选择题

1. 实现数据完整性判别的主要手段的是（ D ）

A、对称加密算法　B、非对称加密算法C、混合加密算法　D、散列算法

2. 不属于 RFID 标签安全技术的有（ D ）

A、法拉第罩法　　B、主动干扰法　　C、封杀标签法　　D、地址过滤法

3. Alice 有一对密钥（$K_{A\,公开}$，$K_{A\,秘密}$），Bob 有一对密钥（$K_{B\,公开}$，$K_{B\,秘密}$），Alice 对信息 M 签名且加密的过程为：M’= $K_{B\,公开}$（$K_{A\,秘密}$（M））。Bob 收到密文后，进行解密和签名验证的过程为（ C ）

A、$K_{B\,公开}$（$K_{A\,秘密}$（M’））　　B、$K_{A\,公开}$（$K_{A\,公开}$（M’））

C、$K_{A\,公开}$（$K_{B\,秘密}$（M’））　　D、$K_{B\,秘密}$（$K_{A\,秘密}$（M’））

4. 不属于 3G 网络的技术有（ B ）

A、WCDMA　　B、TCP/IP

C、TD-SCDMA　　D、CDMA2000

5. 下列选项中不属于主动攻击的是（ B ）

A、重放　　B、流量分析　　C、篡改　　D、伪装

6. 防火墙的类别不包括（ A ）

A、病毒过滤防火墙　　B、双穴主机防火墙

C、应用代理防火墙　　D、包过滤防火墙

7. DoS 攻击破坏了（ A ）

A、可用性　　B、保密性　　C、完整性　　D、真实性

8. 数字签名必须满足的条件是（ C ）。

A、既能用于签名，有能用于加密和解密

B、只能对消息摘要进行签名

C、收发双方都不可以否认

D、保证签名值能正确还原成被签名的明文

9. 物联网的核心技术是（ B ）

A、集成电路　　B、射频识别　　C、无线电　　D、操作系统

10. 主要用于加密机制的协议是:（ D ）。

A、HTTP　　B、FTP　　C、TCP/IP　　D、WEP

11. WLAN 的流行标准有（ D ）

A、SP100.11a　　B、IPv6　　C、IEEE 802.15.4　　D 、 IEEE 802.11n

12. 在 RFID 中物联网中间件具有以下特点（ D ）

A、应用架构独立　　B、分布数据存储　　C、数据加工处理　　D、以上全是

13. 防火墙用于将 Internet 和内部网络隔离（ B ）

A、是防止火灾的硬件设施　　B、是保护网络安全的软件和硬件设施

C、是保护线路不受破坏的软件和硬件设施　　D、是起抗电磁干扰作用的硬件设施

14. 负责对物联网收集到的信息进行处理、管理、决策的后台计算处理平台属于（ A ）

A、应用层　　B、网络层

C、传输层　　D、感知层

15. 物联网技术是基于射频识别技术而发展起来的新兴产业，射频识别技术主要是基于（ C ）方式进行信息传输的。

A、同轴电缆　　B、双绞线

C、电场和磁场　　D、声波

16. μTESLA 是一种（ D ）

A、对称加密协议　　B、非对称加密协议　　C、密钥分配协议　　D、广播认证协议

17. 属于入侵检测系统的结构是（ D ）

A、基于主机系统的结构　　B、基于网络系统的结构

C、基于分布式系统的结构　　D、以上都是

18. 无线传感器网络安全协议 SPINS 包含（ A ）模块。

A、SNEP　　B、IPSec　　C、IDS　　D、IPS

19. 分析破译 DES 和 RSA 密码体制的关键分别是（ B ）

A、陷门信息、大整数的因数分解　　B、S 盒的设计、大整数的因数分解

C、大整数的因数分解、陷门信息　　D、S 盒的设计、陷门信息

20. VPN 协议是属于（ B ）的远程服务协议

A、物理层　　B、网络层　　C、传输层　　D、应用层

21. 属于数字签名方案的是（ B ）

A、KDC　　B、DSS　　C、TCP　　D 、 Diffie-Hellman

22. 属于安全协议的是：（ D ）。

A、HTTP　　B、FTP　　C、IP　　D、IPSec

23. 在无线传感器网络中，可以抵御黑洞攻击的是（ D ）

A、认证　　B、监测　　C、冗余机制　　D、以上全是

24. 常见的古典密码是（ A ）

A、替换加密　　B、流密码　　C、对称密码　　D、以上全是

25. CA 的主要功能是（ A ）

A、颁发证书　　B、提供保密性

C、验证完整性　　D、实施询问-应答

26. DES 的分组长度为（ C ）

A、32 位　　B、56 位

C、64 位　　D、128 位

27. 在无线传感器网络中，由于传感器节点的计算和存储资源有限，通常采用轻量级的加密算法，例如（ B ）

A、μTESLA　　B、NTRU　　C、RSA　　D、以上都不是

28. IPSec 协议是属于（ B ）的安全协议

A、物理层　　B、网络层　　C、传输层　　D、应用层

29. 云计算的安全问题有（ A ）

A、信任问题　　B、可靠性问题

C、开放问题　　D、共享问题

30. Diffie-Hellman 算法可用于（ D ）

A、数字签名　　B、加密　　C、认证　　D、密钥分配

31. 在无线传感器网络中，可以抵御泛洪攻击的是（ A ）

A、客户端谜题　　B、扩频和跳频　　C、冗余路径　　D、以上全是

32. AES 的分组长度为（ D ）

A、128 位　　B、192 位

C、256 位　　D、以上都是

33. 下列选项中属于被动攻击的是（ B ）

A、重放　　B、流量分析　　C、篡改　　D、伪装

34. 防火墙从结构上分为单一主机防火墙、路由集成防火墙和（ A ）

A、分布式防火墙　　B、双穴主机防火墙

C、应用代理防火墙　　D、包过滤防火墙

35. DoS 攻击破坏了消息的（ A ）

A、可用性　　B、保密性　　C、完整性　　D、真实性

36. 属于网络安全的协议是（ D ）。

A、HTTP　　B、FTP　　C、TCP/IP　　D、SSL

37. SM4 是我国官方公布的第一个商用密码算法，它是一种（ A ）。

A、对称密码算法　　B、非对称密码算法　　C、流密码算法　　D、散列函数算法

38. 公钥密码体制也称为非对称密码体制，典型的公钥密码体制是（ C ）

A、DES　　B、AES　　C、RSA　　D、以上都不是

39. 身份认证过程中，被认证对象的属性可以是（ D ）

A、口令　　B、数字签名　　C、生理特征　　D、以上都是

40. IPSec 协议组中用于认证的协议是（ B ）

A、ESP　　B、AH　　C、IKE　　D、SA

41. 公钥基础设施能为用户提供多种安全服务，但不包括（ B ）

A、身份认证　　B、访问控制　　C、数据保密性　　D、时间戳服务

42. 入侵防御系统面对的挑战有（ D ）

A、单点故障　　B、性能瓶颈　　C、误报和漏报　　D、以上都是

43. 经过网络连接将自身从一台计算机分发到其他计算机系统中的病毒是（ B ）

A、计算机病毒　　B、蠕虫病毒　　C、木马病毒　　D、以上都不是

44. 认证能够防止的攻击有（ A ）

A、伪装　　B、窃听　　C、数据攻击　　D、以上都能

45. 信息安全中的安全目标和需求通常都强调三元组，不包括以下的（ D ）

A、可用性　　B、保密性　　C、完整性　　D、不可否认性

46. 以下描述错误的是（ C ）

A、满足所有的安全需求，才算达到安全目标。

B、一个安全服务可能是多个安全需求的组成要素。

C、不同的安全服务的组合只能实现相同的安全需求。

D、不同的安全机制组合能够完成不同的安全服务

47. 以下属于古典加密技术的是（ D ）

A、摩斯密码　　B、维吉尼亚密码　　C、藏头诗　　D、以上都是

48. IPSec 协议中的 AH 完成的功能包括（ C ）

A、消息加密　　B、防窃听　　C、身份认证　　D、以上都是

49. 双宿主机防火墙是（ A ）

A、用一台装有两块网卡的堡垒主机做防火墙。

B、一台堡垒主机上只有一个 IP 地址。

C、安装在防火墙和路由器之间。

D、由两个路由器和一个堡垒主机构成。

50. 以下关于数字签名标准 DSS 的说法正确的是（ B ）。

A、DSS 的算法基础是 DES

B、DSS 的输入为消息的散列值、随机数和签名者的私钥

C、DSS 主要保护通信双方之间的消息的保密性

D、以上都错误

51. SSL 协议是基于 Web 应用的安全协议，是一种用于（ B ）的安全协议。

A、应用层　　B、传输层　　C、网络层　　D、物理层

52. 我国的王小云教授在 2004 年国际密码学会议上破解了（ C ）算法。

A、DES　　B、RSA　　C、MD5　　D、ECC

53. 3DES 的加密方案为（ A ）

A、加密-解密-加密　　B、解密-加密-解密

C、加密-加密-加密　　D、解密-解密-解密

54. 支付宝平台采用的人脸支付技术采用的身份认证手段是基于（ B ）

A、用户所知道的　　B、用户本身的　　C、用户所拥有的　　D、以上都不是

55. 下列关于 Diffie-Hellman 算法的描述错误的是（ D ）

A、D-H 算法是第 1 个公开密钥的算法

B、D-H 算法的目的是进行密钥的安全交换

C、D-H 算法的安全性基于求离散对数的困难性

D、D-H 算法本身也可以用于加密和解密消息

56. PKI 为用户提供密钥和证书管理，其典型的系统中不包括（ C ）

A、认证机构 CA　　B、注册机构 RA　　C、消息摘要　　D、证书发布系统

57. 入侵检测系统采用的技术包括（ C ）

A、数据加密和消息认证　　B、数据和端口扫描

C、异常检测和误用检测　　D、以上都是

58. 恶意代码是一种计算机程序，其分类不包括（ C ）

A、计算机病毒　　B、蠕虫和木马病毒　　C、异常代码　　D、复合型病毒

59. 下列关于 RSA 算法的描述错误的是（ A ）

A、RSA 算法是一种非常著名的分组对称密码算法

B、RSA 中的加密和解密密钥互为乘法逆元

C、RSA 是基于大合数的质因子分解问题的困难性

D、RSA 算法的加密函数是一个单向陷门函数

60. 在安全机制中，与安全服务有关的机制是（ D ）

A、加密　　B、数字签名　　C、访问控制　　D、以上都是

61. 当密钥$k=3$时，用凯撒密码对“top”进行加密后得到密文（ C ）

A、xst　　B、vqr

C、wrs　　D、ytu

62. 我国官方公布的第一个商用密码算法，也是一种分组对称密码算法，它是（ B ）

A、DES　　B、SM4　　C、RC4　　D、AES

63. DES 的安全强度依赖于（ D ）

A、密钥长度　　B、迭代次数　　C、S 盒的设计　　D、以上都是

64. 下列属于散列算法的是（ A ）

A、MD5　　B、3DES　　C、ECC　　D、DSA

65. 下列关于散列函数描述正确的是（ C ）。

A、散列函数可以用于加密和解密

B、将固定分组长度的明文输入散列函数后，得到不同长度的 Hash 值

C、如果 Hash 值过短，则容易遭受生日攻击

D、HMAC 无法有 Hash 函数构建，只能用 MAC 函数构建

66. 数字签名技术无法解决（ D ）

A、否认　　B、伪造　　C、冒充　　D、流量监听

67. 以下描述错误的是（ C ）

A、验证发送方的身份称为实体认证。

B、认证无法自然地提供保密功能。

C、散列函数不能提供消息认证功能。

D、认证中心可以批准或拒绝认证请求，以及颁发认证证书。

68. 下列属于 IPsec 的组成模块的是（ D ）

A、AH　　B、ESP　　C、IKE　　D、以上都是

69. 蠕虫病毒一般会采用的传播工具是（ C ）

A、寄生　　B、用户复制　　C、远程登录　　D、漏洞补丁

70. 特洛伊木马是（ A ）

A、一种伪装成正常程序的恶意代码　B、通过自我复制感染组网内的计算机的

C、寄生在其他程序中的，因此难以被发现　D、一种普通的计算机病毒

71. 椭圆曲线密码算法是（ B ）。

A、复杂度很低的对称密码算法　B、复杂度很低的非对称密码算法

C、复杂度很高的非对称密码算法　D、复杂度很高的对称密码算法

72. DSS 采用了（ B ）散列算法，给出了一种数字签名算法 DSA。

A、MD5　B、SHA　C、DES　D、RSA

73. 下列密码算法中采用了单向陷门函数的是（ C ）

A、维吉尼亚密码　B、AES　C、RSA　D、DES

74. 3DES 在加密时的处理步骤是（ C ）

A、加密-加密-加密　B、解密-解密-解密

C、加密-解密-加密　D、以上都不是

判断题

1. Sybil 攻击的特点是多个恶意节点具有一个身份。（ × ）

2. 射频识别卡都是非接触式的。（ ✓ ）

3. DES、AES、RSA 都是对称加密算法。（ × ）

4. Diffie-Hellman 算法只能用于密钥协商，不能用于数据加密。（ ✓ ）

5. MAC 算法是使用散列函数求解消息摘要的算法，求解过程无需密钥的参与。（ × ）

6. IPSec 协议、PGP 协议、UDP 协议都是网络安全协议。（ × ）

7. Hash-Lock、Good Reader 和 David 数字图书馆协议均属于 RFID 安全密码协议。（ ✓ ）

8. 隧道技术是 IDP 的核心实现技术。（ × ）

9. 在无线传感器网络中，设置竞争门限和冗余路径都可以抵御耗尽攻击。（ × ）

10. 国家密码 SM3、SM4 算法均为单向散列函数。（ × ）

11. NTRU 被认为是实现空间最小的轻量级公钥加密算法。（ ✓ ）

12. SNEP 协议提供了数据认证、重放保护以及消息新鲜度的功能。（ ✓ ）

13. 扩频技术可以用来防御泛洪攻击。（ × ）

14. 2G 只提供单向认证，3G 和 4G 均提供双向认证。（ ✓ ）

15. 单向散列函数既可以用于数字签名，又可以用于加密和解密。（ × ）

16. 参与 AKA 的主体有用户终端、被访问网络和归属网络。（ ✓ ）

17. IEEE 802.11、Bluetooth 和 ZigBee 都是远距离无线低速接入方法的典型代表。（ × ）

18. 入侵防御系统和入侵检测系统是独立于防火墙的智能化安全技术。（ × ）

19. Hash 链协议和基于 Hash 的 ID 变化协议都是 RFID 的安全协议。（ ✓ ）

20. WEP 是针对远距离无线通信网络定义的一种加密和认证协议。（ × ）

21. WEP 协议、PGP 协议、UDP 协议都是网络安全协议。（ × ）

22. 冗余路径和探测机制都可用于防御怠慢和贪婪攻击。（ ✓ ）

23. 方向误导攻击又称排水攻击，攻击者声称自己具有一条高质量的路由到基站的路径。（ × ）

24. 物联网具有优势的领域主要包括智能电网、智能交通、物流管理和医疗管理等。（ ✓ ）

25. 在 WSN 中设计安全方案时，需要考虑网络中的节点密度、拓扑结构、计算和存储能力、通信能力，以及能量限制。（ ✓ ）

26. 实现用户所有的安全要求也就达到了用户的安全目标。（ ✓ ）

27. 保密性、完整性和可用性是相辅相成的，可以全部满足。（ × ）

28. 模运算与求余运算不同。（ × ）

29. 凯撒密码属于多表代换密码。（ × ）

30. 针对散列函数的攻击时建立在生日悖论之上的。（ ✓ ）

31. 入侵防御系统能够提供主动性的防御。（ ✓ ）

32. DES 的明文分组长度是 64 位。（ ✓ ）

33. 安全机制分为特定安全机制和普通安全机制。（ ✓ ）

34. 两个整数a，b分别被m除，如果所得的商相同，则称a与b对模m是同余的。（ × ）

35. 模运算在普通实数域上进行运算后，再去模取余。（ ✓ ）

36. 密码分析和穷举攻击都无法破解非对称加密技术。（ × ）

37. DES 的初始密钥为 64 位，其奇偶校验位也能参与加密运算。（ × ）

38. 消息认证就是身份认证。（ × ）

39. IPSec 是一组安全协议集，在 IPv4 中是可选服务，在 IPv6 中是必须支持的功能。（ ✓ ）

40. 防火墙的基本功能就是访问控制。（ ✓ ）

41. 入侵检测串联在网络中，与防火墙实施联动。（ × ）

42. 计算机病毒具有传染性、潜伏性、隐蔽性、多态性和破坏性。（ ✓ ）

43. 普通安全机制在同一时间只针对一种安全服务实施。（ × ）

44. 消息的完整性是指保护信息和信息处理方法的准确性和原始性。（ ✓ ）

45. 古典加密技术主要使用代换或者置换技术。（ ✓ ）

46. DES 是用来取代 AES 的高级机密标准。（ × ）

47. 公钥密码体制也称非对称密码体制，其加密和解密的密钥是不同的。（ ✓ ）

48. SSL 协议是常见的传输层的安全协议。（ ✓ ）

49. 入侵防御系统是在防火墙之前的第一道安全闸门。（ × ）

50. 入侵检测系统是利用过滤器对数据进行筛选的。（ × ）

51. 恶意代码都具有自我复制的能力。（ × ）