2019 年信息安全工程师上午真题

1、《中华人民共和国网络安全法》第五十八条明确规定，因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经（ ）决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

A. 国务院
B. 国家网信部门
C. 省级以上人民政府
D. 网络服务提供商

2、2018 年 10 月，含有我国 SM3 杂凑算法的 ISO/IEC10118-3：2018《信息安全技术杂凑函数第 3 部分：专用杂凑函数》由国际标准化组织(ISO)发布，SM3 算法正式成为国际标准。SM3 的杂凑值长度为（ ）。

A. 8 字节
B. 16 字节
C. 32 字节
D. 64 字节

3、 BS7799 标准是英国标准协会制定的信息安全管理体系标准，它包括两个部分：《信息安全管理实施指南》和《信息安全管理体系规范和应用指南》。依据该标准可以组织建立、实施与保持信息安全管理体系，但不能实现（ ）。

A. 强化员工的信息安全意识，规范组织信息安全行为
B. 对组织内关键信息资产的安全态势进行动态监测
C. 促使管理层坚持贯彻信息安全保障体系
D. 通过体系认证就表明体系符合标准，证明组织有能力保障重要信息

4、为了达到信息安全的目标，各种信息安全技术的使用必须遵守一些基本原则，其中在信息系统中，应该对所有权限进行适当地划分，使每个授权主体只能拥有其中的一部分权限，使它们之间相互制约、相互监督，共同保证信息系统安全的是 （ ）。

A. 最小化原则
B. 安全隔离原则
C. 纵深防御原则
D. 分权制衡原则

5、等级保护制度已经被列入国务院《关于加强信息安全保障工作的意见》之中。以下关于我国信息安全等级保护内容描述不正确的是（　）。
A.对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输和处理这些信息的信息系统分等级实行安全保护
B.对信息系统中使用的信息安全产品实行按等级管理
C.对信息系统中发生的信息安全事件按照等级进行响应和处置
D.对信息安全从业人员实行按等级管理，对信息安全违法行为实行按等级惩处

6、研究密码破译的科学称为密码分析学。密码分析学中，根据密码分析者可利用的数据资源，可将攻击密码的类型分为四种，其中适于攻击公开密钥密码体制，特别是攻击其数字签名的是　（　）。
A.仅知密文攻击
B.已知明文攻击
C.选择密文攻击
D.选择明文攻击

7、基于 MD4 和 MD5 设计的 S/Key 口令是一种一次性口令生成方案，它可以对访问者的身份与设备进行综合验证，该方案可以对抗（　）。
A.网络钓鱼
B.数学分析攻击
C.重放攻击
D.穷举攻击

8、对于提高人员安全意识和安全操作技能来说，以下所列的安全管理方法最有效的是（　）。
A.安全检查
B.安全教育和安全培训
C.安全责任追究
D.安全制度约束

9、访问控制是对信息系统资源进行保护的重要措施，适当的访问控制能够阻止未经授权的用户有意或者无意地获取资源。信息系统访问控制的基本要素不包括（　）。
A.主体
B.客体
C.授权访问
D.身份认证

10、下面对国家秘密定级和范围的描述中，不符合《中华人民共和国保守国家秘密法》要求的是（　）。
A.对是否属于国家和属于何种密级不明确的事项，可由各单位自行参考国家要 求确定和定级，然后报国家保密工作部门备案
B.各级国家机关、单位对所产生的秘密事项，应当按照国家秘密及其密级的具 体范围的规定确定密级，同时确定保密期限和知悉范围
C.国家秘密及其密级的具体范围，由国家行政管理部门分别会同外交、公安、 国家安全和

其他中央有关机关规定
D.对是否属于国家和属于何种密级不明确的事项，由国家保密行政管理部门， 或省、自治区、直辖市的保密行政管理部门确定

11、数字签名是对以数字形式存储的消息进行某种处理，产生一种类似于传统手书签名功效的信息处理过程。数字签名标准 DSS 中使用的签名算法 DSA 是基于 ElGamal 和 Schnorr 两个方案而设计的。当 DSA 对消息 m 的签名验证结果为 True,也不能说明（ ）。
A.接收的消息 m 无伪造
B.接收的消息 m 无篡改
C.接收的消息 m 无错误
D.接收的消息 m 无泄密

12、IP 地址分为全球地址（公有地址）和专用地址（私有地址），在文档 RFC1918 中，不属于专用地址的是 （ ）。
A. 10. 0. 0. 0 到 10. 255. 255. 255
B. 255. 0. 0. 0 到 255. 255. 255. 255
C. 172. 16. 0. 0 到 172. 31. 255. 255
D. 192. 168. 0. 0 到 192. 168. 255. 255

13、人为的安全威胁包括主动攻击和被动攻击。主动攻击是攻击者主动对信息系统实施攻击，导致信息或系统功能改变。被动攻击不会导致系统信息的篡改，系统操作与状态不会改变。以下属于被动攻击的是 （ ）。
A.嗅探
B.越权访问
C.重放攻击
D.伪装

14、确保信息仅被合法实体访问，而不被泄露给非授权的实体或供其利用的特性是指信息的（ ）。
A.完整性
B.可用性
C.保密性
D.不可抵赖性

15、安全模型是一种对安全需求与安全策略的抽象概念模型，安全策略模型一般分为自主访问控制模型和强制访问控制模型。以下属于自主访问控制模型的是 （ ）。
A. BLP 模型
B.基于角色的存取控制模型
C. BN 模型
D.访问控制矩阵模型

16、认证是证实某事是否名副其实或者是否有效的一个过程。以下关于认证的叙述中， 不正确的是（ ）。

A.认证能够有效阻止主动攻击
B.认证常用的参数有口令、标识符、生物特征等
C.认证不允许第三方参与验证过程
D.身份认证的目的是识别用户的合法性，阻止非法用户访问系统

17、虚拟专用网 VPN 是一种新型的网络安全传输技术，为数据传输和网络服务提供安全通道。VPN 架构采用的多种安全机制中，不包括（　）。
A.隧道技术
B.信息隐藏技术
C.密钥管理技术
D.身份认证技术

18、 Android 系统是一种以 Linux 为基础的开放源代码操作系统，主要用于便携智能终端设备。Android 采用分层的系统架构，其从高层到低层分别是（　）。
A.应用程序层、应用程序框架层、系统运行库层和 Linux 核心层
B.Linux 核心层、系统运行库层、应用程序框架层和应用程序层
C.应用程序框架层、应用程序层、系统运行库层和 Linux 核心层
D.Linux 核心层、系统运行库层、应用程序层和应用程序框架层

19、文件加密就是将重要的文件以密文形式存储在媒介上，对文件进行加密是一种有效的数据加密存储技术。基于 Windows 系统的是（　）。
A. AFS
B. TCFS
C. CFS
D. EFS

20、数字水印技术通过在数字化的多媒体数据中嵌入隐蔽的水印标记，可以有效实现对数字多媒体数据的版权保护功能。以下关于数字水印的描述中，不正确的是（　）。
A.隐形数字水印可应用于数据侦测与跟踪
B.在数字水印技术中，隐藏水印的数据量和鲁棒性是一对矛盾
C.秘密水印也称盲化水印，其验证过程不需要原始秘密信息
D.视频水印算法必须满足实时性的要求

21、（　）是指采用一种或多种传播手段，将大量主机感染 bot 程序，从而在控制者和被感染主机之间形成的一个可以一对多控制的网络。
A.特洛伊木马
B.僵尸网络
C. ARP 欺骗
D.网络钓鱼

22、计算机取证是指能够为法庭所接受的、存在于计算机和相关设备中的电子证据的确认、保护、提取和归档的过程。以下关于计算机取证的描述中，不正确的是（　）。
A.为了保证调查工具的完整性，需要对所有工具进行加密处理

B.计算机取证需要重构犯罪行为
C.计算机取证主要是围绕电子证据进行的
D.电子证据具有无形性

23、强制访问控制(MAC)可通过使用敏感标签对所有用户和资源强制执行安全策略。 MAC 中用户访问信息的读写关系包括下读、上写、下写和上读四种，其中用户级别高于文件级别的读写操作是 （ ）。
A.下读
B.上写
C.下写
D.上读

24、恶意代码是指为达到恶意目的而专门设计的程序或代码。以下恶意代码中，属于脚本病毒的是 （ ）。
A. Worm. Sasser, f
B. Trojan. Huigezi. a
C. Harm. formatC. f
D. Script. Redlof

25、蜜罐是一种在互联网上运行的计算机系统，是专门为吸引并诱骗那些试图非法闯入他人计算机系统的人而设计的。以下关于蜜罐的描述中，不正确的是（ ）。
A.蜜罐系统是一个包含漏洞的诱骗系统
B.蜜罐技术是一种被动防御技术
C.蜜罐可以与防火墙协作使用
D.蜜罐可以查找和发现新型攻击

26、已知 DES 算法 S 盒如下:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

如果该 S 盒的输入 110011,则其二进制输出为( )。
A. 1110
B. 1001
C. 0100
D. 0101

27、外部网关协议 BGP 是不同自治系统的路由器之间交换路由信息的协议，BGP-4 使用四种报文:打开报文、更新报文、保活报文和通知报文。其中用来确认打开报文和周期性地证实邻站关系的是（ ）。

A.打开报文
B.更新报文
C.保活报文
D.通知报文

28、电子邮件系统的邮件协议有发送协议 SMTP 和接收协议 POP3/IMAP4。SMTP 发送协议中，发送身份标识的指令是（　）。
A. SEND
B. HELP
C. HELO
D. SAML

29、（　）能有效防止重放攻击。
A.签名机制
B.时间戳机制
C.加密机制
D.压缩机制

30、智能卡的片内操作系统 COS 一般由通信管理模块、安全管理模块、应用管理摸块和文件管理模块四个部分组成。其中数据单元或记录的存储属于　（　）。
A.通信管理模块
B.安全管理模块
C.应用管理模块
D.文件管理模块

31、PKI 是一种标准的公钥密码密钥管理平台。在 PKI 中，认证中心 CA 是整个 PKI 体系中各方都承认的一个值得信赖的、公正的第三方机构。CA 的功能不包括（　）。
A.证书的颁发
B.证书的审批
C.证书的加密
D.证书的备份

32、SM2 算法是国家密码管理局于 2010 年 12 月 17 日发布的椭圆曲线公钥密码算法，在我们国家商用密码体系中被用来替换（　）算法。
A. DES
B. MD5
C. RSA
D. IDEA

33、数字证书是一种由一个可信任的权威机构签署的信息集合。PKI 中的 X. 509 数字证书的内容不包括（　）。
A.版本号
B.签名算法标识

C.证书持有者的公钥信息
D.加密算法标识

34、下列关于数字签名说法正确的是（　）。
A.数字签名不可信
B.数字签名不可改变
C.数字签名可以否认
D.数字签名易被伪造

35、含有两个密钥的 3 重 DES 加密：$C = E_{K_1}[D_{K_2}[E_{K_1}[P]]]$，其中 K1≠K2，则其有效的密钥长度为（　）。
A. 56 位
B. 112 位
C. 128 位
D. 168 位

36、 PDR 模型是一种体现主动防御思想的网络安全模型，该模型中 D 表示（　）。
A. Design（设计）
B. Detection（检测）
C. Defense（防御）
D. Defend（保护）

37、无线传感器网络 WSN 是由部署在监测区域内大量的廉价微型传感器节点组成，通过无线通信方式形成的一个多跳的自组织网络系统。以下针对 WSN 安全问题的描述中，错误的（　）。
A.通过频率切换可以有效抵御 WSN 物理层的电子干扰攻击
B.WSN 链路层容易受到拒绝服务攻击
C.分组密码算法不适合在 WSN 中使用
D.虫洞攻击是针对 WSN 路由层的一种网络攻击形式

38、有一些信息安全事件是由于信息系统中多个部分共同作用造成的，人们称这类事件为“多组件事故”，应对这类安全事件最有效的方法是（　）。
A.配置网络入侵检测系统以检测某些类型的违法或误用行为
B.使用防病毒软件，并且保持更新为最新的病毒特征码
C.将所有公共访问的服务放在网络非军事区（DMZ）
D.使用集中的日志审计工具和事件关联分析软件

39、数据备份通常可分为完全备份、增量备份、差分备份和渐进式备份几种方式。其中将系统中所有选择的数据对象进行一次全面的备份，而不管数据对象自上次备份之后是否修改过的备份方式是（　）。
A.完全备份
B.增量备份
C.差分备份

D.渐进式备份

40、IPSec 协议可以为数据传输提供数据源验证、无连接数据完整性、数据机密性、抗重播等安全服务。其实现用户认证采用的协议是（　）。
A. IKE 协议
B. ESP 协议
C. AH 协议
D. SKIP 协议

41、网页木马是一种通过攻击浏览器或浏览器外挂程序的漏洞，向目标用户机器植入木马、病毒、密码盗取等恶意程序的手段，为了要安全浏览网页，不应该 （　）。
A.定期清理浏览器缓存和上网历史记录
B.禁止使用 ActiveX 控件和_Java 脚本
C.在他人计算机上使用“自动登录”和“记住密码”功能
D.定期清理浏览器 Cookies

42、包过滤技术防火墙在过滤数据包时，一般不关心（　）。
A.数据包的源地址
B.数据包的目的地址
C.数据包的协议类型
D.数据包的内容

43、信息安全风险评估是指确定在计算机系统和网络中每一种资源缺失或遭到破坏对整个系统造成的预计损失数量，是对威胁、脆弱点以及由此带来的风险大小的评估。在信息安全风险评估中，以下说法正确的是（　）。
A.安全需求可通过安全措施得以满足，不需要结合资产价值考虑实施成本
B.风险评估要识别资产相关要素的关系，从而判断资产面临的风险大小。在对这些要素的评估过程中，不需要充分考虑与这些基本要素相关的各类属性
C.风险评估要识别资产相关要素的关系，从而判断资产面临的风险大小。在对 这些要素的评估过程中，需要充分考虑与这些基本要素相关的各类属性
D.信息系统的风险在实施了安全措施后可以降为零

44、入侵检测技术包括异常入侵检测和误用入侵检测。以下关于误用检测技术的描述中，正确的是（　）。
A.误用检测根据对用户正常行为的了解和掌握来识别入侵行为
B.误用检测根据掌握的关于入侵或攻击的知识来识别入侵行为
C.误用检测不需要建立入侵或攻击的行为特征库
D.误用检测需要建立用户的正常行为特征轮廓

45、身份认证是证实客户的真实身份与其所声称的身份是否相符的验证过程。目前，计算机及网络系统中常用的身份认证技术主要有：用户名/密码方式、智能卡认证、动态口令、生物特征认证等。其中能用于身份认证的生物特征必须具有（　）。
A.唯一性和稳定性

B.唯一性和保密性
C.保密性和完整性
D.稳定性和完整性

46、无论是哪一种 Web 服务器，都会受到 HTTP 协议本身安全问题的困扰，这样的信息系统安全漏洞属于（　）。
A.开发型漏洞
B.运行型漏洞
C.设计型漏洞
D.验证型漏洞

47、互联网上通信双方不仅需要知道对方的地址，也需要知道通信程序的端口号。以下关于端口的描述中，不正确的是（　）。
A.端口可以泄露网络信息
B.端口不能复用
C.端口是标识服务的地址
D.端口是网络套接字的重要组成部分

48、安全电子交易协议 SET 中采用的公钥密码算法是 RSA,采用的私钥密码算法是 DES，其所使用的 DES 有效密钥长度是（　）。
A. 48 位
B. 56 位
C. 64 位
D. 128 位

49、Windows 系统的用户管理配置中，有多项安全设置，其中密码和帐户锁定安全选项设置属于（　）。
A.本地策略
B.公钥策略
C.软件限制策略
D.帐户策略

50、中间人攻击就是在通信双方毫无察觉的情况下，通过拦截正常的网络通信数据，进而对数据进行嗅探或篡改。以下属于中间人攻击的是（　）。
A.DNS 欺骗
B.社会工程攻击
C.网络钓鱼
D.旁注攻击

51、APT 攻击是一种以商业或者政治目的为前提的特定攻击，其中攻击者采用口令窃听、漏洞攻击等方式尝试进一步入侵组织内部的个人电脑和服务器，不断提升自己的权限，直至获得核心电脑和服务器控制权的过程被称为（　）。
A.情报收集

B.防线突破
C.横向渗透
D.通道建立

52、无线局域网鉴别和保密体系 WAPI 是一种安全协议，也是我国无线局域网安全强制性标准，以下关于 WAPI 的描述中，正确的是（　）。
A. WAPI 系统中，鉴权服务器 AS 负责证书的颁发、验证和撤销
B.WAPI 与 WIFI 认证方式类似，均采用单向加密的认证技术
C.WAPI 中，WPI 采用 RSA 算法进行加解密操作
D.WAPI 从应用模式上分为单点式、分布式和集中式

53、Snort 是一款开源的网络入侵检测系统，它能够执行实时流量分析和 IP 协议网络的数据包记录。以下不属于 Snort 配置模式的是（　）。
A.嗅探
B.包记录
C.分布式入侵检测
D.网络入侵检测

54、 SSL 协议（安全套接层协议）是 Netscape 公司推出的一种安全通信协议，以下服务中，SSL 协议不能提供的是（　）。
A.用户和服务器的合法性认证服务
B.加密数据服务以隐藏被传输的数据
C.维护数据的完整性
D.基于 UDP 应用的安全保护

55、 IPSec 属于（　）的安全解决方案。
A.网络层
B.传输层
C.应用层
D.物理层

56、物理安全是计算机信息系统安全的前提，物理安全主要包括场地安全、设备安全和介质安全。以下属于介质安全的是（　）。
A.抗电磁干扰
B.防电磁信息泄露
C.磁盘加密技术
D.电源保护

57、以下关于网络欺骗的描述中，不正确的是（　）。
A. Web 欺骗是一种社会工程攻击
B.DNS 欺骗通过入侵网站服务器实现对网站内容的篡改
C.邮件欺骗可以远程登录邮件服务器的端口 25
D.采用双向绑定的方法可以有效阻止 ARP 欺骗

58、在我国，依据《中华人民共和国标准化法》可以将标准划分为：国家标准、行业 标准、地方标准和企业标准 4 个层次。《信息安全技术信息系统安全等级保护基本要求》 （GB/T 22239-2008）属于（ ）。
A.国家标准
B.行业标准
C.地方标准
D.企业标准

59、安全电子交易协议 SET 是由 VISA 和 MasterCard 两大信用卡组织联合开发的电子商务安全协议。以下关于 SET 的叙述中，不正确的是（ ）。
A. SET 协议中定义了参与者之间的消息协议
B.SET 协议能够解决多方认证问题
C.SET 协议规定交易双方通过问答机制获取对方的公开密钥
D.在 SET 中使用的密码技术包括对称加密、数字签名、数字信封技术等

60、PKI 中撤销证书是通过维护一个证书撤销列表 CRL 来实现的。以下不会导致证书被撤销的是（ ）。
A.密钥泄漏
B.系统升级
C.证书到期
D.从属变更

61、以下关于虚拟专用网 VPN 描述错误的是（ ）。
A. VPN 不能在防火墙上实现
B.链路加密可以用来实现 VPN
C.IP 层加密可以用来实现 VPN
D. VPN 提供机密性保护

62、常见的恶意代码类型有：特洛伊木马、蠕虫、病毒、后门、Rootkit、僵尸程序、 广告软件。2017 年 5 月爆发的恶意代码 WannaCry 勒索软件属于（ ）。
A.特洛伊木马
B.蠕虫
C.后门
D. Rootkit

63、防火墙的安全规则由匹配条件和处理方式两部分组成。当网络流量与当前的规则匹配时，就必须采用规则中的处理方式进行处理。其中，拒绝数据包或信息通过，并且通 知信息源该信息被禁止的处理方式是（ ）。
A. Accept
B. Reject
C. Refuse
D. Drop

64、网络流量是单位时间内通过网络设备或传输介质的信息量。网络流量状况是网络中的重要信息，利用流量监测获得的数据，不能实现的目标是（　）。
A.负载监测
B.网络纠错
C.日志监测
D.入侵检测

65、在下图给出的加密过程中 M_i, i=1, 2, …, n 表示明文分组，C_i, i=1, 2, …, n 表示密文分组，IV 表示初始序列，K 表示密钥，E 表示分组加密。该分组加密过程的工作模式是（　）。

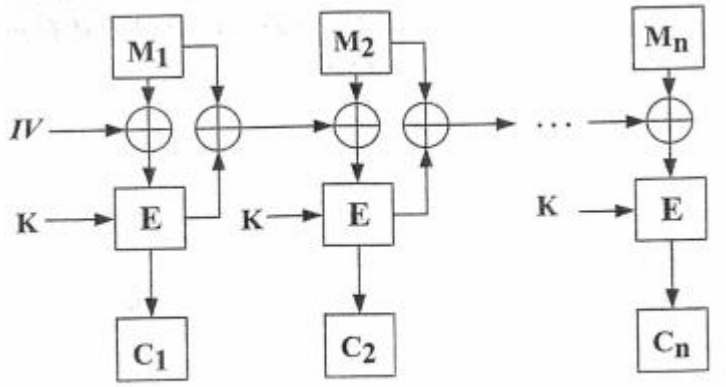

图 分组加密过程

A. ECB
B. CTR
C. CFB
D. PCBC

66、目前网络安全形势日趋复杂，攻击手段和攻击工具层出不穷，攻击工具日益先进，攻击者需要的技能日趋下降。以下关于网络攻防的描述中，不正确的是（　）。
A.嗅探器 Sniffer 工作的前提是网络必须是共享以太网
B.加密技术可以有效抵御各类系统攻击
C.APT 的全称是高级持续性威胁
D.同步包风暴(SYN Flooding)的攻击来源无法定位

67、（　）攻击是指借助于客户机/服务器技术,将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。
A.缓冲区溢出
B.分布式拒绝服务
C.拒绝服务
D. 口令

68 如果对一个密码体制的破译依赖于对某一个经过深入研究的数学难题的解决，就认为相应的密码体制是（　）的。

A.计算安全
B.可证明安全
C.无条件安全
D.绝对安全

69、移位密码的加密对象为英文字母，移位密码采用对明文消息的每一个英文字母向前推移固定化 y 位的方式实现加密。设 key=3，则对应明文 MATH 的密文为(　)。
A. OCVJ
B. QEXL
C. PDWK
D. RFYM

70、基于公开密钥的数字签名算法对消息进行签名和验证时，正确的签名和验证方式是(　)。
A.发送方用自己的公开密钥签名，接收方用发送方的公开密钥验证
B.发送方用自己的私有密钥签名，接收方用自己的私有密钥验证
C.发送方用接收方的公开密钥签名，接收方用自己的私有密钥验证
D.发送方用自己的私有密钥签名，接收方用发送方的公开密钥验证

71-75、The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. A block cipher is, in a sense, a modern embodiment of Alberti's polyalphabetic cipher: block ciphers take as input a block of (　) and a key, and output a block of ciphertext of the same size. Since messages are almost always longer than a single block, some method of knitting together successive blocks is required. Several have been developed, some with better security in one aspect or another than others. They are the mode of operations and must be carefully considered when using a block cipher in a cryptosystem.
The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are(　)designs which have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted). Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken. See Category: Block ciphers.
Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined (　)the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output(　)is created based on an internal state which changes as the cipher operates. That state change is controlled by the key, and, in some stream ciphers, by the plaintext stream as well. RC4 is an example of a well-known, and widely used, stream cipher; see Category: Stream ciphers.
Cryptographic hash functions (often called message digest functions) do not necessarily use keys, but are a related and important class of cryptographic

algorithms. They take input data (often an entire message), and output a short fixed length hash, and do so as a one-way function. For good ones, ( ) (two plaintexts which produce the same hash) are extremely difficult to find.
Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key is used to authenticate the hash value on receipt. These block an attack against plain hash functions.
A. plaintext
B. ciphertext
C. data
D. hash

A. stream cipher
B. hash function
C. Message authentication code
D. Block cipher

A. of
B. for
C. with
D. in

A. hash
B. stream
C. ciphertext
D. plaintext

A. collisons
B. image
C. preimage
D. solution