密码学导论30题详解（中俄对照）

以下是根据提供的PPT源代码（the sources）整理的《密码学导论》30个考试问题的详细中俄双语对照答案：

1. 信息安全基本概念：攻击、漏洞、安全策略、网络攻击分类

Основные понятия ИБ: атаки, уязвимости, политика безопасности, классификация сетевых атак

- **攻击 (Атака)**：任何旨在收集、破坏信息，或破坏系统资源及其访问权限的恶意活动。它也是对系统机密性、完整性或可用性造成威胁的尝试。 **Атака**: Любой вид вредоносной деятельности, направленной на сбор, разрушение информации или уничтожение ресурсов системы. Это попытка поставить под угрозу конфиденциальность, целостность или доступность системы.
- **漏洞 (Уязвимость)**：系统、安全程序或内部控制中的弱点，可能被威胁源利用。 **Уязвимость**: Слабое место в системе, процедурах безопасности или реализации, которое может быть использовано источником угрозы.
- **安全策略 (Политика безопасности)**：规定系统正确行为的规则集合，或对保护要求的陈述。 **Политика безопасности**: Набор правил, определяющих правильное поведение системы, или формулировка требований к защите объектов.
- **攻击分类 (Классификация атак)**:
  - **被动攻击 (Пассивные)**：仅观察数据流（如流量分析、窃听），不改变数据。 **Пассивные атаки**: Только наблюдение за данными (анализ трафика, прослушивание) без изменения содержимого.
  - **主动攻击 (Активные)**：包括拒绝服务 (DoS)、修改数据流（中间人攻击）、伪造数据和重放攻击。 **Активные атаки**: Включают отказ в

обслуживании (DoS), модификацию потока данных (MitM), фальсификацию и повторное использование.

2. 主要安全服务和加密机制

Основные сервисы и криптографические механизмы безопасности

- **安全服务 (Сервисы)**：机密性（防窃听）、认证（确认来源）、完整性（防篡改）、不可抵赖性、访问控制和可用性。 **Сервисы безопасности**: Конфиденциальность, аутентификация, целостность, невозможность отказа, контроль доступа и доступность.
- **加密机制 (Механизмы)**：对称加密算法（同钥）、非对称加密算法（双钥）和哈希函数（定长摘要）。 **Криптографические механизмы**: Алгоритмы симметричного шифрования, асимметричного шифрования и хеш-функции.

3. 对称加密算法：强度概念、应用领域、操作类型

Алгоритмы симметричного шифрования: стойкость, применение, типы операций

- **计算安全性 (Вычислительная стойкость)**：如果破译代价超过信息价值，或破译时间超过信息有效期，则该算法是安全的。 **Вычислительная стойкость**: Алгоритм безопасен, если цена расшифровки больше цены сообщения или время расшифровки больше срока жизни сообщения.
- **应用领域 (Области применения)**：大规模数据加密、生成随机数以及转换为单向哈希函数。 **Области применения**: Шифрование данных, создание случайных чисел и хеширование.
- **基本操作 (Типы операций)**：代换（S-box）、置换（P-box）、位异或（XOR）、模加运算和循环移位。 **Типы операций**: Табличная подстановка (S-box), перемещение (P-box), XOR, сложение по модулю и циклический сдвиг.

4. 费斯妥网络与 SP 网络

Сеть Фейстеля и SP-сеть

- Feistel网络 (Сеть Фейстеля)：将输入块分为两半，轮函数 F 处理后与另一半 XOR 并交换。优点是解密与加密结构相同，只需逆序使用子密钥，且即使 F 不可逆，整体结构也保持可逆。 Сеть Фейстеля: Делит блок на две части; функция F обрабатывает одну ветвь и выполняется XOR с другой, затем они меняются местами. Обратима даже если F необратима; для расшифрования используется тот же алгоритм с обратным порядком ключей.
- SP网络 (SP-сеть)：由代换层（S-layer，产生混淆）和置换层（P-layer，产生扩散）交替组成的结构，如 AES 算法。 SP-сеть: Состоит из чередующихся слоев подстановки (S-box для конфузии) и перестановки (P-box для диффузии). Пример — AES.

5. DES 与 三重 DES (3DES)

Алгоритмы DES и тройной DES

- DES：64位数据块，56位有效密钥，16轮处理。已被暴力破解攻破。 DES: Блок 64 бита, ключ 56 бит, 16 раундов. Уязвим к атакам грубой силы.
- 3DES：采用“加密-解密-加密”（EDE）模式，使用两个或三个不同密钥，有效克服了 DES 密钥过短的问题。 Тройной DES: Использует три операции (зашифрование-расшифрование-зашифрование) с двумя или тремя ключами для повышения безопасности.

6. 对称算法 Blowfish, IDEA, GOST 28147

Алгоритмы Blowfish, IDEA, ГОСТ 28147

- Blowfish：快速的 Feistel 网络算法，使用 16 轮处理和四个 32 位 S-box。 Blowfish: Быстрый алгоритм на основе сети Фейстеля, 16 раундов и четыре 32-битных S-box.
- IDEA：基于 64 位块，其安全性源于异或、模 2^{16} 加法和模 2^{16}+1 乘法这三种不相容运算的组合。 IDEA: Блок 64 бита; безопасность основана на смешивании операций XOR, сложения по модулю 2^{16} и умножения по модулю 2^{16}+1.

- GOST 28147-89：俄罗斯标准，采用 32 轮 Feistel 网络，密钥长度为 256 位。 ГОСТ 28147-89: Российский стандарт, 32 раунда сети Фейстеля, ключ 256 бит.

7. Rijndael (AES) 算法：数学基础与结构

Алгоритм Rijndael (AES): математические основы и структура

- 数学基础：操作基于有限域 GF(2^8)，字节被视为系数属于 {0,1} 的多项式，乘法需模不可约多项式 m(x) = x^8 + x^4 + x^3 + x + 1。 Математические основы: Операции в поле GF(2^8); байты трактуются как полиномы, умножение выполняется по модулю m(x) = x^8 + x^4 + x^3 + x + 1.
- 结构：128位数据块，每轮包含：字节代换 (ByteSub)、行移位 (ShiftRow)、列混淆 (MixColumn) 和轮密钥加 (AddRoundKey)。 Структура: Блок 128 бит; раунд включает ByteSub, ShiftRow, MixColumn и AddRoundKey.

8. “草蜢”算法 (GOST 34.12-2015)

Алгоритм ГОСТ 34.12-2015 «Кузнечик»

- 特点：俄罗斯新标准，采用 SP 网络结构。数据块 128 位，密钥 256 位，共 10 轮处理。 Особенности: Новый российский стандарт, SP-сеть. Блок 128 бит, ключ 256 бит, 10 раундов.
- 结构：采用 XSL 变换方案（密钥加、非线性代换、线性变换）。 Структура: Использует схему XSL (подмешивание ключа, нелинейное и линейное преобразования).

9. 流加密算法：Salsa20 与 ChaCha20

Поточные алгоритмы шифрования: Salsa20 и ChaCha20

- 原理：通过将密钥流（Gamma）与明文位异或实现加密。 Принцип: Шифрование путем наложения гамма-последовательности (XOR) на открытый текст.
- Salsa20/ChaCha20：基于 ARX（加法-旋转-异或）操作，软件运行极快且抗计时攻击。ChaCha20 是对 Salsa20 的改进，旨在提高扩散性。 Salsa20/ChaCha20: Основаны на операциях ARX (сложение, ротация, XOR);

очень быстрые в программной реализации и устойчивы к тайминг–атакам.

10. 对称加密的工作模式

Режимы выполнения алгоритмов симметричного шифрования

- **ECB（电子密码本）**：块独立加密，相同明文块产生相同密文，不安全。 **ECB**: Независимое шифрование блоков; одинаковые блоки дают одинаковый шифртекст (небезопасно).
- **CBC（密码块链接）**：当前明文块先与前一密文块 XOR 再加密，需初始化向量 (IV)。 **CBC**: Сцепление блоков (XOR с предыдущим); требует вектор инициализации (IV).
- **CTR（计数器模式）**：加密计数器值并与明文 XOR，支持并行处理。 **CTR**: Шифрование счетчика и XOR с текстом; позволяет распараллеливание.

11. 伪随机数生成方法

Способы создания псевдослучайных чисел

- **要求**：随机性（分布均匀、独立）和不可预测性。 **Требования**: Случайность (однородность, независимость) и непредсказуемость.
- **方法**：循环加密（加密递增计数器）或使用 ANSI X9.17 标准（结合时间戳、种子和对称加密）。 **Методы**: Циклическое шифрование или генератор ANSI X9.17 (использует дату/время и мастер–ключи).

12. 加密哈希函数的要求

Требования к криптографическим хеш–функциям

- **性质**：任意长度输入变为定长输出。 **Свойства**: Вход любой длины дает выход фиксированной длины.
- **安全性**：单向性（难逆推）、抗弱碰撞性（给定消息难找同哈希消息）和抗强碰撞性（难找哈希相同的任意两消息）。 **Безопасность**: Односторонность, устойчивость к нахождению первого и второго прообраза, а также коллизиям.

13. 默克尔–丹姆加德结构 (MD) 与哈希算法

Структура Меркля — Дамгора, MD5, SHA–1, SHA–2, ГОСТ 3411

- **MD结构**：将消息分块，迭代使用压缩函数处理，最后进行强化处理（补齐长度）。 **Структура MD**: Итеративный метод сжатия блоков сообщения с последующим упрочнением (добавление длины).
- **算法比较**：MD5（128位，不安全）、SHA–1（160位）、SHA–2（256/512位，常用）、GOST 3411（256位，俄罗斯标准）。 **Алгоритмы**: MD5 (128 бит), SHA–1 (160 бит), SHA–2 (256/512 бит), ГОСТ 3411 (256 бит).

14. SHA–3 哈希函数

Хеш–функция SHA–3

- **原理**：采用海绵构造 (Sponge construction)。分为“吸收”阶段（消息 XOR 进内部状态）和“挤出”阶段（从内部状态导出输出）。 **Принцип**: Конструкция «губки». Этап «впитывания» (XOR сообщения в состояние) и этап «отжимания» (извлечение хеша).
- **优势**：由于内部状态包含额外位，能有效抵御长度扩展攻击。 **Преимущество**: Устойчивость к атаке удлинением сообщения благодаря наличию емкости (capacity).

15. 消息认证码 (MAC)

Коды аутентификации сообщений (MAC)

- **目的**：使用共享密钥验证消息的完整性和来源可靠性。 **Цель**: Проверка целостности и источника сообщения с помощью общего секрета.
- **标准**：HMAC（基于哈希函数嵌套密钥）、Poly1305（极快的一次性认证器）。 **Стандарты**: HMAC (на основе хеш–функций) и Poly1305 (быстрый одноразовый аутентификатор).

16. 公钥密码学概念与用途

Криптография с открытым ключом

- **原理**：使用一对密钥（公开的公钥和保密的私钥）。基于具有陷门的单向函数。 **Принцип**: Пара ключей (открытый KU и закрытый KR). Основана на односторонних функциях с люком.
- **用途**：机密性加密、数字签名（确认身份与不可抵赖性）、密钥交换。 **Использование**: Шифрование, цифровая подпись (аутентификация) и обмен ключей.

17. RSA 算法

Алгоритм RSA

- **基础**：基于大整数因子分解的困难性。 **Основа**: Трудность задачи факторизации больших целых чисел.
- **计算**：公钥 \{e, n\}，私钥 \{d, n\}。加密 C = M^e \pmod n，解密 M = C^d \pmod n。 **Вычисления**: Открытый ключ \{e, n\}, закрытый \{d, n\}. Шифрование C = M^e \pmod n, расшифрование M = C^d \pmod n.

18. 迪菲–赫尔曼 (Diffie–Hellman) 算法

Алгоритм Диффи–Хеллмана

- **目的**：允许双方在不安全的信道上商定一个共享秘密密钥。 **Цель**: Безопасный обмен секретным ключом по открытому каналу.
- **安全性**：基于离散对数问题的困难性。但易受中间人攻击，因为不提供身份认证。 **Безопасность**: Трудность вычисления дискретных логарифмов. Уязвим к атаке «man–in–the–middle» без аутентификации.

19. 数字签名标准 GOST 3410 与 DSS

Стандарты цифровой подписи ГОСТ 3410 и DSS

- **DSS**：基于离散对数，签名由 (r, s) 组成，过程引入随机数 k 使得签名具有随机性。 **DSS**: Основан на дискретном логарифме, подпись (r, s). Использование случайного k делает подпись рандомизированной.

- **GOST 3410**：俄罗斯标准，原理类似 DSS 但使用 GOST 哈希函数且 s 计算方式不同。 **ГОСТ 3410**: Российский стандарт, аналогичен DSS, но использует хеш-функцию ГОСТ и другую формулу для s.

20. 椭圆曲线密码学 (ECC)

Криптография на эллиптических кривых

- **定义**：在满足方程 y^2 = x^3 + ax + b \pmod p 的点集上进行运算。 **Определение**: Операции над множеством точек на кривой y^2 = x^3 + ax + b \pmod p.
- **优势**：在同等安全性下，密钥长度比 RSA 短得多，效率更高（例如 160位 ECC 对标 1024位 RSA）。 **Преимущество**: Эквивалентная защита при значительно меньшей длине ключа (160 бит ECC \approx 1024 бит RSA).

21. 使用可信第三方的认证协议

Протоколы с использованием третьей доверенной стороны

- **KDC (密钥分发中心)**：每个用户与 KDC 共享一个主密钥，用于分发临时的会话密钥。 **KDC**: Каждый участник разделяет мастер-ключ с центром распределения ключей для получения сеансовых ключей.
- **防重放攻击**：使用时间戳或挑战/响应（Nonce）机制。 **Защита от replay-атак**: Использование отметок времени или случайных чисел (nonce).

22. Kerberos 协议

Протокол Kerberos

- **核心机制**：使用对称加密和票据 (Ticket) 提供认证。组件包括认证服务器 (AS) 和票据授予服务器 (TGS)。 **Механизм**: Аутентификация на основе симметричного шифрования и билетов (tickets). Включает AS и TGS.
- **版本差异**：v5 支持多种加密算法、允许票据转发，并引入了 предаутентификация 以缓解针对密码的猜测攻击。 **Различия v4 и v5**: v5 поддерживает разные типы шифрования, перенаправление билетов и механизм предварительной аутентификации.

23. 公钥基础设施 (PKI) 与 X.509 证书

Инфраструктура открытого ключа и сертификаты X.509

- **PKI**：管理证书生命周期的系统，包括硬件、软件和策略。 **PKI**: Совокупность аппаратуры, ПО и политик для управления жизненным циклом сертификатов.
- **X.509**：国际标准的证书格式，由 CA 签名，将公钥与主体身份绑定。 **X.509**: Международный стандарт формата сертификата, подписанный CA и связывающий открытый ключ с субъектом.

24. 证书库与撤销方式

Репозиторий и способы отмены сертификатов

- **撤销原因**：私钥泄露、身份变更或 CA 吊销。 **Причины отмены**: Компрометация ключа, изменение имени или увольнение сотрудника.
- **方式**：CRL（定期发布的黑名单列表）或 OCSP（在线查询实时状态）。 **Способы**: CRL (список отмененных сертификатов) или OCSP (онлайн-протокол запроса статуса).

25. TLS 协议中的认证与密钥交换

Аутентификация и обмен ключей в протоколе TLS

- **分层结构**：分为记录协议（提供机密性/完整性）和握手协议（协商算法和密钥）。 **Уровни**: Протокол Записи (конфиденциальность/целостность) и протокол Рукопожатия (согласование параметров).
- **流程**：通过握手协议交换 Nonce，验证服务器证书，通过 RSA 或 DH 确定预主密钥并导出主密钥。 **Процесс**: Обмен сообщениями Hello, верификация сертификатов, согласование премастер-секрета и вычисление мастер-секрета.

26. 防火墙分类与包过滤

Классификация межсетевых экранов. Пакетные фильтры

- **无状态过滤 (Stateless)**：仅检查单个数据包的 IP/端口，不考虑连接上下文。 **Пакетные фильтры без состояния**: Анализируют только заголовки (IP, порты) отдельных пакетов независимо друг от друга.
- **有状态检查 (Stateful)**：维护状态表，跟踪 TCP 握手过程，仅允许属于有效连接的包通过。 **Анализ состояния**: Отслеживает историю соединений с помощью таблицы состояний (TCP флаги, сессии).

27. 应用层防火墙

Межсетевые экраны прикладного уровня

- **功能**：深度解析应用协议（HTTP, FTP 等），能识别特定命令和数据内容（如拦截病毒附件或危险脚本）。 **Функции**: Глубокий анализ прикладных протоколов; могут блокировать конкретные команды (напр., put в FTP) или типы контента.
- **代理 (Proxy)**：作为中间人，不许客户端与服务器直接通信。 **Прокси**: Действует как посредник, не допуская прямого взаимодействия между хостами.

28. 防火墙策略

Политики межсетевого экрана

- **核心原则**：默认拒绝 (Deny by default) —— 只允许明确授权的流量通过。 **Основной принцип**: «Deny by default» — блокируется всё, что явно не разрешено.
- **依据**：IP 地址、协议类型、应用程序特征、用户身份及网络活跃度（如空闲超时自动关闭连接）。 **Основания**: IP-адреса, протоколы, приложения, идентификация пользователя и сетевая активность.

29. 具有 NAT 功能的防火墙

Межсетевые экраны с возможностями NAT

- **作用**：将内网私有地址转换为外部公共地址，隐藏内网结构，防止外部主动发起连接。 **Роль**: Преобразование частных адресов в публичные; скрытие внутренней сети и предотвращение входящих сессий извне.
- **ALG (应用层网关)**：协助处理载荷中包含 IP 地址的特殊协议（如 FTP）。 **ALG**: Помогает протоколам, использующим IP-адреса внутри содержимого (например, FTP).

30. 防火墙网络拓扑 (DMZ)

Топология сети при использовании межсетевых экранов (DMZ)

- **DMZ（隔离区）**：位于内网与外网之间的中间网段，存放对外开放的服务器（Web, Mail）。 **DMZ**: Промежуточная зона для публичных серверов (Web, Mail) между внешней и защищенной внутренней сетями.
- **防御原则**：即使 DMZ 服务器被攻破，由于防火墙的隔离，黑客也难以直接进入核心内网。 **Принцип защиты**: Взлом серверов в DMZ не должен означать автоматический доступ ко всей внутренней сети.