚🎓

Удачи на экзамене!