学号：_____ 姓名：_____ 专业班级：_____ 学院：_____

装 订 线 内 不 要 答 题

浙江农林大学继续教育学院考试卷（一）

课程名称：电子商务安全与支付 层次:本科学习形式:函授考试方式：开卷

注意事项： 1.本试卷满分 100 分。
2.考试时间 120 分钟。

题号	一	二	三	四	五	六	得分
得分							
评阅人							

一、单项选择题（每题 1.5 分，共 15 分）

题号	1	2	3	4	5	6	7	8	9	10
答案	A	C	D	B	A	B	B	C	D	C

1．在电子商务活动中，持卡人给商家发送订购信息和自己的付款账户信息，但不愿让商家看到自己的付款账户信息，也不愿让处理商家付款信息的第三方看到订货信息，这时可采用（ ）技术解决这个问题。

A．双重签名 B.盲签名 C．定向签名 D.多重签名

2．以下（ ）不是数字签名的主要特点。

A.不可伪造 B.不可抵赖

C.可重用 D.可验证

3．实现不可否认的技术主要是( ) 。

A．数据加密 B．数字水印 C．身份认证 D．数字签名

4．移动支付中使用的移动设备不包括（ ）。

A．手机 B．固定电话

C．iPAD D．PDA

5．FEDWIRE 是一个（ ）。

A．美元国际支付系统 B．英镑票据清算系统

C．传递银行间金融交易的电信系统

D. 欧元区各成员国中央银行的大批量实时清算系统

6. 下列安全性最高的防火墙是（　　）。

A. 屏蔽路由器　　B.屏蔽子网　C.屏蔽主机　D.双宿主主机

7. 在 SSL 中，对数据进行封装.压缩.认证和加密的是（　　）。

A. 握手协议　B. 记录协议

C. 报警协议　D. 更改密码规程协议

8. 下列不属于贷记支付的是（　　）。

A. 网络银行支付　　B. 银行卡支付

C. 代扣水费　　D. 第三方支付平台支付

9. 下列不属于 RA 功能的是（　　）。

A. 对数字证书申请人进行合法性确认

B. 注册.注销.批准或拒绝对用户数字证书属性的变更要求

C. 批准生成密钥对和数字证书的请求及恢复备份密钥的请求

D. 向申请者颁发数字证书

10. 下图中用到的移动支付技术是（　　）。

A. 红外线　　B. 蓝牙

C. NFC　　D. WLAN

二、多项选择题（每题 3 分，共 15 分）

题号	1	2	3	4	5
答案	ABC	BCD	AB	ABCDE	ACD

1. VPN 有哪几种类型（　　）。

A. Access VPN　　B. Intranet VPN

C. Extranet VPN　　D. Internet VPN

2. 支付过程包括下述 （　　）过程。

A. 交换　B. 交易　C. 清算　D. 结算　E. 收款

3. 在电子商务中,非对称加密技术通常用于（　　）场景。

A.加密大量数据　　B.加密通信会话的密钥

C.数字签名　　D.验证数字签名的真实性

4. 电子现金的特点是（　　）。

A. 独立性与多功能性　　B. 匿名性　　C.灵活性

D. 经济性与较高效率　　E.较好的安全性

5. 下列（　　）是对称加密的算法。

A. DES　　B. RSA　　C. AES　　D. 三重 DES

三、判断题（每题 1.5 分，共 15 分）

本题型暂无复习资料。

四、名词解释（每题 3 分，共 15 分）

本题型暂无复习资料。

五、简答题（每题 5 分，共 20 分）

1.简述电子商务的安全需求及应对技术。

答：(1)身份可认证性 可采用数字证书技术（1 分）

（2）保密性 可采用加密技术（1 分）

（3）完整性 可采用数字摘要技术（1 分）

（4）不可否认性 可采用数字签名技术（1 分）

（5）可控性 可采用防火墙技术（1 分）

2、简述信用卡在线支付 SET 模式的优缺点。

答：优点：（1）每一步骤都通过数字证书验证对方身份，达到了电子支付安全性的要求；

（2）使用双重数字签名，商家只能看到被允许看到的订单信息，而无法看到信用卡信息。商家只能够将信用卡信息传递到银行，由银行解密得到其中的明文。（2.5）

缺点：（1）在一个 SET 交易过程中，耗时较长，完成一个 SET 的过程耗时 1-2 分钟，

甚至需要更多的时间。

（2）由于 SET 协议过于复杂，使用麻烦，成本较高，一般只适用于具有电子钱包的客户使用。（2.5 分）

3、简述数字摘要的含义及其特点。

答：数字摘要又叫消息摘要，利用单向的散列函数（hash 函数，哈希函数）将需要加密的明文“摘要”成一串固定长度（如 128 位）的散列值，称为数字摘要。(2 分)

特点：（1）根据所用的散列函数，生成的散列值有固定的长度。（1 分）

（2）一定信息的散列值具有惟一性，即不同的信息摘要生成的散列值，其结果一定是不同的，而同样的信息其散列值则一定是一样的。（1 分）

（3）散列函数还是一种单向函数，即只能从原信息摘要成散列值，而无法从散列值还原成原信息。（1 分）

4、简述第三方支付与第三方支付平台的区别。

答：首先，第三方支付是一种支付方式，或者说是一种支付渠道。（1.5 分）在这种支付方式中，由第三方独立机构担当买卖双发的“信用中介”，同事提供与多家银行支付结算系统的对接。第三方支付平台则是由网络、技术、软件、服务等构成的实现第三方支付的平台系统。（1 分）

其次，第三方支付平台是第三方支付这种支付方式得以实现所必需的媒介。（1.5 分）没有第三方支付平台，第三方支付只能停留在理论层面，而不能真正付诸实施。（1 分）

六. 论述题（每题 10 分，共 20 分）

1、论述防火墙的功能及其安全策略。

答：(1) 过滤进、出网络的数据；

(2) 管理进、出网络的访问行为；

(3) 封堵某些禁止的业务；

(4) 记录通过防火墙的信息内容和活动；

(5) 对网络攻击检测和告警。 （5 分）

安全策略： 1）一切未被允许的都是禁止的。防火墙只允许用户访问开放的服务，其它未开放的服务都是禁止的。这种策略比较安全，因为允许访问的服务都是经过筛选的，但限制了用户使用的便利性。（2.5 分）

2) 一切未被禁止的都是允许的。防火墙允许用户访问一切未被禁止的服务，除非某项服务被明确地禁止。这种策略比较灵活，可为用户提供更多的服务，但安全性要差一些。（2.5 分）

2. 论述提升电子商务安全的措施。

答：(1)加强教育和宣传：通过大众媒体普及电子商务的安全知识，提高用户的认识。积极组织研讨会和培训课程，培养电子商务网络营销安全管理人才；

(2)采用多重网络技术：确保网络信息安全，包括网络监控、防火墙设置、加密技术等措施，以保护企业数据的安全。积极采用最新的安全技术，如人工智能、区块链等，以应对日益复杂的网络攻击。

(3)健全法律法规：严格执法，确保电子商务平台遵守相关法律法规，防范网络违法犯罪活动；

(4)支付安全：建立完善的支付系统，采用可靠的支付渠道，并加强用户身份验证。定期对支付系统进行安全性评估，及时发现和修复潜在漏洞；

(5)监管合规：遵守相关法律法规，包括个人隐私保护、电子合同签署等。加强对第三方合作伙伴的监管，确保其符合安全标准

以上每点 2 分，其余答案也可酌情给分。

学号：_____ 姓名：_____ 专业班级：_____ 学院：_____

装 订 线 内 不 要 答 题

浙江农林大学继续教育学院考试卷（二）

课程名称：电子商务安全与支付 层次:本科学习形式:函授考试方式：开卷

注意事项： 1.本试卷满分 100 分。
2.考试时间 120 分钟。

题号	一	二	三	四	五	六	得分
得分							
评阅人							

一、单项选择题（每题 1.5 分，共 15 分）

题号	1	2	3	4	5	6	7	8	9	10
答案	B	A	A	B	C	D	A	C	C	B

1．与传统的支付方式相比,以下（ ）不是电子支付的特征。

A.电子支付采用先进的技术通过数字流转来完成信息传输。

B.电子支付是在封闭的系统中运作的。

C.电子支付对软件.硬件设施的要求很高。

D.电子支付具有方便.快捷.高效.经济的优势。

2．电路级网关又称（ ）,它工作在会话层。

A.线路级网关 B.内部网关

C.外部网关 D.线路网关

3．在黑客攻击技术中，（ ）是黑客发现获得主机信息的一种最佳途径。

A. 端口扫描 B. 缓冲区溢出 C. 网络监听 D. 口令破解

4．电子现金的制作过程中，用到的是下列哪种签名技术（ ）。

A. 双重签名 B. 盲签名 C. 定向签名 D. 多重签名

5．SWIFT 是一个（ ）。

A. 美元国际支付系统 B. 英镑票据清算系统

C. 传递银行间金融交易信息的电信系统

D. 欧元区各成员国中央银行的大批量实时清算系统

6．在电子商务支付中,第三方支付平台的主要作用是（　　）。

A.代替银行进行资金托管

B.代替消费者进行商品购买

C.代替卖家发货

D.作为中介在买家和卖家之间转移资金

7．在 SSL 中，确定加密所用密码的是（　　）。

A．握手协议　　B．记录协议

C．报警协议　　D．更改密码规程协议

8．在电子商务中,使用数字证书的主要目的是（　　）。

A.加密通信内容　　B.压缩通信数据

C.验证通信双方的身份　　D.加速数据传输速度

9. 目前主流的的近距离移动支付技术是（　　）。

A．红外线　　B. 蓝牙　　C. NFC　　D. WLAN

10. 我国电子商务领域一部重要的电子商务综合立法是(　　)。

A.《非金融机构支付服务管理办法》

B.《中华人民共和国电子商务法》

C.《中华人民共和国消费者权益保护法》

D.《中华人民共和国电子签名法》

二、多项选择题（每题 3 分，共 15 分）

题号	1	2	3	4	5
答案	ABCD	ABD	ABCD	AD	ABC

1. 在电子商务环境中,数据备份和恢复计划的重要性体现在（　　）。

A.防止数据丢失　　B.应对自然灾害和人为错误

C.遵守数据保护法规　　D.加速系统故障后的恢复时间

2. 关于电子商务支付中的加密技术,以下（　　）是正确的。

A.对称加密使用相同的密钥进行加密和解密

B.非对称加密使用一对密钥,一个用于加密,另一个用于解密

C.加密技术可以确保数据的机密性,但不一定能确保数据的完整性

D.数字证书通常用于非对称加密中,以验证公钥的合法性

3. VPN 的实现技术包括（　　）。

A. 隧道技术　　B. 加解密技术

C. 密钥管理技术　　D. 身份认证技术

4. 防火墙系统采用哪两种安全策略？（　　）

A. 一切未被允许的都是禁止的　　B. 一切未被通过的都是非法的

C. 一切未被拒绝的都是合法的　　D. 一切未被禁止的都是允许的

5. 电子汇兑系统可分为（　　）等部分。

A.通信系统　　B.资金调拨系统

C.清算系统　　D.支付系统

三、判断题（每题 1.5 分，共 15 分）

本题型暂无复习资料。

四、名词解释（每题 3 分，共 15 分）

本题型暂无复习资料。

五、简答题（每题 5 分，共 20 分）

1. 简述 SSL 协议的功能。

答：服务器认证:允许客户机确认服务器身份，支持 SSL 协议的客户机软件能使用公钥密码技术来检查服务器的数字证书，判断其是否是由客户所信任的合法认证机构所发的。（2 分）

确认用户身份：支持 SSL 协议的服务器软件也能使用公钥密码技术检查客户所持数字证书的合法性。（2 分） 保证数据传输的机密性和完整性。（1 分）

2.简述交易不可否认性的含义以及保证方法（至少说明一种方法）。

答：不可否认性是指在由收发双方所组成的系统中，确保任何一方无法抵赖自己曾经作过的操作，从而防止中途欺骗的特性。（2 分）网络支付系统中的不可否认性是一般是使用数字签名数字证书，确保是该用户在操作，现在一般都是数字证书+密码，以保证账户的安全性。只要是使用了数字证书和密码操作的交易，就说明了是该用户发起请求，因为同时具备了这个条件，不可否认是该用 户在进行操作。（3 分）

3. 简述电子合同的基本特征。
答：（1）电子合同的要约和承诺是以数据电文的形式通过互联网进行的；（2）电子合同的交易主体 具有虚拟性和广泛性；（3）电子合同的成立、变更和解除无须采用传统的书面形式；（4）电子合同生效的 方式、时间和地点与传统合同不同，不需要经过传统的签字；（5）电子合同必须设定相应的标准，需要相应的技术支持。（每点各 1 分）

4. 简述合并账单支付模式的优点。
答：（1）支付方式非常方便，只需要输入自己网络介入的用户名和密码即可；（1 分）
（2）合并账单模式是一种延迟付款的方式，因此付款人可先利用该现金于其他用途或得到消费额度最多一个月的利息收入；（2 分）
（3）ICP 可对消费者缴费信用状况事先评估，信用不佳者可拒绝提供服务。（2 分）

六、论述题（每题 10 分，共 20 分）

1.论述电子支付的特点。
答：(1) 电子支付是采用先进的技术通过数字流转来完成信息传输的，其各种支付方式都是采用数字化的方式进行款项支付的；而传统的支付方式则是通过现金的流转、票据的转让及银行的汇兑等物理实体的流转来完成款项支付的。（2.5 分）
(2) 电子支付的工作环境是基于一个开放的系统平台（即因特网）之中；而传统支付则是在较为封闭的系统中运作。（2.5 分）
(3) 电子支付对软、硬件设施的要求很高，一般要求有联网的终端、相关的软件及其他一些配套设施；而传统支付则没有这么高的要求。（2.5 分）
(4) 电子支付具有方便、快捷、高效、经济的优势。用户只要拥有一台上网的电脑或手机，便可足不出户，在很短的时间内完成整个支付过程。支付费用仅相当于传统支付的几十分之一，甚至几百分之一。（2.5 分）

2.论述信用卡在线支付 SSL 模式的过程。
答： 1）持卡客户连接上网，在商家电子商务网站选择商品或服务，填写订货信息。
2）持卡客户确认订货单的商品与资金金额信息，在选择付款方式时选择用信用卡

方式及信用卡类别；提交后，订货单发往商家电子商务服务器。
3）商家服务器向持卡客户回复收到的订单查询 ID，但并不确认发货；商家服务器生成相应订单号，加上其他支付相关信息发往发卡银行（或借助第三方网络支付平台）。
4）在订货单提交后，持卡客户机浏览器弹出新窗口页面，提示即将建立与发卡银行端网络服务器的安全连接，SSL 协议机制接入开始。
5）持卡客户端自动验证发卡银行端网络服务器的数字证书。
6）持卡验证发卡银行端网络服务器的数字证书后，SSL 握手协议完成，意味着持卡客户端浏览器与发卡银行端网络服务器的安全连接通道已经建立，进入正式加密通信。
7）出现相应发卡银行的支付页面，显示从商家发来的相应订单号及支付金额信息，持卡客户填入自己的信用卡号以及支付密码，确认支付。
8）支付成功后，屏幕提示将离开安全的 SSL 连接。持卡客户确认离开后，持卡客户端与银行服务器的 SSL 连接结束，SSL 介入结束。
9）发卡银行在后台把相关资金转入商家资金账号，发送付款成功信息给商家。商家收到银行发来的付款成功信息后，发送收款确认信息给持卡客户，承诺发货。

学号：_____ 姓名：_____ 专业班级：_____ 学院：_____

装 订 线 内 不 要 答 题

浙江农林大学继续教育学院考试卷（三）

课程名称：电子商务安全与支付 层次:本科学习形式:函授考试方式：开卷

注意事项： 1.本试卷满分 100 分。
2.考试时间 120 分钟。

题号	一	二	三	四	五	六	得分
得分							
评阅人							

一、单项选择题（每题 1.5 分，共 15 分）

题号	1	2	3	4	5	6	7	8	9	10
答案	C	D	A	B	C	B	D	A	B	D

1．以下（ ）不是电子商务支付的特征。

A.方便 B.快捷 C.封闭性 D.经济

2．电子商务交易安全是一个（ ）过程。

A.静态 B.保护-反馈

C.保护-反馈-修正 D.保护-反馈-修正-再保护

3．SSL 协议是（ ）之间实现加密传输的协议。

A. 传输层和应用层 B. 物理层和数据层

C. 物理层和系统层 D. 物理层和网络层

4．当前流行的电子支付类型主要是（ ）之间或相互之间的流转。

A.银行金融系统和安全机构

B.支付指令在用户和电子支付机构

C.认证机构处理商家支付信息和顾客支付指令

D.网上商店的关键设备

5．下列属于扫码支付可以双离线模式的应用场景是（ ）。

A．超市收银员用扫描枪扫码支付 B. 自动贩卖机的扫码支付

C. 扫码乘公交　　D. 扫码打印出的对方二维码支付

6. 计算机病毒是能够破坏计算机正常工作的.（　　）的一组计算机指令或程序。

A. 系统自带　　B. 人为编制　　C. 机器编制　　D. 自动生成

7. 关于防火墙，以下（　　）说法是错误的。

A. 防火墙能隐藏内部 IP 地址

B. 防火墙能控制进出内外的信息流向和信息包

C. 防火墙能提供 VPN 功能

D. 防火墙能阻止来自内部的威胁

8. 以下（　　）是支付二维码的使用方式?

A.付款方主扫模式　　B.支付客户端模式

C.支付指令模式　　D.接入系统模式

9. 有关数字人民币的说法错误的是（　　）。

A. 数字人民币是数字形式的法定货币

B. 数字人民币钱包要进行实名认证

C. 数字人民币可以脱离银行账户体系独立使用

D. 数字人民币可以不通过国际资金汇兑系统完成支付

10. 关于 SET 支付模式，下列说法错误的是（　　）。

A.SET 支付主要用于 B2C 模式的支付。

B.SET 模式中使用双重签名保障买家在购物过程中的隐私安全。

C.使用 SET 支付必须在电脑上下载电子钱包软件。

D.SET 支付模式架构简单.支付速度快。

二、多项选择题（每题 3 分，共 15 分）

题号	1	2	3	4	5
答案	ABCD	ABCD	BC	ABC	ABD

1. 为提高电子商务支付安全性,第三方支付平台通常会采取（　　）措施。

A.实施多层身份验证机制　　B.对交易进行实时监控和风险评估

C.与银行建立安全的数据传输通道　　D.提供交易纠纷解决服务

2. 为了预防电子商务支付中的欺诈行为,商家可以采取哪些措施（　　）。

A.建立严格的身份验证流程

B.对交易进行实时监控和风险评估

C.提供详细的退换货政策和客户服务支持

D.鼓励用户使用第三方支付平台进行交易

3. 下列属于我国支付清算系统的是（　　）。

A. CHIPS　　B.HVPS　　C.BEPS　　D.SWIFT　　E.FEDWIRE

4. 以下（　　）措施有助于提高电子商务支付的安全性。

A.使用双重身份验证

B.定期检查支付系统和软件的安全更新

C.存储用户密码时使用哈希函数并加盐

D.允许用户通过电子邮件接收支付链接进行支付

5. 以下哪些是关于电子商务支付安全的最佳实践（　　）。

A.只在可信的网站上购物

B.使用强密码并定期更换

C.开启浏览器的“记住密码”功能以简化购物流程

D.定期检查银行账户和交易记录

三、判断题（每题 1.5 分，共 15 分）

本题型暂无复习资料。

四、名词解释（每题 3 分，共 15 分）

本题型暂无复习资料。

五、简答题（每题 5 分，共 20 分）

1. 简述常规计算机病毒的防范措施。
答：（1）建立良好的安全习惯；（2）关闭或删除系统中不需要的服务；（3）及时安装防火墙
经常升级操作系统的安全补丁；（4）使用复杂的密码；(5)使用专业的防病毒软件进行全面监控。（每点各 1 分）

2. 网络协议的安全风险。
答：1）网络协议（软件）自身的设计缺陷和实现中存在的一些安全漏洞，容易受到被不法者侵入和攻击。（2 分）2）网络协议无有效认证机制和验证通信双方真实性的功能。（1.5 分）3）网络协议缺乏保密机制，没有保护网上数据机密性的功能。（1.5 分）

3.简述数字证书的应用场合和应用流程。
答：数字证书的应用场合：（1）网上交易；（2）工商管理；（3）网上办公；（4）网上招标；（5）网上报税；（6）安全电子邮件。（2.5 分）
数字证书的应用流程：第一阶段：数字证书的注册申请；第二阶段：银行的支付中心对买家的数字证 书进行验证，通过验证后，将买家的所付款冻结在银行中。第三阶段：银行验证服务商和供货商的数字证 书后，将买家冻结在银行中的货款转到服务商和供货商的账户上，完成此项电子交易。（2.5 分）

4.第三方支付的优势。
答：(1)解决了网络时代物流和资金流时间和空间上的不对称问题、(2)有效地减少了电子商务交易中的欺诈行为、节约交易成本，(3)缩短交易周期，提高电子商务的效率、(4)促进银行业务的拓展和服务质量的提高、(5)能够较好地突破网上交易中的信用问题。（每点各 1 分）

六、论述题（每题 10 分，共 20 分）

1.论述目前常用的防火墙分类，各种防火墙的特点。
答：(1)包过滤型防火墙。包过滤型防火墙工作在 OSI 网络参考模型的网络层和传输层，它根据数据包源地址，目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件（访问控制列表）的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。 （3 分）
(2)应用网关型防火墙。应用网关型防火墙是在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时

对数据包进行必要的分析、登记和统计，形成报告。（3 分）
(3)代理服务型防火墙。主要在应用层实现，当代理服务器收到一个客户的连接请求时，先核实该请求，然后将处理后的请求转发给真实服务器，在接受真实服务器应答并做进一步处理后，再将回复交给发出请求的客户。代理服务器在外部网络和内部网络之间，发挥了中间转接的作用。（4 分）

2. 论述移动支付的业务模式。
答：分为远距离和近距离支付业务模式。
远距离支付业务模式分为以下四种。
手机银行模式，手机银行是各商业银行提供的一种主要移动支付方式。一般对用户有两项要求：用户在该商业银行拥有合法账户，用户手机支持相应的技术和协议。（1.5 分）
后台账户（包括话费账户）模式，运营商为每个手机客户建立一个与手机号码绑定的后台支付账户，用户为该帐户充值后，即可在远程合作商户购物，并从该账户进行支付。（1.5 分）
银行卡绑定模式，通过手机号码和银行卡业务密码进行缴费和消费的业务模式。（1.5 分）
虚拟帐户模式，这是一种移动用户使用在第三方支付机构开设的网上虚拟帐户进行支付的业务模式。这种模式要求用户预先将资金转帐或充值到后台服务器的虚拟帐户内，或者将该虚拟帐户与银行卡账户关联，在支付时使用该帐户进行消费。（1.5 分）
近距离支付不通过移动网络，利用近距离无线通信技术进行支付，包括接触式支付和非接触式支付，这种支付方式也就是储值卡式电子钱包支付，每个电子钱包有一个对应的后台支付账户，消费者在储值卡发行机构预存资金并获取储值卡，在购买商品或服务时，通过刷卡完成支付，支付的处理在现场进行，支付完毕，消费者即可得到商品或服务。（4 分）

学号：_____ 姓名：_____ 专业班级：_____ 学院：_____

装 订 线 内 不 要 答 题

浙江农林大学继续教育学院考试卷（四）

课程名称：电子商务安全与支付 层次:本科学习形式:函授考试方式：开卷

注意事项： 1.本试卷满分 100 分。
2.考试时间 120 分钟。

题号	一	二	三	四	五	六	得分
得分							
评阅人							

一、单项选择题（每题 1.5 分，共 15 分）

题号	1	2	3	4	5	6	7	8	9	10
答案	A	B	A	A	B	C	A	C	D	D

1．以下（　　）不是数字证书的主要用途。

A.加密通信数据　　B.验证身份

C.绑定公钥和私钥　　D.验证时间戳

2．在电子商务支付过程中,（　　）环节通常涉及交易双方的身份验证。

A.订单提交　　B.支付确认

C.订单发货　　D.交易评价

3．在中国的整个支付清算体系内，（　　）是全国各支付活动资金最终结算的核心底层系统。

A. CNAPS　　B. CIPS　　C. HVPS　　D. BEPS

4．以下（　　）加密技术最适合用于加密大量数据。

A.对称加密　　B.非对称加密

C.哈希函数　　D.两者都适合

5．（　　）最大的特点是利用互联网进行支付指令的传输,网络基础服务的发展,使得互联网支付的成本较之以前更为低廉和易于获得。

A. 电子汇兑系统　　B.互联网支付系统

C. 电话银行系统　　D.POS 系统

6．在电子商务支付中,使用第三方支付平台的好处不包括（　　）。

A.降低交易风险　　B.提高交易效率

C.隐藏交易双方的真实信息　　D.提供多种支付方式

7．.在电子商务交易中,（　　）主要用于防止信息在传输过程中被篡改。

A.哈希函数　　B.对称加密

C.非对称加密　　D.数字签名

8．电子商务交易安全保障体系是一个（　　）系统。

A.分散型　　B.密集型　　C.复合型　　D.单一型

9．在电子商务支付中，哪个环节最容易出现欺诈行为?

A.订单生成　　B.支付确认

C.订单发货　　D.交易完成后的退款

10．信用卡在线支付 SET 模式中,运用了一系列先进的安全技术与身份认证手段,不包括（　　）。

A. 私有密钥加密　　B.数字证书

C.共卡密钥加密　　D. 网络管理系统

二、多项选择题（每题 3 分，共 15 分）

题号	1	2	3	4	5
答案	ABC	ABCD	BC	ABCD	ABC

1．第三方支付平台的优势表现在哪些方面（　　）。

A.有利于降低社会交易成本　　B.有利于提高企业竞争力

C.有利于提升银行的信息化水平　　D.有利于提高安全性

2．计算机信息系统的运行安全有（　　）。

A. 系统风险管理　　B. 审计跟踪

C. 备份与恢复　　D. 应急

3．物理隔离卡主要分为（　　）。

A. 单个硬盘物理隔离卡　　B. 单硬盘物理隔离卡

C. 双硬盘物理隔离卡　　D. 多硬盘物理隔离卡

4. 传统电子支付系统有（　　）。

A. ATM 系统　　B. POS 系统

C. 电话银行系统　　D. 电子汇兑系统

5. 合并账单支付模式具有以下优点（　　）。

A.支付方式方便　　B.延迟付款

C.ICP 可对消费者缴费信用状况事先评估　　D.安全性好

三、判断题（每题 1.5 分，共 15 分）

本题型暂无复习资料。

四、名词解释（每题 3 分，共 15 分）

本题型暂无复习资料。

五、简答题（每题 5 分，共 20 分）

1. 简述如何将对称和非对称加密方式结合使用。

答：1）发送方生成一私密密钥对信息进行加密。（1 分）

2）发送方用接收方的公钥对私密密钥进行加密。（1 分）

3）发送方将加密后的密文和加密后的密钥通过网络发送给接收方。（1 分）

4）接收方用自己的私钥对加密后的密钥进行解密，得到私密密钥。（1 分）

5）接收方用得到的私密密钥对加密后的密文进行解密，得到原文信息。（1 分）

用图形表现出上述过程也给分。

2. 简述目前密钥的自动分配途径。

答：密钥分配是密钥管理中的最大问题，目前典型的有两类自动密钥分配途径：集中式分配方案和分布式分配方案。（2 分）

集中式分配方案是指利用网络中的密钥管理中心来集中管理系统中的密钥，密钥管理中心接受系统中用户的请求，为用户提供安全分配密钥的服务。（1.5 分）

分布式分配方案是指网络中各主机具有相同的地位，他们之间的密钥分配取决于他们自己的协商，不受任何其他方面的限制。（1.5 分）

3.简述信用卡支付 SSL 模式的优缺点。

答：信用卡在线支付 SSL 模式有以下优点：

（1）流程很简单，信用卡在线支付模式中，SSL 模式是流程最简单的模式；（1 分）

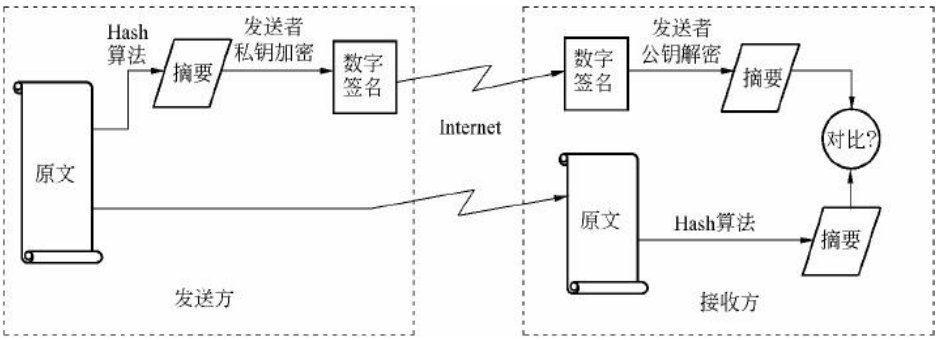
（2）架构简单，认证过程比较简便，处理速度快，费用较低；（1 分）

（3）使用方便，付款人只需在选购商品后输入卡号、有效期、姓名等资料立即就可以完成付款。（1 分）
信用卡在线支付 SSL 模式存在以下缺点：
（1）付款人的信用卡资料信息先传送到商家，再转发给银行，付款人无法确认商家是否能够保密自己的相关信息；（1 分）
（2）只能提供交易中客户与服务器间的双方认证，在涉及多方的电子交易中，SSL 协议并不能协调各方间的安全传输和信任关系。因此无法达到电子支付的“不可否认性”要求。（1 分）

4.简述 VPN 的含义及其功能。
答：VPN 被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定隧道。使用这条隧道可以对数据进行几倍加密达到安全使用互联网的目的。（2.5 分）虚拟专用网是对企业内部网的扩展。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的 内部网建立可信的安全连接，用于经济有效地连接到商业伙伴和用户的安全外联 网虚拟专用网。VPN 主要采用隧道技术、加解密技术、密钥管理技术和使用者 与设备身份认证技术。（2.5 分）

六、论述题（每题 10 分，共 20 分）

1. 结合图形说明 RSA 数字签名的过程。
答：



（图 4 分）
1）发送方通过 Hash 函数将要发送的信息摘要成一段数字摘要；
2）发送方用自己的私钥对数字摘要进行签名；
3）发送方将签名和原文信息一起传送给接收方；
4）接收方用发送方的公钥对签名进行验证，得到预期的摘要；

5）接收方将收到的原文信息用 Hash 函数摘要成实际摘要，将其和预期的摘要进行对比，如
果一致，说明信息确实是发送方所发送的，且在传递过程中没有被篡改。
（说明 6 分）

2. 论述我国加强电子商务安全建设的意义。
答：首先，保护消费者和企业的信息安全。电子商务安全建设能够保护消费者的个人信息和财务数据，防止数据泄露、篡改和未经授权的访问，增强消费者对电子商务的信任。同时，它还能保障企业商业机密和声誉，避免因安全漏洞导致的经济损失和竞争劣势。
其次，维护交易的安全性和完整性。电子商务安全建设确保交易数据的机密性、完整性和可用性，防止交易数据被篡改或伪造，保障交易的完整性和准确性。
此外，促进电子商务的健康发展。加强电子商务安全建设有利于降低交易成本，营造诚实守信的电子商务发展环境，促进“互联网+”和大众创业、万众创新健康发展 3。通过建立健全守信激励与失信惩戒制度，构建以信用为核心的市场监管体系，整顿规范电子商务市场秩序，营造良好的市场信用环境。
最后，提升国家经济竞争力。电子商务作为国民经济的重要组成部分和重要经济增长点，其健康发展对推动供给侧结构性改革、扩大有效供给、加快转变经济发展方式、激发市场主体活力、增强经济发展内生动力起到了积极的推动和引领作用。
综上所述，加强电子商务安全建设对于保护信息安全、维护交易安全、促进电子商务健康发展以及提升国家经济竞争力具有重要意义。
（以上每点各 2 分）

学号：_____ 姓名：_____ 专业班级：_____ 学院：_____

装 订 线 内 不 要 答 题

浙江农林大学继续教育学院考试卷（五）

课程名称：电子商务安全与支付 层次:本科学习形式:函授考试方式：开卷

注意事项： 1.本试卷满分 100 分。
2.考试时间 120 分钟。

题号	一	二	三	四	五	六	得分
得分							
评阅人							

一、单项选择题（每题 1.5 分，共 15 分）

题号	1	2	3	4	5	6	7	8	9	10
答案	A	C	A	B	D	B	B	D	B	C

1．电子商务安全的核心是（ ）安全。

A. 数据 B. 网络 C. 计算机 D. 系统

2．第三方支付平台的主要特点不包括（ ）。

A.支付中介 B. 中立.公正 C.成本低 D.技术中间件

3．SSL 协议是（ ）之间实现加密传输的协议。

A. 传输层和应用层 B. 物理层和数据层

C. 物理层和系统层 D. 物理层和网络层

4．在电子商务交易中,（ ）技术通常用于保障数据的机密性?

A.哈希函数 B.对称加密

C.非对称加密(公钥加密) D.两者都用于保障机密性

5．以下（ ）不是电子商务支付过程中可能遇到的风险?

A.交易欺诈 B.系统故障导致支付失败

C.自然灾害导致数据丢失 D.正常的价格变动

6．通过获取用户在 A 网站的账户而尝试登陆 B 网站，这种攻击称为（ ）。

A.拒绝服务攻击 B. 撞库 C. 缓冲区溢出攻击 D. 利用默认账号攻击

7．以下（　　）不是防火墙的主要功能?

A.访问控制　　B.数据加密　　C.入侵检测　　D.日志记录

8．公钥基础设施(PKI)的核心是（　　）。

A.数字签名　　B.密钥管理　　C.加密技术　　D.数字证书

9. 微信支付以绑定（　　）的快捷支付为基础,向用户提供安全.快捷.高效的支付服务。

A.邮箱　　B.银行卡　　C.QQ 号　　D.支付宝

10. 实际应用时一般利用（　　）加密技术进行密钥的协商和交换，利用（　　）加密技术进行用户数据的加密

A．非对称　非对称　　B．对称　　对称

C．非对称 对称　　D．对称　　非对称

二、多项选择题（每题 3 分，共 15 分）

题号	1	2	3	4	5
答案	ABD	ABC	ABCD	ABCD	ABC

1. 实体安全包括（　　）。

A. 环境安全　　B. 设备安全

C. 物理安全　　D. 媒体安全

2. 电子商务面临的主要安全问题有（　　）。

A.电子商务系统风险　　B.电子商务交易风险

C.管理与法律风险　　D.信用风险

3. CHIPS 系统有如下（　　）特点

A.允许事先存入付款指令　　B.完善的查询服务功能

C.自动化程度高　　D.安全性好

4. 电子银行安全评估的内容包括

A.安全策略　　B.内控制度建设

C.风险管理状况　　D.系统安全性

5. 在电子商务中,关于移动支付的安全性,以下说法正确的是（　　）。

A.移动支付容易受到恶意软件的攻击

B.使用生物识别技术(如指纹.面部识别)可以提高支付安全性

C.只有在可信的应用商店下载支付应用才能降低风险

D.移动支付的安全性完全依赖于支付平台的技术实力

三、判断题（每题 1.5 分，共 15 分）

本题型暂无复习资料。

四、名词解释（每题 3 分，共 15 分）

本题型暂无复习资料。

五、简答题（每题 5 分，共 20 分）

1. 简述扫码支付的原理。

答：1）用户打开支付宝 App 时，会向服务器端申请令牌种子；（1 分）

2）支付宝服务器会根据算法生成一个令牌种子，返回给支付宝 App；（1 分）

3）支付宝 App 得到令牌种子后，根据算法生成付款码(可以离线生成)（1 分）

4）付款码中含有令牌信息以及用户账户信息，服务器进行认证以此完成支付过程。（2 分）

2. 简述公钥加密技术的优缺点。

答：优点：必须由两个密钥的配合使用才能完成加解密全过程，有助于加强数据的安全性

公钥的发布不成问题，它没有特殊的发布要求，

可以在网上公开。

非对称加密可用于数字签名。（3 分）

缺点：加密和解密的速度很慢，不适合对大量的文件信息进行加密，一般只适用对少

量数据如对密钥进行加密。（2 分）

3. 简述信用卡在线支付 SSL 模式的优点。

（1）流程很简单，信用卡在线支付模式中，SSL 模式是流程最简单的模式；（1.5 分）

（2）架构简单，认证过程比较简便，处理速度快，费用较低；（1.5 分）

（3）使用方便，付款人只需在选购商品后输入卡号、有效期、姓名等资料立即就可以完成付款。（2 分）

4. 简述计算机病毒的主要传播途径？
答：（1）因特网传播：①通过电子邮件传播，②通过浏览网页和下载软件传播，③通过及时通讯软 件传播；（2）局域网传播；（3）通过不可转移的计算机硬件设备传播；（4）通过移动存储设备传播;(5)无线设备传播。（每点各一分）

六、论述题（每题 10 分，共 20 分）

1. 论述信用卡在线支付 SET 模式的过程。
（1）消费者与在线商店协商有关购买事宜；
（2）消费者利用自己的 PC 机通过因特网选定所要购买的物品，并在计算机上输入订货单，订货单上包括在线商店、购买物品名称及数量、交货时间及地点等相关信息。
（3）在线商店通过电子商务服务器作出应答，告诉消费者所填定货单的货物单价、应付款数、交货方式等信息是否准确，是否有变化。
（4）消费者选择付款方式，确认订单，签发付款指令。此时 SET 开始介入。在 SET 中，消费者必须对定单和付款指令进行数字签名。同时利用双重签名技术保证商家看不到消费者的账号信息。
（5）在线商店接受订单后，向消费者所在银行请求支付认可。信息通过支付网关到收单银行，再到电子货币发行公司确认。
（6）批准交易后，收单银行返回确认信息给在线商店。
（7）收单银行通知发卡银行请求支付。
（可酌情给分）

2.论述数字人民币与第三方支付的区别。
答：从定义和发行上区别。从货币定位看,数字人民币由中国人民银行发行，是一种和纸钞、硬币等价的法定货币，定位于流通中现金（M0），属于基础货币范畴，其法律地位与现金相同。微信支付、支付宝只是支付工具，而非数字货币。微信支付、支付宝只是依托数字技术平台提供交易、支付和清算服务，实现以法定货币计价和记账转移。（2.5 分）从发行管理上看,数字人民币由中国人民银行发行，指定运营机构负责数字人民币的运营和兑换服务，并实现可控匿名，属于双层运营体系下的混合型央行数字货币。（2.5 分）从应用客群看,数字人民币面向公众发行，可广泛地用于个人和企业等各类日常交易场景。（2.5 分）从支付角度看,数字人民币以数字形式存在，自身具有价值，且以国家信用作为担保，支持与银行账户松耦合，因此数字人民币能够作为数字化支付手段，并在一定程度上支持匿名交易。（2.5 分）

学院：_____ 专业班级：_____ 姓名：_____ 学号：_____

装 订 线 内 不 要 答 题

浙江农林大学继续教育学院考试卷（六）

课程名称：电子商务安全与支付 层次:本科学习形式:函授考试方式：开卷

注意事项： 1.本试卷满分 100 分。
2.考试时间 120 分钟。

题号	一	二	三	四	五	六	得分
得分							
评阅人							

一、单项选择题（每题 1.5 分，共 15 分）

题号	1	2	3	4	5	6	7	8	9	10
答案	B	C	B	A	B	D	C	D	A	C

1. 关于第三方支付,以下错误的说法是（ ）。

A. 第三方支付是最近几年出现的新的支付清算组织

B. 第三方支付是提供电子支付指令交换和计算的非法人组织

C. 第三方支付平台是架构在虚拟支付层上的

D. 第三方支付是典型的应用支付层架构

2．关于 NFC 下面（ ）说法是错误的。

A. NFC 是一种短距离的高频无线通信技术

B. NFC 允许电子设备之间进行接触式点对点数据传输交换数据

C. NFC 包含基于软件加密的无卡支付的便捷性

D. 用于付款和购票.用于电子票证.用于智能媒体

3．有关数字人民币的说法错误的是（ ）。

A. 数字人民币是数字形式的法定货币

B. 数字人民币钱包要进行实名认证

C. 数字人民币可以脱离银行账户体系独立使用

D. 数字人民币可以不通过国际资金汇兑系统完成支付

4．在电子商务支付系统中,为了防止重复支付,通常会采用（　　）机制。

A. 唯一交易号　　B. 支付密码　　C. 账户余额限制　　D. 验证码

5．电子商务中的安全要求最严格的层次是（　　）。

A. 网络层　　B. 应用层　　C. 传输层　　D. 数据链路层

6．在电子商务中,数字签名的主要作用是（　　）。

A. 加密信息　　B. 压缩信息大小

C. 隐藏信息内容　　D. 验证信息完整性

7．电子商务相关标准体系中,电子合同标准属于（　　）类标准

A. 基础标准　　B. 安全标准　　C. 交易标准　　D. 服务标准

8．以下（　　）不是电子商务安全的主要技术。

A. 防火墙技术　　B. 加密技术

C. 认证技术　　D. 搜索引擎优化(SEO)

9. 以下（　　）电子商务支付中的安全威胁。

A. 网络拥堵　　B. 木马病毒　　C. 钓鱼攻击　　D. 恶意软件

10. 按照（　　）的不同,电子支付可以分为卡基支付.网上支付和移动支付。

A. 基本形态　　B. 电子支付指令发起方式

C. 支付指令的传输渠道　　D. 以上都不是

二、多项选择题（每题 3 分，共 15 分）

题号	1	2	3	4	5
答案	ABCD	ABC	BCD	ABC	AC

1. 在移动支付协议中,主要的参与者有（　　）。

A.用户　　B.商家　　C.金融机构　　D.支付网关

2. 入侵检测技术的分类有（　　）。

A.以行为为基础的入侵检测技术　　B. 以主机为基础的入侵检测技术

C.以网络为基础的入侵检测技术　　D.以软件为基础的入侵检测技术

3. 在跨境电子商务支付中,通常需要考虑哪些额外的安全因素（　　）。

A.汇率波动风险　　B.不同国家的支付法规差异

C.国际交易中的欺诈风险　　D.跨境数据传输的安全性

4. 在电子商务支付过程中,为保障用户资金安全,支付平台通常会采取（　　）措施。

A.实时监控交易行为,识别异常交易

B.对大额交易进行额外的身份验证

C.提供交易保险,以应对可能的损失

D.禁止用户更改已完成的交易记录

5. 关于电子商务中的多因素身份验证(MFA)，　以下（　　）说法是正确的。

A.MFA 通过结合多种身份验证方式来提高安全性

B.MFA 可以彻底消除账户被未经授权访问的风险

C.MFA 通常包括密码.短信验证码和生物识别等多种方式

D.MFA 是电子商务支付中保障资金安全的必要手段

三、判断题（每题 1.5 分，共 15 分）

本题型暂无复习资料。

四、名词解释（每题 3 分，共 15 分）

本题型暂无复习资料。

五、简答题（每题 5 分，共 20 分）

1. 简述数字人民币的松耦合性和法偿性的含义。

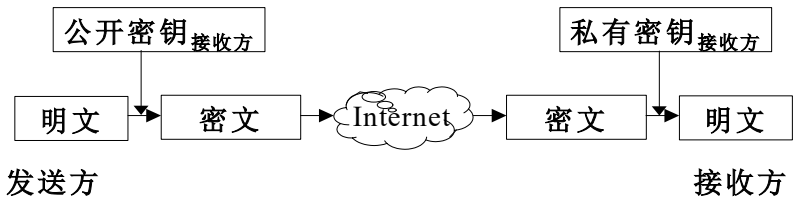
答：松耦合模式：意味着用户既可以选择将数字人民币钱包与自己已经开设的银行账户进行绑定，同时也可以选择仅凭数字人民币钱包、脱离传统银行账户体系独立使用。（2.5 分）

人民币的法偿性：中华人民共和国的法定货币是人民币。以人民币支付中华人民共和国境内的一切公共的和私人的债务，任何单位和个人不得拒收。（2.5 分）

2.简述对称加密技术的优缺点。
答：优点：效率高，算法简单，系统开销小，速度比公钥加密技术快得多，适合加密大量的数据，应用广泛。（2.5 分）
缺点：发送方和接收方必须预先共享秘密密钥，而不能让其他任何人知道。需要使用大量的密钥，密钥的发布、共享和管理困难。无法满足互不相识的人进行私人谈话的保密要求，难以解决数字签名验证的问题。（2.5 分）

3. 简述第三方支付模式的种类。
答：第三方支付有两种支付模式：网关支付模式和账户支付模式。（2 分）
网关支付模式是指第三方支付平台仅作为支付通道将买方发出的支付指令传递给银行，银行完成转账后，再将信息传递给支付平台，支付平台将支付结果通知商户并进行结算。(1 分)
账户支付模式分为两种：直付支付模式与间付支付模式。直付支付模式交易双方以虚拟账户资金进行交易付款。间付支付模式的支付平台是指承担买卖双方中间担保的第三方支付平台（2 分）

4.简述非对称加密中加密模式的过程。
答：发送方用接收方的公开密钥对要发送的信息进行加密
发送方将加密后的信息通过网络传送给接收方
接收方用自己的私有密钥对接收到的加密信息进行解密，得到信息明文 （3 分）



（2 分）

六、论述题（每题 10 分，共 20 分）

1. 论述 PKI 含义及主要组成部分的功能。
答：公钥基础设施 PKI，就是指在分布式计算环境中，使用公钥加密技术和证书的安全服务集合。（2.5 分） 一个典型的 PKI 体系结构应该包括认证中心 CA、注册机构 RA、证书持有者、 应用程序、存储仓库五个组成部分。完整的 PKI 包括认证政策的制定、认证规则、运作制度的制定、所涉及的各方法律关系内容以及技术的实现。（2.5 分）
PKI 的主要目的是，通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性。数据的机密性是指数据在传输过程中，不能被

非授权者偷看；数据的完整性是指数据在传输过程中不能被非法篡改； 数据的有效性是指数据不能被否认。（2.5 分）
一个有效的 PKI 系统必须是安全的和透明的，用户在获得加密和数字签名服务时，不需要详细地了解 PKI 是怎样管理证书和密钥的。一个典型、完整、 有效的 PKI 应用系统必须能够实现如下功能：注册、发证、密钥恢复、密钥产生、密钥更新、交叉认证、证书废止。（2.5 分）

2. 论述电子现金的支付过程。
答：（1）用户在 E-cash 发布银行开立 E-cash 账户，用现金服务器账号中预先存入的现金来购买 E-cash 证书，将 E-cash 分成若干包“硬币”。（2.5 分）（2）使用计算机 E-cash 终端软件从 E-cash 银行取出一定数量的 E-cash 存在硬盘上。（2.5 分）（3）用户与同意接受 E-cash 的厂商洽谈，签订订货合同，使用 E-cash 支付所购买商品的费 用，具体做法是卖方的公钥加密 E-cash 后，将它传送给卖方。（2.5 分）（4）接受 E-cash 的厂商与 E-cash 发送银行 之间进行清算，E-cash 银行进行现金划转。（2.5 分）