1威胁源未经许可，却直接或间接获得了对系统资源的访问权，从中窃取有用的数据。这种威胁称为      窃取

2选择口令的原则，不正确的是      为了避免遗忘，越短越好

3对访问控制矩阵的基本操作命令有6种

4有哪些访问控制策略  三种  （自主访问控制DAC，强制访问控制MAC 和基于角色的访问控制RBAC）

5一般的安全军事策略，可以描述为 向下读向上写

6 安全模型的特点  精确无异议  简单抽象 易于理解

7基于角色的访问控制是   中性策略

8使用相同的秘钥进行加解密的体制成为  对称密码体制

如果加密操作和解密操作采用的是相同的密钥，或者从一个密钥易于得出另一个密钥，这样的系统就叫做“对称[密码系统](https://www.baidu.com/s?wd=%E5%AF%86%E7%A0%81%E7%B3%BB%E7%BB%9F&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y1PhPhuj0smHw-nAc1uAP90ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3En10vPH0YP161nHndnHDYrjfY)”，也称为“密钥密码体制”。如果加密使用的密钥和解密使用的密钥不相同，且从一个密钥难以推出另一个密钥，这样的[密码系统](https://www.baidu.com/s?wd=%E5%AF%86%E7%A0%81%E7%B3%BB%E7%BB%9F&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y1PhPhuj0smHw-nAc1uAP90ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3En10vPH0YP161nHndnHDYrjfY)称为“[非对称](https://www.baidu.com/s?wd=%E9%9D%9E%E5%AF%B9%E7%A7%B0&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y1PhPhuj0smHw-nAc1uAP90ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3En10vPH0YP161nHndnHDYrjfY)[密码系统](https://www.baidu.com/s?wd=%E5%AF%86%E7%A0%81%E7%B3%BB%E7%BB%9F&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y1PhPhuj0smHw-nAc1uAP90ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3En10vPH0YP161nHndnHDYrjfY)”，也称为“[公钥密码体制](https://www.baidu.com/s?wd=%E5%85%AC%E9%92%A5%E5%AF%86%E7%A0%81%E4%BD%93%E5%88%B6&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y1PhPhuj0smHw-nAc1uAP90ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3En10vPH0YP161nHndnHDYrjfY)”

9 属于多表代换的密码体制是 D 维多尼亚密码体制     [A]　移位密码体制[B]　仿射密 码体制[C]　代换密码体制[D]　维吉尼亚密码体制  其他是单表代换密码体制

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 关于自信息量的说法，错误的是  D | | | | | | | |
|  | | | [A]　是事件概率的单调递减函数 | | | | |
|  | | | [B]　具有可加性 | | | | |
|  | | | [C]　确定事件发生，得不到任何信息 | | | | |
|  | | | | | | | |
| [1] | | | | 未经许可直接或间接获得了对系统资源的访问权，从中窃取有用数据，称为 窃取 |  | |
| [2] | | | | 未经许可，但成功获得了对系统某项资源的访问权并更改称篡改 |  | |
| [3] | | | | 未经许可，在系统中产生虚假数据，称为 伪造 |  | |
| [4] | | | | 未经许可，使得资源不能使用，称为 拒绝服务 |  | |
| [5] | | | | 属于“硬攻击”手段的是 断电 |  | |
| [6] | | | | 属于“软”攻击手段的是 删除程序 |  | |
| [7] | | | | 硬件设施的脆弱性包括 静电可以影响计算机正常工作 |  | |
| [8] | | | | 软件系统的脆弱性包括  操作平台软件有漏洞 |  | |
| [9] | | | | 网络通信的脆弱性包括 通信线路可能被搭线窃听 |  | |
| [10] | | | | 信息系统安全分为 4类 |  | |
| [11] | | | | 自然灾害引起的安全问题，称为 物理安全 |  | |
| [12] | | | | 工作人员失误引起的安全问题属于 认识安全 |  | |
| [13] | | | | 采用具有一定安全性质的硬件或软件，保护信息系统的安全是 技术安全 |  | |
| [14] | | | | 防止信息非授权的泄露，称为 保密性 |  | |
| [15] | | | | 保持信息不被篡改的特性，称为 完整性 |  | |
| [16] | | | | 授权用户能使用资源的性质称为  可用性 |  | |
| [17] | | | | 在再授权范围内控制信息的流向称为  可控性 |  | |
|  | | | |  | | 18 不能否认自己的行为 是抗抵赖性 |
| [19] | | | | 抗干扰的能力称为  可靠性 |  | |
| [20] | | | | 防止非法用户进入系统的技术称为 身份鉴别 |  | |
| [21] | | | | 保证所有的访问都是经过授权的，称为 访问控制 |  | |
| [22] | | | | 使得信息沿着能保证信息安全的方向流动，称为   信息流控制 |  | |
| [23] | | | | 阻止传输过程中，数据被窃取的最好方法是  数据加密 |  | |
| [24] | | | | 防止用户逻辑推理获取数据的方法是  推理控制 |  | |
| [25] | | | | 违反安全策略的方式，传输信息的隐蔽通道，称为 隐通道 |  | |
| [26] | | | | 监视、记录、控制用户活动的机制称为 审计 |  | |
|  |  |  | | | | |
| [27] | | | | 根据安全的需要，系统应设置管理的类，有 3类 |  | |
| [28] | | | | 选择口令时，应该 用户容易记忆 |  | |
| [29] | | | | 根据用户知道什么，验证身份，包括 口令验证 |  | |
| [30] | | | | 根据用户拥有什么进行验证，包括 磁卡 |  | |
| [31] | | | | 根据用户的生物特征验证身份包括 指纹 声音 视网膜 |  | |
| [32] | | | | r权，是指 读权 |  | |
| [33] | | | | w权是指 写权 |  | |
| [34] | | | | a权是指 添加权 |  | |
| [35] | | | | e权是指 执行权 |  | |
| [36] | | | | o权是指 拥有权 |  | |
| [37] | | | | c权是指 控制权 |  | |
| [38] | | | | d权是指 删除权 |  | |
| [39] | | | | 访问控制的基本操作，包括  6种 |  | |
| [40] | | | | 关于实体，正确的说法是 在一定的场合下主体都可以作为客体 |  | |
| [41] | | | | 自主访问控制称为 DAC |  | |
| [42] | | | | 强制访问控制称为 MAC |  | |
| [43] | | | | 基于角色的访问控制，称为 RBAC |  | |
| [44] | | | | 基于客套访问能力的表，称为 。。 |  | |
| [45] | | | | 主体所能访问的客体的表，称为 。。。 |  | |
| [46] | | | | 在自主访问控制中，客体拥有者具有全部的控制权，称为  集中性管理模式 |  | |
| [47] | | | | 客体的拥有者不加限制的把控制权，授予其他主体的管理模式，称为 。。。。 |  | |
| [48] | | | | 不属于自主访问控制的特点的是 |  | |
|  | | | | A | | 以保护个人资源的安全为目标 |
|  | | | | B | | 为用户提供了灵活性 |
|  | | | | C | | 对系统的保护力度比较薄弱 |
|  | | | | D | | 能阻止恶意攻击 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [49] | | | | 强制访问控制的特点是  能阻止恶意攻击 |  | |
| [50] | | | | 按照 军事安全策略，首要保护的属性是 保密性 |  | |
| [51] | | | | 按照商业安全策略，首要保护的属性是 |  | |
|  | | | | A | | 保密性 |
|  | | | | B | | 完整性 |
|  | | | | C | | 可用性 |
|  | | | | D | | 抗抵赖性 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [52] | | | | 一般密级划分为4个级别，按照从低到高的顺序，分别是 一般，秘密，机密，绝密 |  | |
| [53] | | | | 军事安全策略为 |  | |
|  | | | | A | | 向上读，向上写 |
|  | | | | B | | 向上读，向下写 |
|  | | | | C | | 向下读，向上写 |
|  | | | | D | | 向下读，向下写 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [54] | | | | 限制用户对数据的操纵，不能任意进行，而应该按照可保证数据完整性的受控方式进行，称为 |  | |
|  | | | | A | | 良性事务 |
|  | | | | B | | 职责分散 |
|  | | | | C | | 自主访问控制 |
|  | | | | D | | 强制访问控制 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [55] | | | | 把一个操作分成几个子操作，并由不同的用户分别执行，称为 职责分散 |  | |
| [56] | | | | 不属于 安全模型的特点的是 |  | |
|  | | | | A | | 精确 |
|  | | | | B | | 无歧义 |
|  | | | | C | | 简单 |
|  | | | | D | | 可以限制系统的功能 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [57] | | | | BLP模型属于 多级安全策略模型 |  | |
| [58] | | | | BLP模型中，请求元素g代表 get or give |  | |
| [59] | | | | BLP模型中，请求元素r代表 |  | |
|  | | | | A | | release |
|  | | | | B | | release or rescind |
|  | | | | C | | rescind |
|  | | | | D | | return |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [60] | | | | BLP模型中，请求元素c代表 change or create |  | |
| [61] | | | | BLP模型中，请求元素d代表 |  | |
|  | | | | A | | do |
|  | | | | B | | do-while |
|  | | | | C | | do or delete |
|  | | | | D | | delete |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [62] | | | | BLP模型中，判定集中，yes代表 请求被执行 |  | |
| [63] | | | | BLP模型中，判定集中，no代表 请求被拒绝 |  | |
| [64] | | | | BLP模型中，判定集中，error代表 系统出错 |  | |
| [65] | | | | BLP模型中，判定集中，"?”代表 请求出错 |  | |
| [66] | | | | BLP模型中，f1用于 给系统的每一个主体分配密级 |  | |
| [67] | | | | BLP模型中，f2用于 给系统的每一个客体分配密级 |  | |
| [68] | | | | BLP模型中，f3用于 给系统的每一个主体分配范畴集 |  | |
| [69] | | | | BLP模型中，f4用于 给系统的每一个客体分配范畴集 |  | |
| [70] | | | | BLP模型中，f1,f3用于 给系统的每一个主体分配安全标记 |  | |
| [71] | | | | BLP模型中，f2,f4用于 给系统的每一个客体分配安全标记 |  | |
| [72] | | | | **BLP模型，不属于系统的安全特性的是** |  | |
|  | | | | A | | 自主安全性 |
|  | | | | B | | 简单安全性 |
|  | | | | C | | \*-特性 |
|  | | | | D | | 强制安全性 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [73] | | | | 按照BLP模型，自主授权的安全性质，是 自主安全性 |  | |
| [74] | | | | 按照BLP模型，低安全级的主体，不允许获得高安全级客体信息的安全性质，是 。。 |  | |
| [75] | | | | 按照BLP模型，定义的状态转换规则，共有 10条 |  | |
| [76] | | | | 主体请求得到某客体的读权，需要使用 规则1 |  | |
| [77] | | | | 主体请求得到某客体的添加权，需要使用 规则2 |  | |
| [78] | | | | 主体请求得到某客体的执行权，需要使用 规则3 |  | |
| [79] | | | | 主体请求得到某客体的写（w）权，需要使用 规则4 |  | |
| [80] | | | | 主体请求释放对某客体的执行权，需要使用 规则5 |  | |
| [81] | | | | 主体请求释放对某客体的读权权，需要使用 |  | |
|  | | | | A | | 规则3 |
|  | | | | B | | 规则4 |
|  | | | | C | | 规则5 |
|  | | | | D | | 规则6 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [82] | | | | 主体请求释放对某客体的写（w）权，需要使用 |  | |
|  | | | | A | | 规则4 |
|  | | | | B | | 规则5 |
|  | | | | C | | 规则6 |
|  | | | | D | | 规则7 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [83] | | | | 主体请求释放对某客体的添加权，需要使用 |  | |
|  | | | | A | | 规则5 |
|  | | | | B | | 规则6 |
|  | | | | C | | 规则7 |
|  | | | | D | | 规则8 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [84] | | | | 主体A请求授予主体B对客体O的访问权，适用于 |  | |
|  | | | | A | | 规则6 |
|  | | | | B | | 规则7 |
|  | | | | C | | 规则8 |
|  | | | | D | | 规则9 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [85] | | | | 主体A撤消主体B对客体o的读权，适用于 |  | |
|  | | | | A | | 规则6 |
|  | | | | B | | 规则7 |
|  | | | | C | | 规则8 |
|  | | | | D | | 规则9 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [86] | | | | 主体A撤消主体B对客体o的写（w）权，适用于 规则7 |  | |
| [87] | | | | 主体A撤消主体B对客体o的添加权，适用于 |  | |
|  | | | | A | | 规则7 |
|  | | | | B | | 规则8 |
|  | | | | C | | 规则9 |
|  | | | | D | | 规则10 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [88] | | | | 主体A撤消主体B对客体o的执行权，适用于 规则7 |  | |
| [89] | | | | 引入角色的机制是 RBAC |  | |
| [90] | | | | RBAC96模型族中，基础模型是  RBAC0 |  | |
| [91] | | | | RBAC96模型族中，引入角色层次的是 RBAC1 |  | |
| [92] | | | | RBAC96模型族中，引入约束的是 |  | |
|  | | | | A | | RBAC0 |
|  | | | | B | | RBAC1 |
|  | | | | C | | RBAC2 |
|  | | | | D | | RBAC3 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [93] | | | | RBAC96模型族中， 包含角色层次和约束的模型是 RBAC2 |  | |
| [94] | | | | 试遍所有密钥的破译方法是 穷举攻击 |  | |
| [95] | | | | 通过分析明文密文的统计规律的破译方法，称为 统计分析攻击 |  | |
| [96] | | | | 只知道密文，分析密钥的方法属于  。。 |  | |
| [97] | | | | 已知若干组明文密文对的破译方法，称为 已知明文攻击 |  | |
| [98] | | | | 可以使用加密机的破译方法，称为 选择明文攻击 |  | |
| [99] | | | | 可以使用解密机的破译方法称为 选择密文攻击 |  | |
| [100] | | | | 使用移位密码算法，加密“abc”，设密钥为a，则加密结果为 |  | |
|  | | | | A | | abc |
|  | | | | B | | bcd |
|  | | | | C | | cdf |
|  | | | | D | | dfg |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [101] | | | | 使用移位密码算法，加密“abc”，设密钥为b，则加密结果为 |  | |
|  | | | | A | | abc |
|  | | | | B | | bcd |
|  | | | | C | | cdf |
|  | | | | D | | dfg |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [102] | | | | 使用仿射密码算法，加密“b”，设密钥为<3，1>，则加密结果为 |  | |
|  | | | | A | | b |
|  | | | | B | | c |
|  | | | | C | | d |
|  | | | | D | | e |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [103] | | | | DES的密钥长度是 64 |  | |
| [104] | | | | DES的明文分组长度是 |  | |
|  | | | | A | | 64 |
|  | | | | B | | 32 |
|  | | | | C | | 128 |
|  | | | | D | | 不定长 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [105] | | | | DES属于 |  | |
|  | | | | A | | 序列密码体制 |
|  | | | | B | | 公钥密码体制 |
|  | | | | C | | 非对称密码体制 |
|  | | | | D | | 分组密码体制 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [106] | | | | RSA属于 非对称密码体制 |  | |
| [107] | | | | RSA的理论基础是 大数分解的困难性 |  | |
| [108] | | | | 破译RSA的难度与分解大整数的难度  前者小于或等于后者 |  | |
| [109] | | | | 关于 RSA的作用，说法正确的是  既可以加密数据，又可以数据签名 |  | |
| [110] | | | | 维吉尼亚密码，属于 |  | |
|  | | | | A | | 单表替换 |
|  | | | | B | | 多表替换 |
|  | | | | C | | 现代密码体制 |
|  | | | | D | | 非对称密码体制 |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [111] | | | | AES的密钥长度，可以是128 192 256bits |  | |
| [112] | | | | AES的明文分组长度，不能为 |  | |
|  | | | | A | | 64bits |
|  | | | | B | | 128bits |
|  | | | | C | | 192bits |
|  | | | | D | | 256bits |
| 【题型：单选】【分数：1分】 |  |  | | | | |
| [113] | | | | 在AES体制下，如果明文和密钥的长度都为256bits，则加密圈数为 14圈 |  | |
| [114] | | | | AES属于  对称密码体制 （分组和序列） |  | |
| [115] | | | | 对 16圈DES的威胁比较大的攻击方式是。。 |  | |
| [116] | | | | 关于 一次一密的密码体制，说法正确的是。。 |  | |
| [117] | | | | MD5的计算过程，分为 5步 |  | |
| [118] | | | | MD5的第一步是  附加填充位 |  | |
| [119] | | | | MD5的第2步是 附加长度 |  | |
| [120] | | | | MD5的第3步是  初始化MD缓冲区 |  | |
| [121] | | | | MD5的第4步是 按512位的分组处理输入消息 |  | |
| [122] | | | | MD5的第5步是   输出 |  | |
| [123] | | | | 关于数字签名，说法正确的是  既可以利用公钥密码进行数字签名，也可以利用传统密码进行数字签名 |  | |
| [124] | | | | 身份认证技术包括 用hash函数加密口令，用数字签名方式验证口令，口令的双向认证 |  | |
| [125] | | | | 报文认证技术不包括。。 |  | |
| [126] | | | | 审计过程，首先要进行  事件收集 |  | |
| [127] | | | | 为了更好的对事件进行分析，需要。。 |  | |
| [128] | | | | 需要系统审计员才能操作的是。。 |  | |
| [129] | | | | 可以执行 关闭审计开关的人员是 系统审计员 |  | |

【130】属于审计粒度的有 客体 用户 <用户，客体>

|  |  |  |
| --- | --- | --- |
| [131] | 数据库安全的目标包括  保密性 完整性 可用性 |  |
| [132] | CC的第一部分是 简介和一般模型 |  |
| [133] | CC的第2部分是安全功能要求 |  |
| [134] | CC的第3部分是 安全保证要求 |  |
| [135] | 根据我国国家标准GB17859-1999，一:用户自主保护级，二：系统审计保护级，三：安全标记保护级，四：结构化保护级，五：访问验证保护级 |  |
| [140] | 按照TCSEC的等级划分，最小保护类，称为 D 类 |  |
| [141] | 按照TCSEC的等级划分，自主安全保护类，称为 C类 |  |
| [142] | 按照TCSEC的等级划分，强制安全保护类，称为 B类 |  |
| [143] | 按照TCSEC的等级划分，验证安全保护类，称为 A 类 |  |
| [144] | 影响隐通道带宽的因素，包括 噪音和延迟 编码 原语的选择 不包括数据的多少 |  |
| [146] | 按照X.509版本一的证书结构。版本号的作用是。。 |  |
| [147] | 按照X.509版本一的证书结构。序列号的作用是  证书的唯一标识符 |  |
| [148] | 按照X.509版本一的证书结构。签名算法标识符的作用是 所用的数字签名算法和所需要的参数 |  |
| [149] | 包过滤路由器的优点：保护整个网络，减少暴露的风险，对用户透明，不需要过多设置，可以作为数据包过滤 |  |
| [150] | 下列哪个选项，不属于证书路径约束的类型 。。 |  |

完整的PKI系统必须具有权威认证机构(CA)、数字证书 库、密钥备份及恢复系统、证书作废系统、应 用接口（API）等基本构成部分，构建PKI也将 围绕着这五大系统来着手构建。

古典密码包括  移位 代换 仿射 维吉尼亚 希尔 置换密码

计算机定义：计算机的硬件，软件和数据收到保护，不因 偶然和恶意的原因而遭到破坏，更改和泄露，

系统连续正常运行

信息安全的属性包括： 保密性 完整性 可用性 可控性 抗 抵赖性

TESEC的等级划分  最小保护类 自主安全保护类 强制安全   保护类 验证安全保护类

可信计算机系统评估准则对计算机系统的安全要求包括 安  全策略 标记 责任 识别 保证

双宿主网关的优势：网关将受保护的网络与外部网络完全    隔离，代理服务器提供日志，有助于   发现入侵，可以用于身份验证服务器及   代理服务器等功能，站点系统的名字和   IP地址，对Internet系统是屏蔽的

PKI的保密服务机制包括：生成一个对称密钥，用对称密钥       加密数据，将加密后的数据发送 给对方

RBAC96模型族包括：RBAC0,RBAC1,RBAC2,RBAC3

属于古典密码体制的有：移位密码，仿射密码，维吉尼亚    密码，希尔密码

审计子系统的功能：时间收集功能，事件过滤功能，对事     件的分析和控制功能，日志维护和查     询功能，审计信息安全性保护功能

BLP 向下读 向上写的原则

双宿主网关的优势：网关将受保护的网络与外部网络完全隔离

   代理服务器提供日志，有助于发现入侵

   可以用于身份验证服务器及代理服务器等功能

    站点系统的名字和IP地址，对internet系统是屏蔽的

|  |  |
| --- | --- |
| 按照OSI参考模型，支持连接保密的层包括 物理层 链路层 网络层 传输层 |  |

按照TESEC的等级划分，简述强制安全保护类的等级划分

B1级：标识安全保护  B2级：结构化保护   B3级：安全域

安全模型

准确的描述安全的重要方面及其与系统行为的关系；提高对成功实现安全需求的理解层次