《信息安全技术》课程思政教学案例展示

（一）案例一展示

1.案例主题

现实世界和网络世界的身份识别

2.章节结合

认证理论与技术 身份认证

3.案例意义

本案例分别对现实世界和网络世界场景下身份识别进行安全分析，教育学生警惕安全风险，培养诚信、友善的价值准则。培养学生在认识身份认证的重要性的基础上，能依据不同应用场景的特点科学选择、辩证分析身份认证实现的方法和手段的安全性，从而保护个人、家庭和企业信息安全，共同践行网络安全“为人民、靠人民”的使命。以真实的案例引领学生在专业领域实践身份认证的安全设计，结合科技前沿动态，提升学生自主学习能力的培养。

4.案例教学展示

1）案例描述

1993 年,《纽约客》杂志刊登了一则漫画。画面上一条狗坐在电脑前，对着同伴说:“On the Internet, nobody knows you're a dog”，那时候，基于虚拟和匿名属性让在互联网上的人可以充分隐藏自己。

但是，随着互联网的快速发展，社交应用、网上购物、招聘等各种网站、应用服务收集用户数据成为互联网商业模式的大势，用户的隐私信息在网络上已经无处隐藏。社交网络的发展也让更多的用户接受实名制。

然而，现实却未必如愿，Facebook 爆出“泄露门”事件，韩国网站 Nate 和社交网站 Cyworld 遭到黑客攻击，约 3500 万用户的姓名、电话、邮件和身份证号码外泄，造成垃圾邮件，诈骗电话泛滥成灾。

网络世界的实名，一方面是为了约束用户的网络行为，同时也是对用户身份信息的一种保护。无论是现实世界还是网络世界，既要能正确识别用户身份，同时也要在被正确识别身份后能保护其隐私信息。

2）教学方法与教学设计

（1）教学方法

本节内容采用问题导入、案例分析、影视情境导入和讨论式教学相结合的方式。

（2）教学设计

第一步。问题引入+讨论。教师在对身份认证的目的进行简单介绍后，让同学们讨论一下：现实生活中，什么时候需要证明自己是谁，你是如何证明的？网络世界，什么时候需要证明自己是谁，你是如何证明的？

第二步，案例分析+启发。以电信诈骗（积分兑换短信诈骗）和国际象棋大师骗局（影视素材：抗战连续剧《胭脂》中蓝胭脂帮周宇浩筹集经费，机智对弈世界冠军）两个生活中的常见案例，分析身份欺诈的实施途径，认识身份欺诈带来的危害性。列举一些实际生活场景中的身份识别行为，并结合学生讲述的一些场景下实现身份识别的实现方法，归纳总结出身份认证的三种基本实现方式。

第三步，案例分析+专业反思。以2011年CSDN泄露门事件为例，反思同学们的毕业设计作品中用户注册登录模块应如何实施安全设计。

第四步，现场调查+启发讨论。调查问卷：同学们选择的手机解锁方式是什么？（即如何证明自己是机主身份）。得到统计结果，开展讨论：数字口令、指纹、人脸用于身份证明时可能存在的安全风险？归纳总结：同学们选择的证明机主身份的认证方式是否安全？

第五步，案例分析+前沿速递。在影片《碟中谍 5》中，黑客班吉在面对“步态识别系统”监测时，只能依靠汤姆扮演的伊森通过潜水强行入侵后台数据进行移库。可见，步态难以复制或伪装，成为国内外研究者关注的一种新型的生物特征识别技术，但是其识别算法准确度有待不断提升。

第六步，普法教育。《中华人民共和国个人信息保护法》第二十六条在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。《网络数据安全管理条例（征求意见稿）》第二十五条数据处理者利用生物特征进行个人身份认证的，应当对必要性、安全性进行风险评估，不得将人脸、

步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式，以强制个人同意收集其个人生物特征信息。

5. 案例反思

身份认证是安全体系中最为核心的部分,也是网络信息安全的第一道防线。教学采用以学生为中心，以目标为导向的理念。以身份认证相关理论为知识载体，培养信息安全意识，掌握信息安全风险防御能力，塑造社会主义核心价值观中的诚信、友善、自由、法治。

案例讲解借助学生周围的实际场景、真实案例、影视片段等生活化、可视化的素材激发学生参与互动分析和讨论，润物无声的思政融入，学生思政获得感增强。

（二）案例二展示

1. 案例主题

生活中的密码学

2. 章节结合

密码学概论 代替密码

3. 案例意义

本案例以实际生活中经常面临着各种密码选取之难题，引入古典密码学中的凯撒密码设计，最早期的密码。凯撒大帝不仅有卓越的军事才能更加有科学思维古人的智慧，说明适应新时代的高素质复合型人才的重要性。英国著名数学家、计算机科学之父图灵破解德军的英格尔码密码设计了图灵机，使二战提前 2 年结束。可见，密码系统于国家安全的重要性，使学生明确责任担当。《中华人民共和国密码法》自 2020 年 1 月 1 日起施行，旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。

4. 案例教学展示

1）案例描述

我们的生活中经常面临着需要输入密码的场景,银行卡取款需要输入密码,手机支付需要输入密码，QQ、微信登录需要输入密码。而不少人为了方便记

忆，往往会选择一串简单的数字 123456, 666666, 888888 或者自己的生日作为银行卡取款或手机支付的 6 位密码。这其实就等于给小偷“送钱”。网上经常可以看到一些案例，某人钱包被偷了，钱包里有银行卡和身份证，很快卡里的钱就被小偷取走了，因为小偷很轻松输入身份证上登记的生日取走了卡里的钱。也就是说，这样的密码形同虚设。人们常说的这个密码在密码学中只是“口令”。

古罗马时期伟大人物的凯撒大帝，需要与前线打仗的将军们交换军事情报，为防止信使被俘虏后泄露通信的内容，设计了一种代替密码方法。其设计思想可以帮助我们设置好记并且安全的生活密码。

2）教学方法与教学设计

（1）教学方法

本节内容采用问题导入、案例分析和讨论式教学相结合的方式。

（2）教学设计

第一步。问题引入+讨论。在我们的日常生活中，经常面临着各种账户和口令的设置。提问：同学们的银行卡取款密码是如何设计的？有很多人选择自己的生日、电话号码或家庭门牌号等数字串。因为大家觉得这些数字好记不会忘，却忽略了一个问题，你的这些个人信息很多人都知道，根本不是秘密，怎么能保护你的钱财安全？

第二步，案例分析+讨论。以凯撒密码作为代替密码的典型案例，分析代替密码的设计思想，并对代替密码进行安全性分析。如，凯撒密码安全性的关键在于密钥 k 的取值。一旦 k 被泄露，密码表将被重构，因此 k 的取值就是最高机密了。

第三步，实践应用。以凯撒密码思想为例，设计生活中用于支付的数字密码。首先，选取不易遗忘的数字串作为明文，比如交大 50 周年校庆纪念日 210919。然后，选择一个密钥数字 k，比如 5，以数字做加法运算，便可得到支付密码 765464。用此方法，可以快速的设计出一串不易猜测的支付密码。

第四步，深入分析。鉴于凯撒密码密钥数字的难抗击穷举攻击的特点，可以采用改进的代替密码算法，以一个密钥短语设计密码表，提高安全性。而我们的支付密码的密钥数字也可类似处理。避免将简单数字串或个人相关信息

串设置为支付密码，也不建议将密码写在笔记本里（防止偷窥或遗失）。

第五步，普法教育。《中华人民共和国密码法》第十二条任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统。任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。

5. 案例反思

密码技术是保障网络与信息安全的核心技术和基础支撑，直接关系国家政治安全、经济安全、国防安全和信息安全。5G、物联网、云计算、大数据、人工智能、区块链等新技术新业态都与密码紧密融合。密码与老百姓日常生活也息息相关，身份认证、消费支付、网络交易、个人信息保护、财产保护等，背后都有密码在发挥着作用。

案例讲解从个人实际应用需求上升到国家安全层面，突出密码技术的重要地位及其实用价值，培养学生用科学精神武装思想，增强数据安全意识，共同维护国家安全。

（三）案例三展示

1. 案例主题

密钥的安全分发

2. 章节结合

密钥管理 密钥分配

3. 案例意义

本案例分别对现实生活和密码学中的密钥分发方式进行安全性分析，教育学生警惕安全风险，以全局和局部的辩证思想分析密钥策略。培养学生充分认识密钥的重要地位，并能依据密钥用途科学选择、辩证分析密钥分发安全策略，保护个人、家庭、企业、国家信息安全，共同践行网络安全“为人民、靠人民”的使命。以真实的生活案例警示学生明辨是非，提升自主学习能力的培养。

4. 案例教学展示

1）案例描述

对称密码体制中，收发双方使用相同的会话密钥加密需要保密的信息，那么收发双方如何通过网络得到相同的对称密钥？非对称密码体制中，为了实现消息来源的可靠性，需要发方用个人私钥加密，那么收方如何知晓发方的公钥，进行正确识别呢？非对称密码体制中，为了实现发送消息的机密性，发方需要使用收方的公钥对信息加密，那么发方如何知晓收方的正确的公钥呢？这就是密钥管理中密钥分发的安全性研究。如果无法做到密钥的安全分发，密码体制便丧失了安全性。

我们熟知的很多冒充移动或交管诈骗，冒充领导或好友诈骗，其实都属于未对电话号码或QQ号（类似密码学中的公钥）分发进行正确识别。

2）教学方法与教学设计

（1）教学方法

本节内容采用问题导入、案例分析和讨论式教学相结合的方式。

（2）教学设计

第一步。问题引入+讨论。密钥依据其所属体制和用途的不同，其分发策略存在很大差异。而制定分发策略，首先需要明确哪些密钥需要分发？发给谁？让同学们讨论一下：现实生活中和前面的课程中，大家了解了哪些密钥？你觉得其中哪些密钥需要发？发给谁？

第二步，案例分析+启发。分别以生活中的家门钥匙、汽车钥匙、安装软件的产品密钥和密码学中涉及的对称密码体制中的会话密钥、非对称密码体制中的公钥和私钥展开分析。从密钥用途推理哪些密钥需要分发。生活中的钥匙可以面对面安全分发，产品密钥只能一个电子设备使用不能分发，而密码学中的会话密钥和公钥则需要通过网络进行分发。

第三步，案例分析+启发。网络是一个不安全的信道，分析公钥在分发的过程中需要保障的安全特性是什么？列举出一些网络分发渠道，并进一步分析这些公钥分发渠道的优缺点，依据实际应用需求进行合理选择。而会话密钥的分发对安全性要求极高，根据安全风险分析，得出结论：它不但要建立在收发双方的公钥已经安全分发之后，而且需要设计基于公钥体制的握手协议和基于公钥体制的双重加密方式。

第四步，生活小常识。请同学们思考一个问题：如果你更换了手机的SIM

卡和手机号，应如何安全的将手机号告知你的朋友，同理，以什么样的方式得到的朋友手机号才是真实的号码？类似的还有QQ号、微信号、网址等的安全识别。其实，生活中的很多电信诈骗行为，都是由误信了骗子的这些信息造成的。

5.案例反思

好的密码算法都是唯密钥而保密的，因此密钥的安全管理是关键所在。密钥管理中有两个难点，一个是密钥的存储，另一个就是密钥的分发。本地使用无需分发的密钥需要保证其物理存储安全，而需要通过不可靠的网络进行分发的密钥，需要构建一个安全的分发渠道。我们将新换的手机号码通过网络告诉朋友，类似非对称密码体制中的公钥分发。而我们的手机不能随意借给他人，类似非对称密码体制中的私钥不得分发，属于密钥的存储安全。

案例讲解以学生的日常生活行为和真实案例等素材启发学生以类比的思维和辩证的思维去分析安全风险，构建安全架构，提高信息安全防御能力。