网络安全技术

朱浩瑾 刘振

上海交通大学 计算机科学与工程系

电信群楼3-509

liuzhen@sjtu.edu.cn

网络安全技术：

- 密码学基础
  - 刘振
- 密码学在区块链中的应用
  - 刘振
- 网络安全
  - 朱浩瑾

- 参考教材
  - 密码学：Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell
  - 网络安全：……

网络安全技术：

- 学习目标：
  - 理解、掌握网络安全中相关的密码学基础
  - 理解、掌握区块链技术中的密码技术的应用
  - 网络各层的攻击与防御
  - 匿名网络，隐私攻击与防护
  - 网络安全协议的实践与攻击

- 成绩评定：
  - 平时成绩60% 考勤、作业、课程设计
  - 期末成绩40% 考试

密码学与网络安全

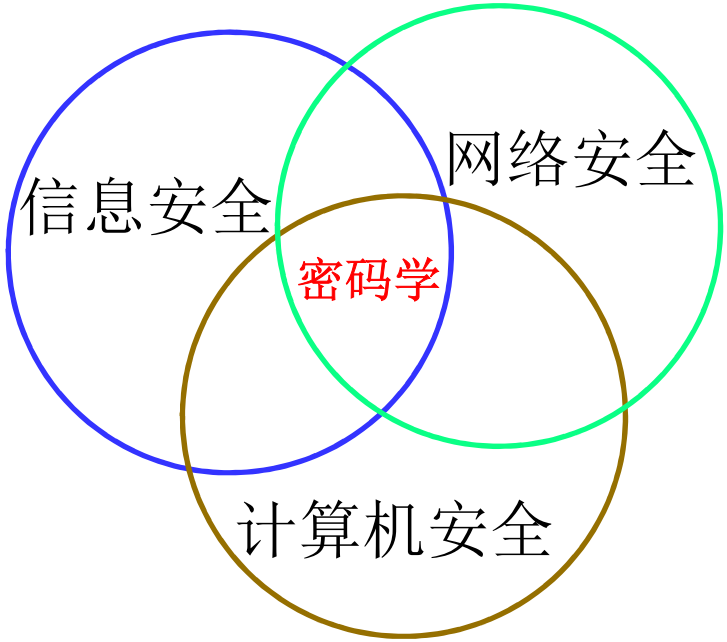
- 传统的网络安全：Network Security, 这个术语是指网络本身的安全，其中一种对网络安全威胁模型的分类为
  - 基于头部的漏洞和攻击
  - 基于协议的漏洞和攻击
  - 基于验证的漏洞和攻击
  - 基于流量的漏洞和攻击

密码学与网络安全

- 网络空间安全：Cyber Security, 是近几年全世界各国都格外重视的、国家战略层面的安全，“网络空间是继陆、海、空、天后的第五疆域”，网络空间安全包括网络相关的安全的方方面面：
  - 网络安全(Network Security)
  - 计算机安全(Computer Security)
  - 信息安全(Information Security)
  - 关键基础设施（例如 电网）的安全
  - ……

密码学与网络安全

- 密码学(Cryptography)：是实现Cyber Security的核心基础与技术之一



密码学与网络安全

- **2012年 火焰（Flame）病毒**
  - 卡巴斯基实验室2012年5月28日宣布，发现了一种破坏力巨大的全新电脑蠕虫病毒“火焰”(Flame)。
  - 这种病毒在中东地区大范围传播，其中伊朗受病毒影响最严重。**攻击的目标是伊朗能源设施，特别是核设施。**
  - “网络战早已不是一种概念，而是现实”，卡巴斯基称，这种新病毒可能是“某个国家专门开发的网络战武器”。
- Flame利用了微软的一个漏洞
  - 对自身代码进行数字签名，杀毒软件认为病毒本身拥有合法证书，从而绕过杀毒软件的查杀
  - 数字签名是一种公钥密码算法
    - 签名=sig(h(m))
    - 可能出现碰撞$h(m_1)=h(m_2)$
      - **MD5哈希算法已被攻破、不再安全**

密码学与网络安全

- **2013年斯诺登事件揭发出的美国“棱镜计划”：**
  - 美国国家安全局（NSA）和联邦调查局（FBI）于2007年启动了一个代号为“棱镜”的秘密监控项目，直接进入美国国际网络公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、苹果等在内的9家国际网络巨头皆参与其中。
  - 监听对象：包括任何在美国以外地区使用参与计划公司服务的客户，或是任何与国外人士通信的美国公民。
  - 监听内容：电邮、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料的细节。
  - 盟友也被监听：欧盟，德国总理默克尔，……
  - 中国：
    - 斯诺登向德国《明镜》周刊提供的文件表明：美国针对中国进行大规模网络进攻，并把中国领导人和华为公司列为目标。攻击的目标还包括商务部、外交部、银行和电信公司等。
    - 美国国家安全局对部分中国企业进行攻击和监听。例如为了追踪中国军方，美国国家安全局入侵了中国两家大型移动通信网络公司。因为担心华为在其设备中植入后门，美国国家安全局攻击并监听了华为公司网络，获得了客户资料、内部培训文件、内部电子邮件、甚至还有个别产品源代码。
    - 美国国家安全局还对中国顶尖高等学府清华大学的主干网络发起大规模的黑客攻击。其中2013年1月的一次攻击中，至少63部电脑和服务器被黑。中国六大骨干网之一的“中国教育和科研计算机网”就设在清华大学，清华的主干网络被黑，意味着数百万中国公民的网络数据可能失窃。

密码学与网络安全

- **2015年-2016年希拉里邮件门事件：**
  - 2015年3月，希拉里承认在任职国务卿期间使用私人邮箱处理约6万封邮件，其中3万封因涉及私人生活已被其团队删除，剩余约3万封公务邮件已于2014年底全部上交国务院。
  - 担任国务卿期间使用私人电子邮箱、而非官方电子邮箱与他人通信，涉嫌违反美国《联邦档案法》。
  - 邮件门事件在2016年美国大选中一直是一个热点问题，在一定程度上也是希拉里败给特朗普的原因之一。“希拉里的支持率每次下跌，必然有“邮件门”如影随形——无论她怎么努力，无论特朗普怎么作死，无论希拉里领先多大，邮件门统统都给拉回去了。”
  - 美国（奥巴马、希拉里）一直指责俄罗斯通过黑客泄露邮件门事件中的信息来抹黑希拉里、从而影响美国大选（帮助特朗普）。

密码学与网络安全

- **2016孟加拉央行失窃事件：**
  - 2016年2月4日，有黑客入侵孟加拉国央行开设在纽约联邦储备银行的账户，以电子转账方式，试图将近10亿美元大笔资金转入菲律宾和斯里兰卡数个账户。
  - 在黑客不断发出指令、转账进行到约8100万美元时，由于一处账户名拼写出错，转账行德意志银行起疑，继而向孟加拉国央行确认交易，孟加拉国央行这才中止转账，避免了进一步更大损失。但8100万美元已经被盗走。
  - 黑客先是攻入央行系统窃取其转移支付的安全证书，之后向纽联储接连发出数十次转账申请。

密码学与网络安全

- 加密勒索软件：

  - 黑客加密受害者的电脑的硬盘文件，向被害者勒索。
  - 黑客要求被害者支付比特币。

密码学与网络安全

- 比特币、区块链

不安全 https://coinmarketcap.com/

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$67,511,877,242	$3,844.90	$8,727,424,065	17,558,800 BTC	0.21%	
2	Ethereum	$14,514,161,204	$138.21	$4,331,637,378	105,012,738 ETH	-0.97%	
3	XRP	$13,187,132,328	$0.318794	$1,170,850,851	41,365,634,610 XRP *	4.92%	
4	EOS	$3,171,758,892	$3.50	$1,750,732,276	906,245,118 EOS *	-3.20%	
5	Litecoin	$2,760,101,865	$45.52	$1,156,239,445	60,638,561 LTC	1.37%	
6	Bitcoin Cash	$2,373,521,555	$134.53	$466,501,623	17,642,550 BCH	1.69%	
7	Tether	$2,043,197,849	$1.01	$8,453,437,621	2,021,459,017 USDT *	0.23%	

密码学与网络安全

- 比特币、区块链
  - 比特币用到的密码学
    - 数字签名
    - Hash函数
    - 比特币/数字货币是应该称作加密货币吗？
  - 保护隐私的数字货币用到的密码学
    - 数字签名变体
    - 零知识
    - 承诺
  - 区块链用到的密码学
    - ……

密码学与网络安全

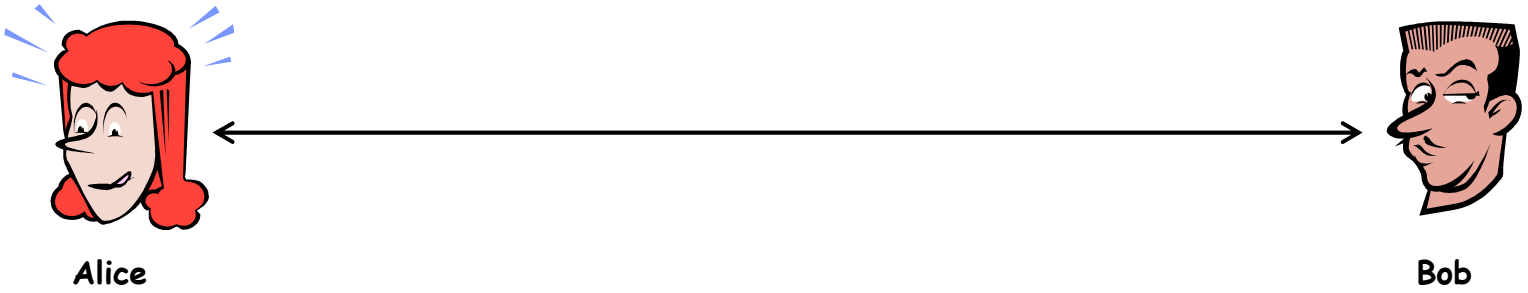
- 比特币安全性事件
  - 2014年2月，当时全球最大的比特币交易平台Mt.Gox出现巨额比特币盗窃事件。由于被窃取的**比特币数量高达85万枚**，市价约为4.8亿美元，Mt.Gox负债激增，最终陷入破产。
  - 2015年1月，欧洲比特币交易平台Bitstamp由于部分操作钱包出现泄漏，导致近**19000枚比特币**被盗。按照当时比特币270美元一枚计价，损失约500万美元。
  - 2016年8月，数字货币交易平台Bitfinex遭遇黑客攻击，近**12万枚比特币**被盗，损失高达7000万美元。
  - 2017年4月，韩国数字货币交易所Youbit首遭黑客入侵，丢失了约**4000枚比特币**。同年12月19日，该交易所再次发生黑客盗窃事件，损失了近17%的总资产。
  - 2018年1月，日本最大比特币交易所之一的Coincheck遭遇史上最大的数字货币被盗事件。根据声明，此次被盗NEM新经币总数达5.23亿个，涉及用户约26万个。按照全额补偿价格计算，补偿金额总计达463亿日元，约合**4.26亿美元**。
  - 2018年2月，意大利数字货币交易所BitGrail宣布其1700万枚NANO数字货币被盗，总价值约合**1.7亿美元**。

密码学与网络安全

- 网络空间安全日益收到重视
- 国外：
  - ……
- 国内：
  - 中央网信小组成立，网络信息安全上升为国家战略
  - 2015年乌镇世界互联网大会,习近平就共同构建网络空间命运共同体提出5点主张
  - 2016年4月19日,习近平强调树立正确的网络安全观
  - ……

主要内容

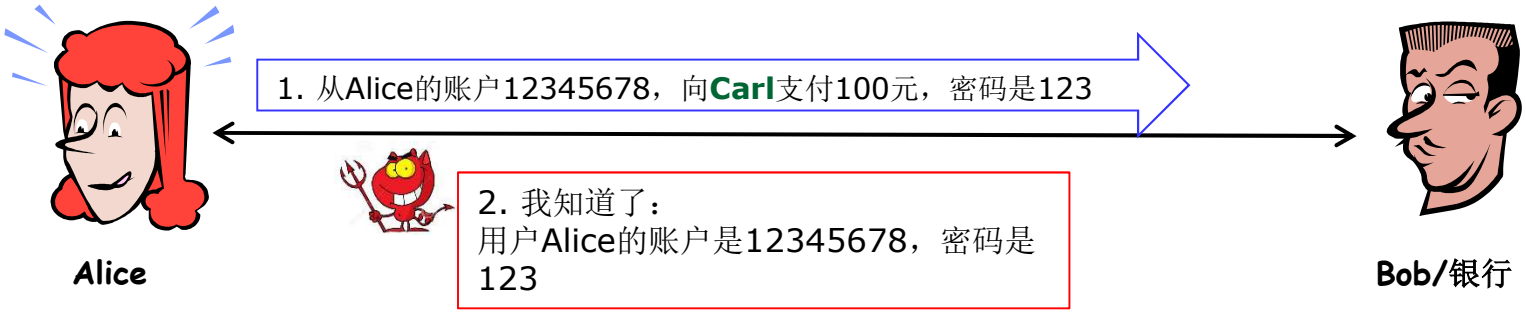
- 密码学基本问题



- 问题1：Alice/Bob： 我和Bob/Alice的通信内容有没有被别人窃听到？（数据保密性）
- 问题2：Bob：我收到的信息是Alice发给我的原始信息吗？有没有被人篡改过？（数据完整性）
- 问题3：Alice/Bob:和我通信的真的是Bob/Alice吗？（数据原发性）

主要内容

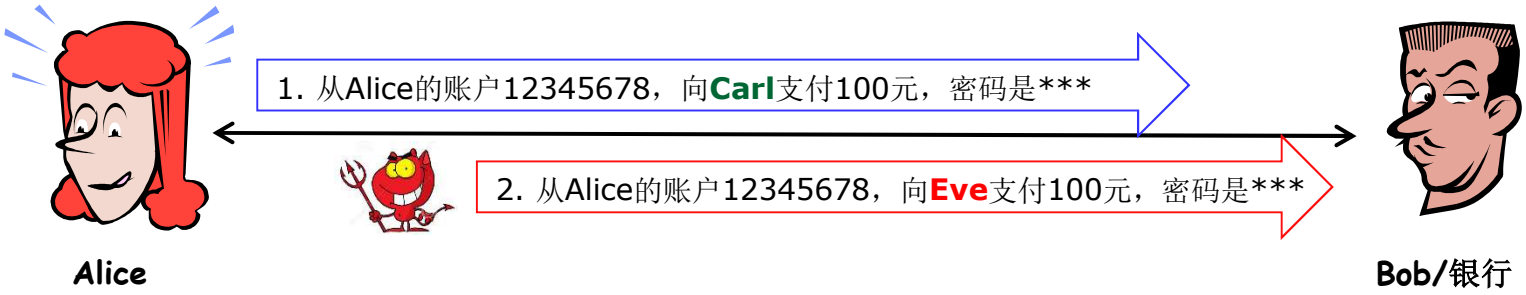
- 密码学基本问题



  - 数据保密性：防止攻击者获得/知道消息内容

主要内容

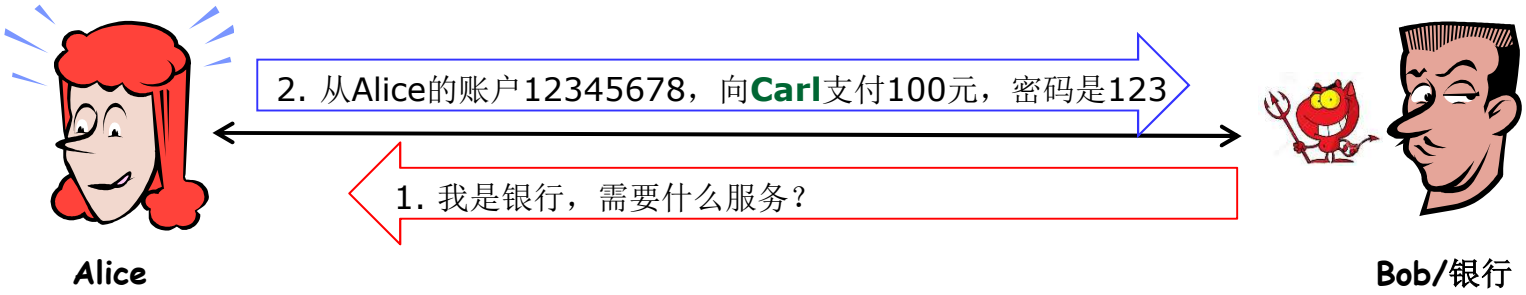
- 密码学基本问题



  - 数据完整性：防止攻击者修改消息内容

主要内容

- 密码学基本问题



  - 数据原发性：防止攻击者伪装其他合法通信对象

主要内容

- 密码学基本问题
  - 数据保密性：
    - 加密
  - 数据完整性：
    - 数字签名
    - 消息认证码
    - Hash
  - 数据原发性：
    - 数字签名
    - 消息认证码

主要内容

- 密码学其他问题
  - 隐私保护
    - 环签名
  - 安全访问控制
    - 属性基加密、同态加密、可搜索加密、……
  - 公平交易
    - 承诺
    - 零知识
  - 安全多方计算
  - 抗量子计算的密码
  - ……

本课程密码学部分主要内容

- 对称加密
- 公钥密码学数学基础
- 公钥加密
- 数字签名
- Hash
- 消息认证码
- PKI
- 身份认证
- 密钥交换
- SSL与IPSEC简介
- 区块链与数字货币中的密码技术应用