

# Modern Cryptography and Its Applications

---

**Yanwei Yu**

**E-mail: [ywyu@ustc.edu.cn](mailto:ywyu@ustc.edu.cn)**



# Outline

- **Why need Cryptography?**
  - importance
- **Where need Cryptography?**
  - practicality
- **About course**
  - Objective, Literature, Schedule, Grading Scheme, Labs, Contact us

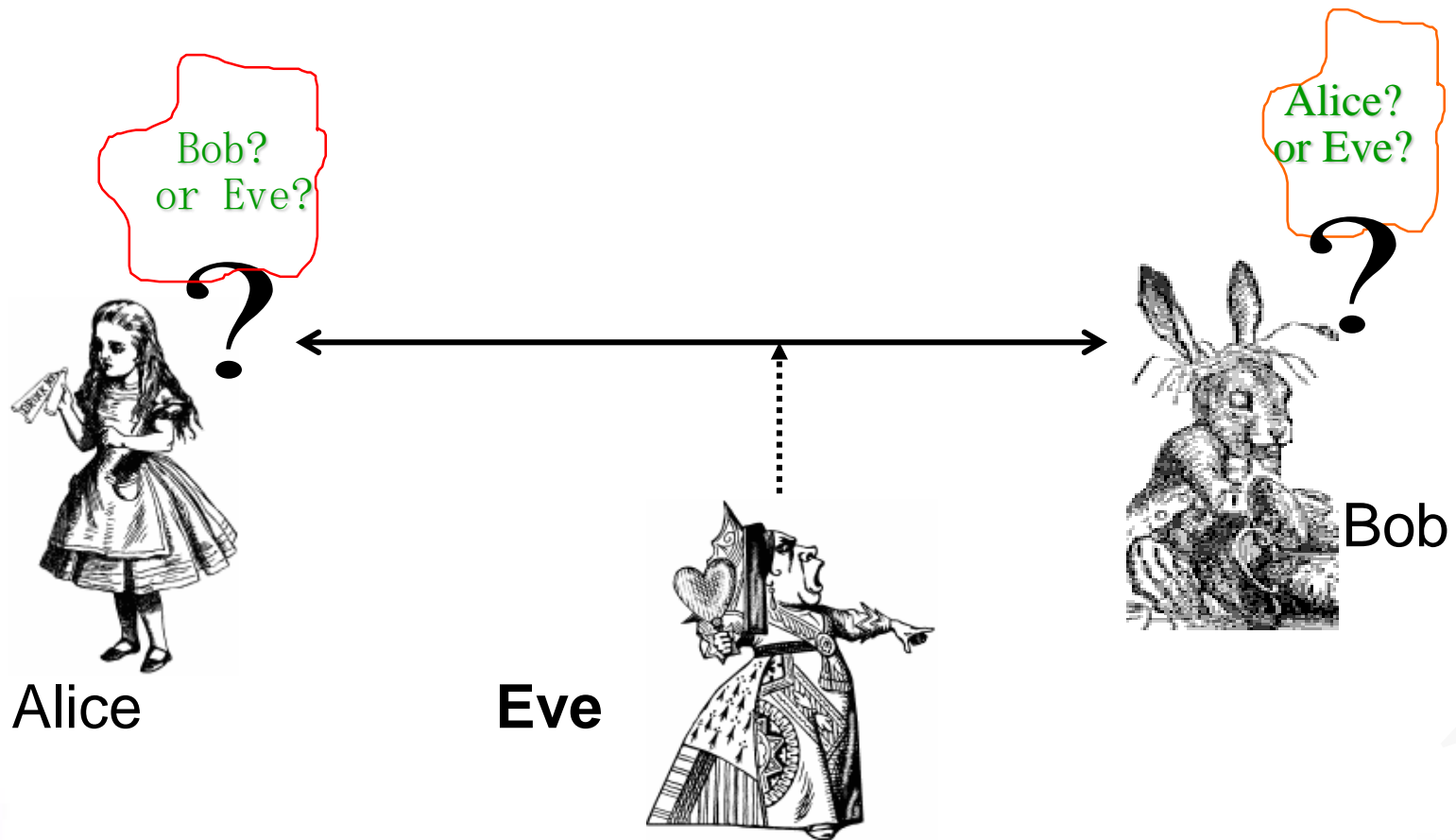


# Why need Cryptography

- **core** part in information security
- **Information security**
  - information + system security
  - protect hardware, software, **network protocol, data**
  - **Provide Security Services (X.800)**
    - **Data Confidentiality** –protection of data from unauthorized disclosure
    - **Data Integrity** - assurance that data received is as sent by an authorized entity
    - **Authentication** - assurance that the communicating entity is the one claimed
    - **Non-Repudiation** - protection against denial by one of the parties in a communication
    - **Access Control** - prevention of the unauthorized use of a resource
    - **Availability**



# Three roles in Cryptography



2021/3/8

- **Data Confidentiality /Secrecy/Privacy**
  - How Alice can send a message to Bob so that Eve won't find out the message?
- **Data Integrity**
  - How to make sure the message was not modified?
- **Authentication, Non-Repudiation**
  - **Authentication**: How Alice can send a message to Bob and Bob knows it's from Alice?
  - **Non-Repudiation**: How Alice can send a message to Bob so that Alice can't deny ever sending the message?



# Where need Cryptography

- Chat on the Internet
- Sign in/Login on web
- Home-Banking
- Home-Shopping
- Email
- Download softwares
- .....



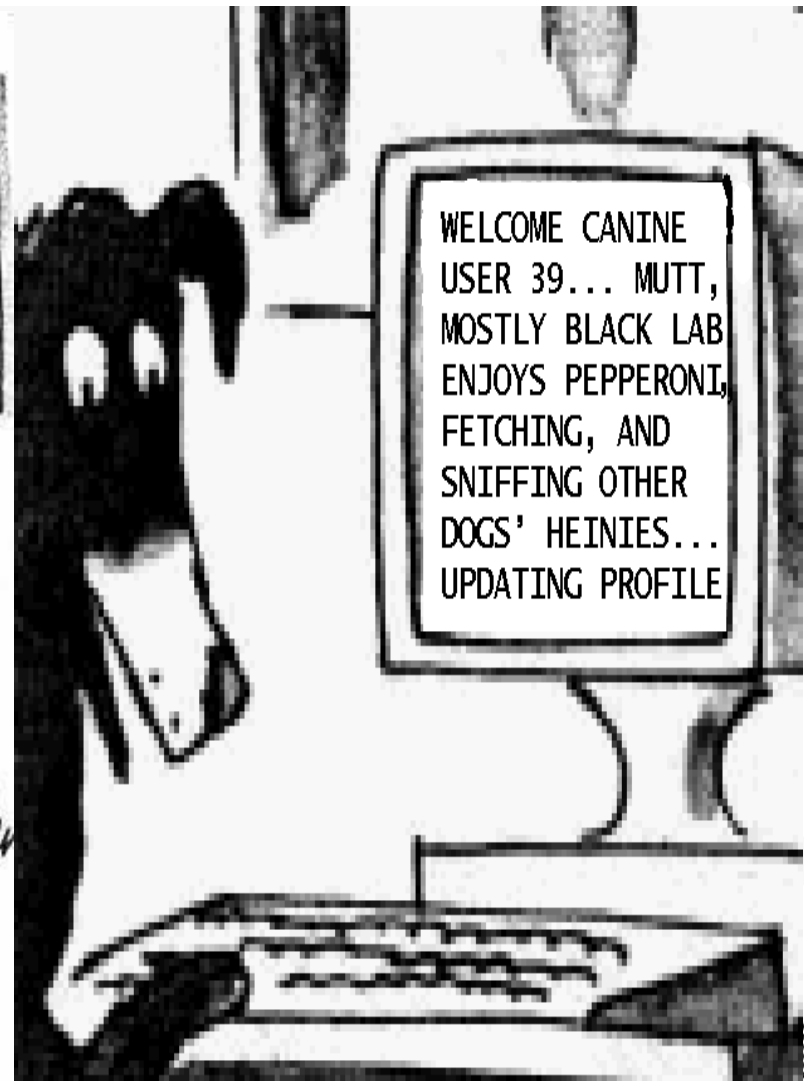
2021/3/8



# Scene1: Chat on the Internet



*"On the Internet, nobody knows you're a dog."*





# “Eve” Anywhere !



2021/3/8





# Scene2: Login on web



中国科学技术大学  
软件学院信息化平台1.0

2012年  
的版本

 用户登陆

用户名:

密 码:

验证码:

 **cA3i** [看不清楚, 换一张](#) [忘记密码?](#)



中国科学技术大学  
软件学院信息化平台

现在的版本

### 登录管理系统

账号:

密码:

验证码:

请输入4位数相加结果

☐ 在此计算机上保存我的信息



刷新



- ▶ 请使用IE 7.0、Firefox 3.6、Chrome 3.0版本以上的浏览器
  - ▶ 不支持IE6;IE10用户若登录不了, 按下F12,浏览器模式中选择IE10兼容性视图;
  - ▶ 通常账号为:学生: 学号;教师:姓名简写;
- [忘记密码?](#)

# Scene3: Sign in Taobao for new customer

Step1

2010  
年版  
本

淘宝网

1 填写账户信息

2 验证账户信息

3 注册成功

账户名:  ✓ 一旦注册成功不能修改  
9个字符

登录密码:  ✓  
弱 中 强

确认密码:  ✓

验证码:  5EX6 5EX6 ↺ 🔊

同意协议并注册

《淘宝服务协议》

中国大陆手

2021/3/8



Software Engineering

11

# Scene3: Sign in Taobao for new customer

Step2

2010  
年版本

360安全浏览器 5.0 正式版

» 文件(F) 查看

http://member1.taobao.com/member/new 可信网站

淘宝网 - 淘! 我喜欢

新会员免费注册

查找: 下一个 上一个 高亮 关闭

手机版 | 亲, 欢迎来淘宝! 请登录 免费注册

淘宝网首页 | 我要买 | 我的淘宝 | 卖家中心 | 联系客服 | 购物车

## 淘宝网

1 填写账户信息

2 验证账户信息

3 注册成功

国家/地区: 中国大陆

您的手机号码: +86

☒ 同意支付宝协议并同步创建支付宝账户

如果已有可不创建

提交

中国大陆手机

Engineering

2021/3/8

12

2010  
年版  
本

360安全浏览器 5.0 正式版

» 文件(F) 查看(V) 收

http://member1.taobao.com/member/new 可信网站

淘宝网 - 淘！我喜欢 新会员免费注册

查找: 下一个 上一个 高亮 关闭

手机版 | 亲，欢迎来到淘宝！请登录 免费注册 淘宝网首页 | 我要买 | 我的淘宝 | 卖家中心 | 联系客服

# 淘宝网

1 填写账户信息

国家/地区: 中国大陆

您的手机号码: +86

☒ 同意支付宝协议并同步创建支付宝账户  
如果已有可不创建

短信获取验证码

手机号码确认:

验证码: 请输入您收到的6位验证码

验证

如果您在1分钟内没有收到验证码, 请 [返回修改手机号码](#)  
或 [57秒后重新发送](#)



2021/3/8



Software Engineering

13

# Scene3: Sign in Taobao for new customer

Step3

2010  
年版本

360安全浏览器 5.0 正式版

» 文件(F) 查看(V)

http://member1.taobao.com/member/new 可信网站

淘宝网 - 淘！我喜欢

淘宝网 - 淘我喜欢！

查找： 下一个 上一个 高亮 关闭

手机版 | aaaa111bb

淘宝网首页 | 我要买 | 我的淘宝 | 卖家中心 | 联系客服 | 购物车 0

1 填写账户信息 2 验证账户信息 3 注册成功

恭喜您，注册成功！[去首页看看](#)

账户名： (手机号 也可作为登录账户名)

新人礼金免费拿，速速来领！[查看详情](#)

此帐号可同时用于天猫、一淘、阿里旺旺登录 [阿里旺旺是什么？](#) | [下载阿里旺旺](#)

帐号安全级别低，请完善[密保问题](#)；推荐使用[手机密令](#)，保护账户安全。

支付宝 您还未绑定支付宝  
没有绑定支付宝

- 已有支付宝账
- 没有支付宝账

2021/3/8

Software Engineering

14

淘宝网 用户注册  
Taobao.com

2021  
年版  
本

手机号码 中国大陆 +86 请输入你的手机号码

验证码 请输入校验码 获取验证码

同意协议并注册

已阅读并同意以下协议 淘宝平台服务协议、隐私权政策、  
法律声明、支付宝及客户端服务协议

切换成企业账户注册



2021/3/8



15

1 设置用户名

2 填写账号信息

3 设置支付方式

✓ 注册成功

登录名

~~123456789~~

请设置登录密码 登录时验证，保护账号信息

登录密码

设置你的登录密码



密码确认

请再次输入你的密码

强度：



- ☐ 6~20个字符
- ☐ 只能包含字母、数字以及标点符号（除空格）
- ☐ 字母、数字和标点符号至少包含2种



淘宝账户名是指什么？

忘记会员名、怎么找回？  
忘记淘宝账号密码，怎么找回？

暂不开启 立即开启  
手机（停机、丢失等）收不到验证码，怎么办？

手机、邮箱正常使用

Software Engineering

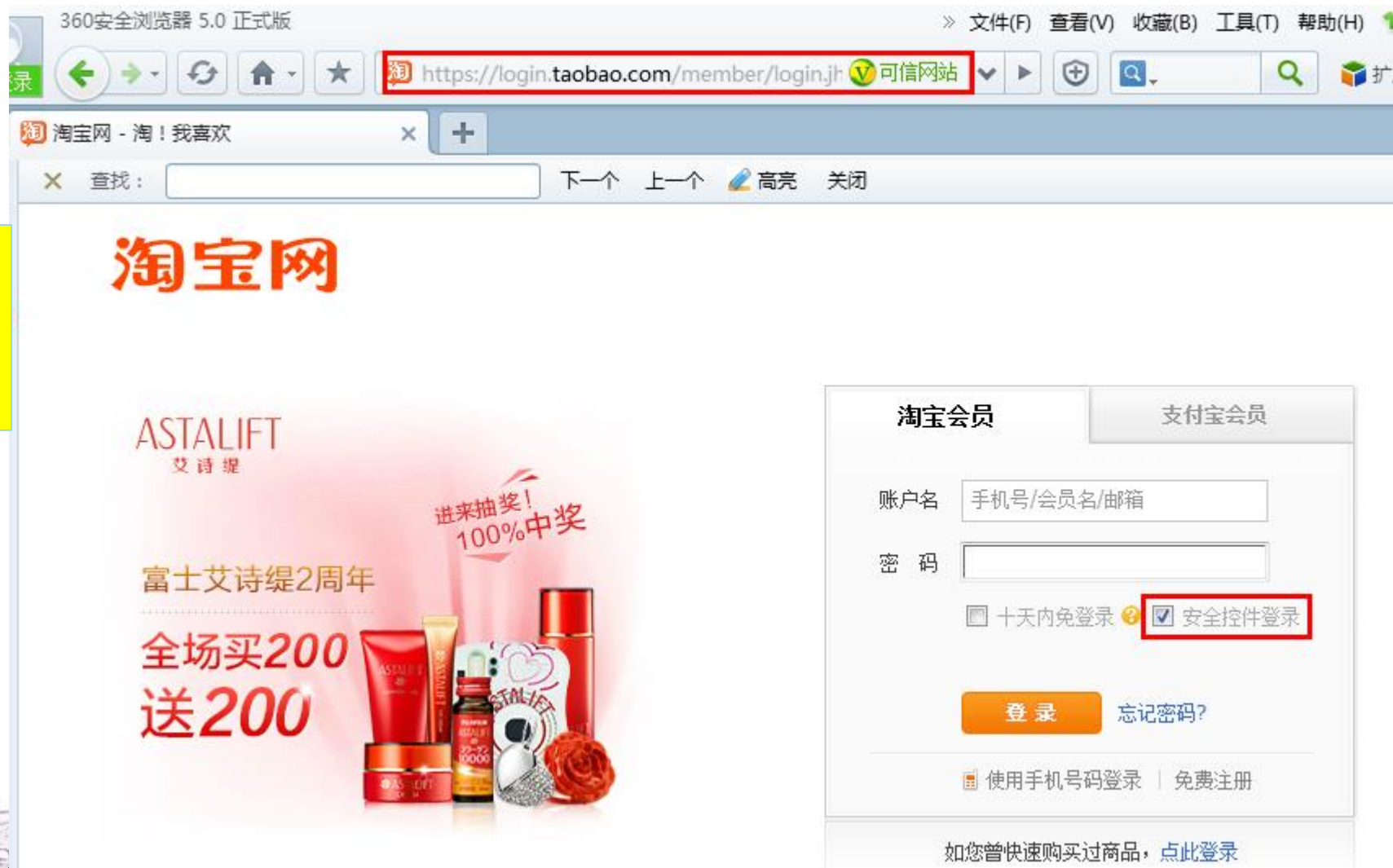
提交

2021  
年版  
本



# Scene4: Login on Taobao

2012  
年版本



2021/3/8

17

## ? 登录小提示

## • 您是否锁定了键盘的大写功能?

请检查您键盘上的"Caps Lock"或"A"灯是否亮着,如果是,请先按一下"Caps Lock"键然后重新输入。

## • 您是否忘记或不小心输入了错误的密码?

您可以通过[忘记会员名](#)或[忘记密码](#)重新设置信息。

## • 您的手机号码输入格式是否正确?

请查看[手机号码输入格式](#)

## • 无法安装控件?

请查看您是否禁用了active控件,更多问题请查看[安全控件安装指南](#)。

## • 仍然有问题?

请到[帮助中心](#)或[淘宝打听](#)获取更多帮助。

保护您的账户,请阅读[密码安全贴士](#),下载[安全浏览器](#),免费[在线杀毒](#)。

淘宝会员

支付宝会员

为了您的账号安全,请输入验证码。

账户名 MyAccount

密 码

验证码

看不清  
换一张

☒ 安全控件登录 ☐ 两周内免登录 ?

登 录

[忘记密码?](#)

使用动态密码 | [免费注册](#)

已经购买过的访客, [点此登录](#)

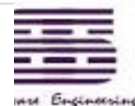
手机登录[m.taobao.com](#),随时随地购物

"登录页面"改进建议

[关于淘宝](#) [营销中心](#) [合作伙伴](#) [帮助中心](#) [诚聘英才](#) [联系我们](#) [网站地图](#) [热门品牌](#) [版权说明](#) [加入商城](#) [淘宝客](#) [交易安全](#)

阿里巴巴集团: [阿里巴巴网络](#) - [中国站](#) [国际站](#) [日文站](#) | [淘宝网](#) | [支付宝](#) | [中国雅虎](#) | [口碑网](#) | [阿里软件](#) | [阿里妈妈](#) | [集团研究中心](#)

Copyright © 2003-2011 Taobao.com 版权所有



2021  
年版本

大牌美妆  
抢! 买1享10

密码登录 短信登录

扫码登录更安全



会员名/邮箱/手机号

请输入登录密码

登录

微博登录 支付宝登录

忘记密码 忘记用户名 免费注册

# Scene5: Home-Banking

2012  
年版  
本

交通银行个人网上银行 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

地址(D) https://pbank.95559.com.cn/personbank/common\_logon.jsp

后退 搜索 收藏夹

EXPO 2010 SHANGHAI CHINA

交通銀行  
BANK OF COMMUNICATIONS  
中国2010年上海世博会全球合作伙伴  
Global Partner of Expo 2010 Shanghai China

金融快线  
BOCOM EXPRESS

个人网上银行登录

短信密码用户登录 证书用户登录 普通用户登录

卡号:

登录密码:

附加码:

安装安全控件

设置登录密码

PEFK8  
点击图片刷新附加码

若您知晓并愿意遵守《交通银行股份有限公司个人电子银行服务协议》、  
《交通银行股份有限公司个人电子银行交易规则》，请点击“登录”进入  
交行个人网上银行。

登录 忘记登录密码

新手指南  
网银向导  
帮助中心  
证书下载  
世博预付卡查询  
动态演示

2021/3/8

Software Engineering

20





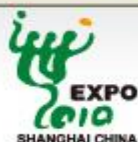
电子银行口令卡正面



电子银行口令卡背面  
(覆膜剥开后的示意图)



2012  
年版  
本



中国2010年上海世博会全球合作伙伴  
Global Partner of Expo 2010 Shanghai China

## 个人网上银行登录



短信密码用户登录



证书用户登录



普通用户登录

卡号:

登录密码:

附加码:



安装安全控件



设置登录密码

PEFK8

点击图片刷新附加码

若您知晓并愿意遵守《交通银行股份有限公司个人电子银行服务协议》、  
《交通银行股份有限公司个人电子银行交易规则》，请点击“登录”进入  
交行个人网上银行。

登 录

忘记登录密码



新手指南



网银向导



帮助中心



证书下载



世博预付卡查询



动态演示



交通银行手机银行

支付简单 理财多样  
转账方便 服务贴心



扫描二维码下载APP

用户名登录

证书登录

昵称/手机号/银行卡号/身份证

如您无法输入密码请下载并安装控件

请输入验证码



登录

新用户注册

找回用户名 | 忘记密码

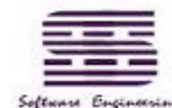


网银向导

用户指南

2019  
年版  
本

2021/3/8



22

# Scene6: Home-Shopping

- Using electronic cash
  - non-digital goods (e.g., books, CDs)
  - services (e.g., travel reservations)
  - digital goods (e.g., software, music, video)
  - micropayments (e.g., database access)

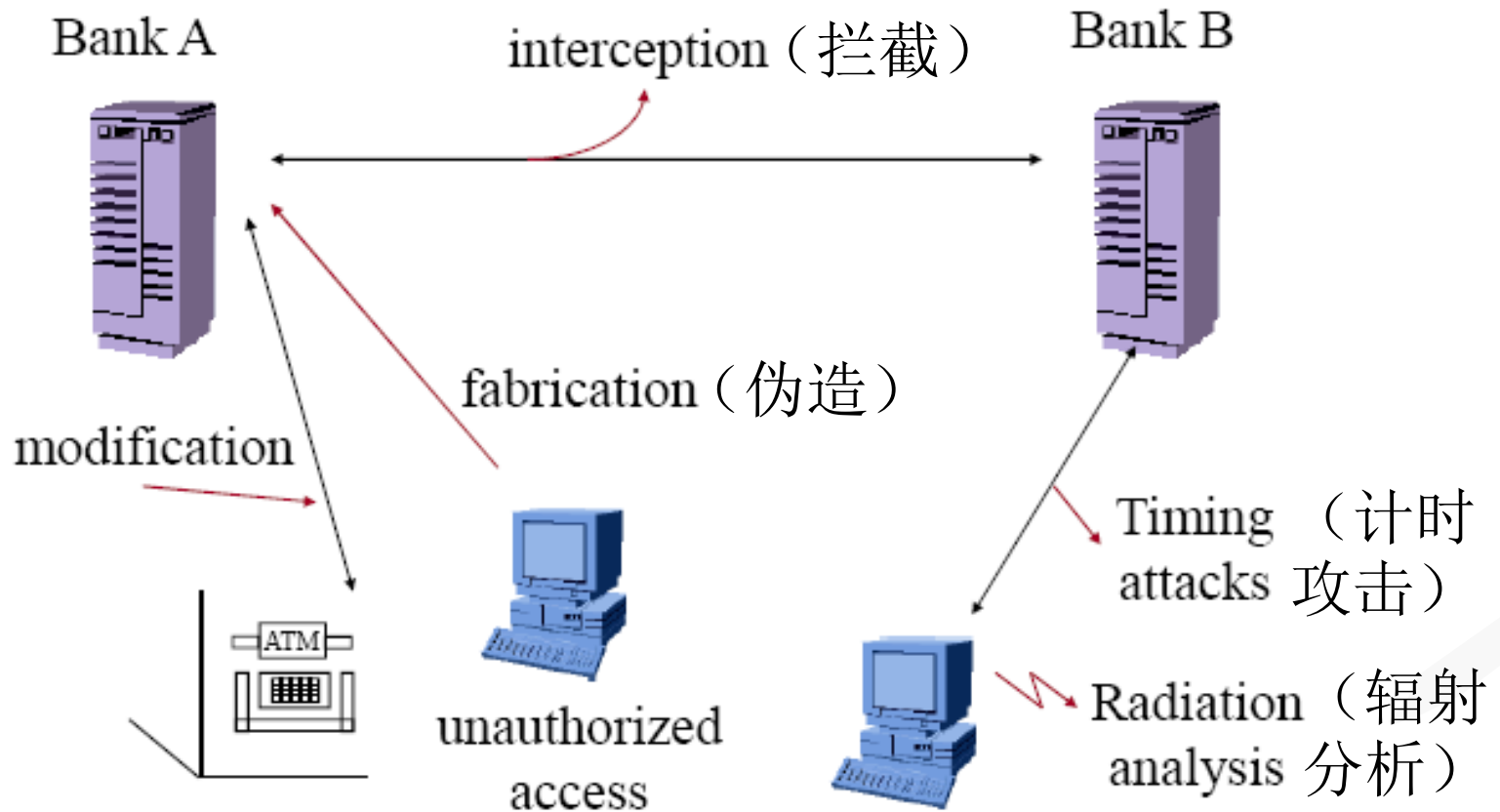


2021/3/8



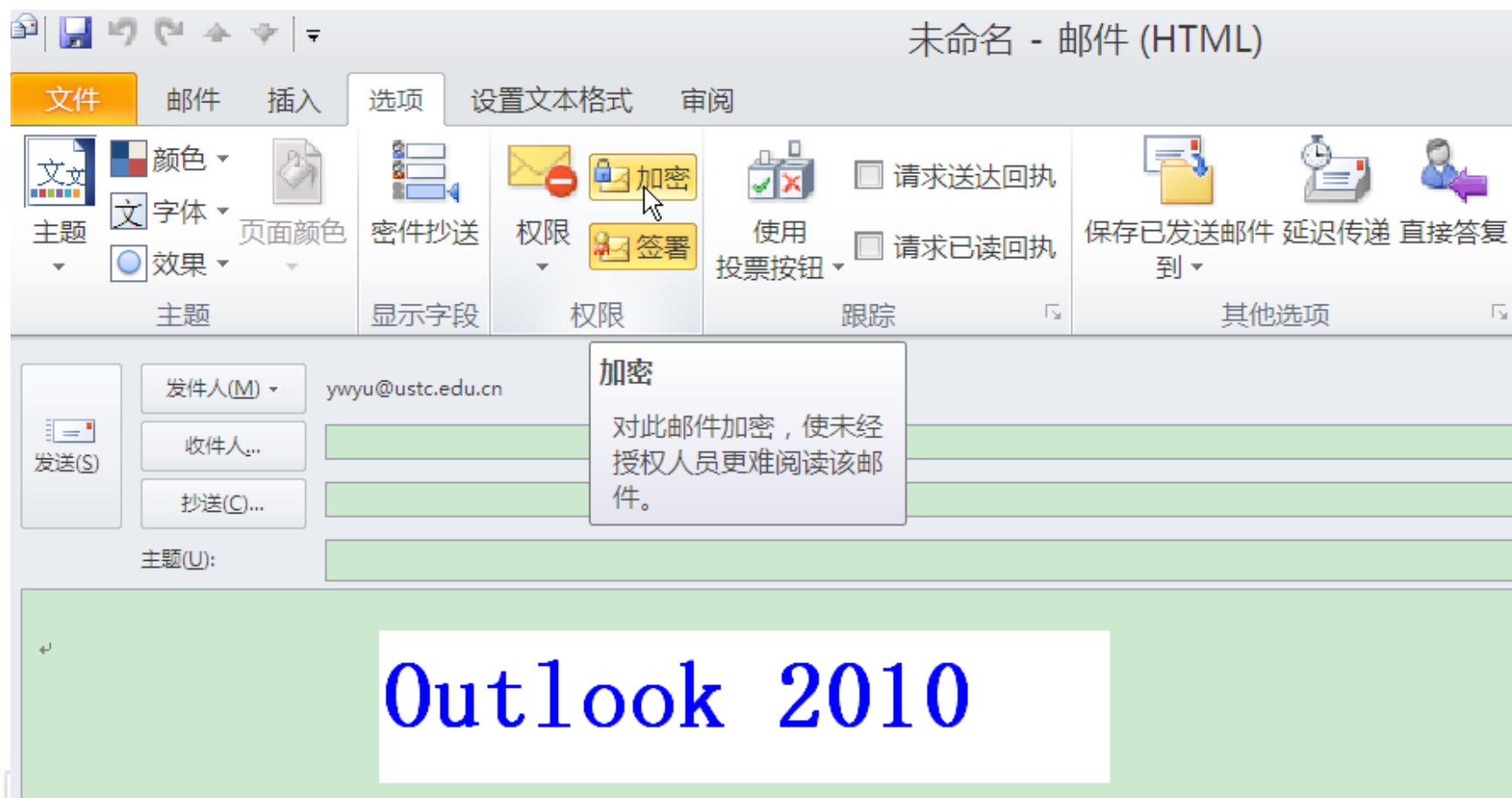
23

# Security Threats in Banking Systems

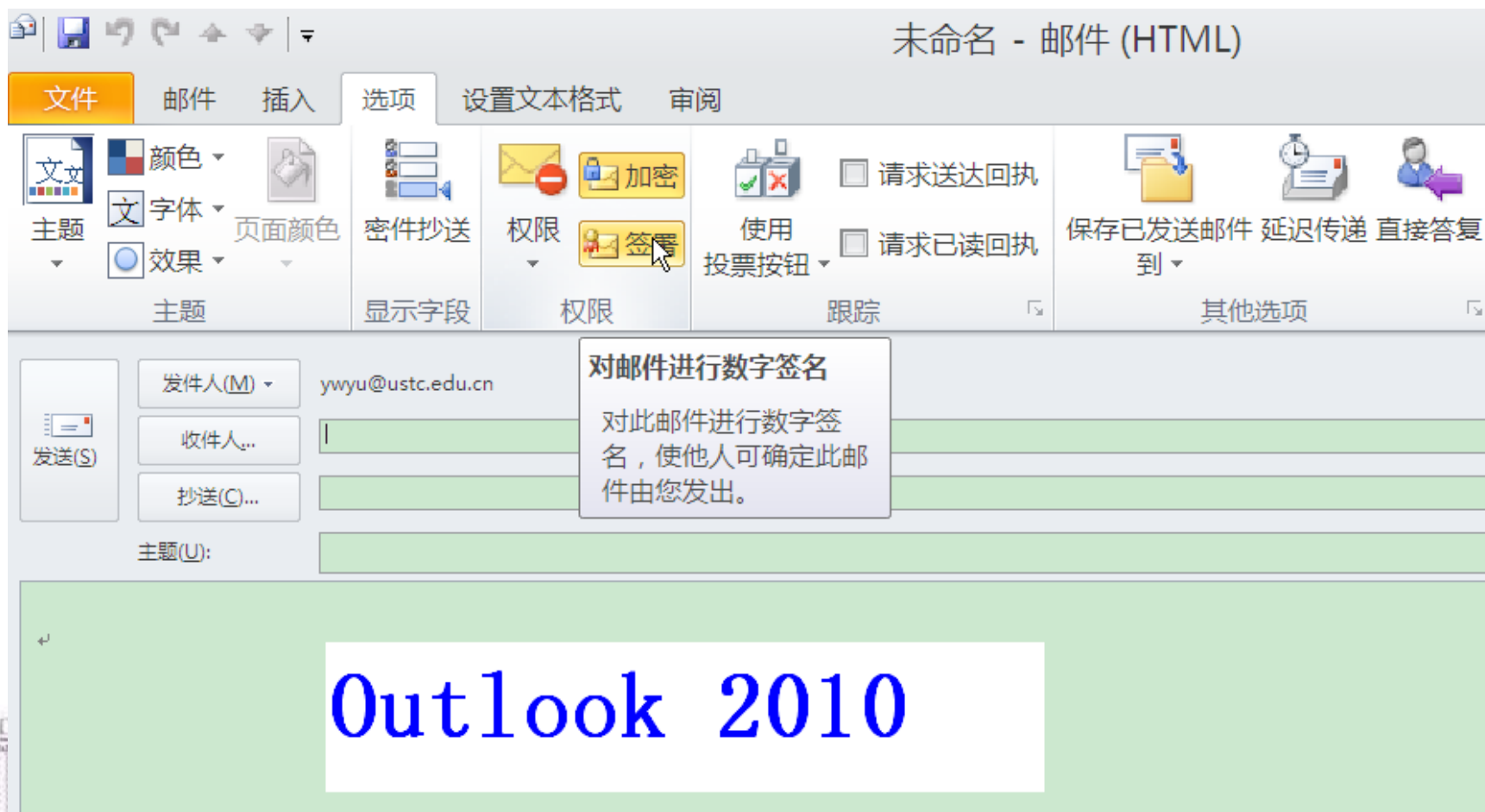




# Scene7: Email: Encryption



# Scene7: Email: Digital Signature



# Scene8: Download softwares



Q 网页 资讯 视频 图片 知道 文库 贴吧 地图 采购 更多

百度为您找到相关结果约33,500,000个

搜索工具

[Visual Studio 2021 下载, VS 编程开发工具 Visual Studio 2021...](#)



2020年9月3日 Visual Studio 2021 官方版是一款专业的VS编程开发工具, Visual Studio 2021 官方版可以帮助用户轻松进行编程操作, Visual Studio 2021 官方版便捷好用, 还具备了一个源代码编辑...

下载之家 百度快照

[帕尔马vs国际米兰:2021年帕尔马难求一胜](#)



3天前 2021年帕尔马还没有在联赛赢得一场胜利。国际米兰在意甲对阵帕尔马最近4个客场赢下了3场。卢卡库在本赛季已经打进了18球送出6次助攻, 本周卢卡库当选意甲二月最佳...

雷速体育 百度快照

[VS 2021 破解版下载 | Visual Studio 2021 中文破解版 32位/64...](#)



2021年1月23日 1、在本站下载好Visual Studio 2021 正式版软件包, 解压缩安装包开始安装, 这里小编以vs2019为例, 点击继续 2、等待安装 3、等待程序加载, 选择您所需要的开发环境 4...

当下软件园 百度快照

其他人还在搜

[visual studio 2021](#) [visual studio](#) [微软vs2021什么时候出](#) [死神vs火影2021最新版下载](#)  
[2020vs2021什么意思](#) [visual studio最新版](#) [vstar2021](#) [2020vs2021图片](#)

[2020 VS 2021](#)

2021年2月19日 2020年和2021年武大早樱对比 去年此时 疫情下的高校校园 是那么寂静 一年后 生机已重归 校园的花再次绽放 欢声笑语来迎春 1武汉大学 ...

n.eastday.com/pnews/1613712084... 百度快照

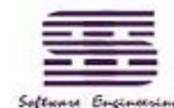
[vs2021破解版-Visual Studio 2021中文破解版 v2.8.3077.12...](#)



2021年2月6日 Visual Studio 2021 中文破解版软件大小: 1.4MB 软件语言: 简体中文 用户评分: 软件类型: 国产软件 授权方式: 免费软件 软件官网: 更新时间: 2021/02/06 软件分类: 编程...



2021/3/8



27

# Scene8: Download softwares

The screenshot displays a web browser window with a software download site. The main content area shows the details for 'Visual Studio 2021中文破解版'. The page includes a navigation bar with categories like '首页', '手机游戏', '手机软件', '电脑软件', and '游戏攻略'. The breadcrumb trail indicates the current location: '当前位置: 首页 > 精品软件 > 编程工具 > Visual Studio 2021中文破解版'. The software details section lists the size (1.4MB), language (Simplified Chinese), license (Free software), and update time (2021/02/06). It also features a '平台检测' (Platform Detection) section with various security logos (无插件, 360通过, 腾讯通过, 金山通过, 瑞星通过) and a user rating section showing 89% positive feedback (100 '好用' votes) and 11% negative feedback (12 '不好用' votes). A '下载' (Download) button is visible on the right side of the page.

当前软件园 / 汇聚当下最新最酷的软件下载站!

最新更新 | 软件分类

艾薇下载  
www.aiweibk.com

首页 手机游戏 手机软件 电脑软件 游戏攻略

当前位置: 首页 > 精品软件 > 编程工具 > Visual Studio 2021中文破解版

Visual Studio 2021中文破解版

软件大小: 1.4MB 软件语言: 简体中文 用户评分: ★★★★★

软件类型: 国产软件 授权方式: 免费软件 软件官网:

更新时间: 2021/02/06 软件分类: 编程工具 运行环境: Windows10, Wi...

平台检测

无插件 360通过 腾讯通过 金山通过 瑞星通过

好用 (100) 不好用 (12)

89% 11%

标签: Visual Studio

发表评论 收藏

2021/3/8

Software Engineering

28

# Summary of security problems

- Are secrets secure? Data Confidentiality
- Are secure free softwares? Data Integrity
- Who is chatting with you? Entity Authentication
- Who creates messages sent to me? Message Authentication
- How can I do if someone deny a fact? Non-Repudiation



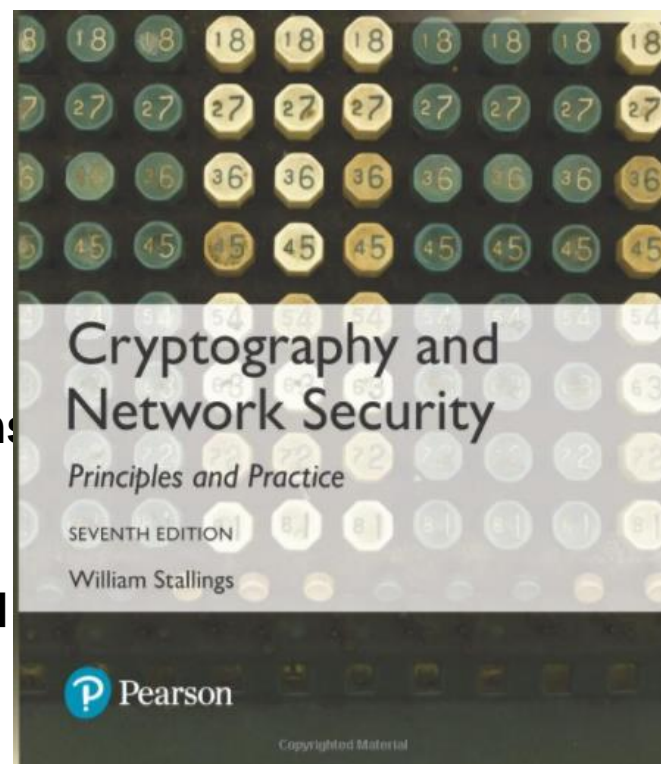
# Course Objective

- Understand Basic principle of cryptographic techniques and Use them safely
  - Encryption, Hash, Digital signature
  - Authentication(Message Authentication, Identification)
- Understand applications of cryptographic techniques
  - Authenticaiton: X.509
  - Cloud security
  - Web Security: Secure storage of password, SSL/TLS, SET,
  - Email Security: PGP, S/MIME
  - IPsec



# Literature

- **Textbook:**  
**Cryptography and Network Security, 7/E.**  
**William Stallings, Pearson, 2016**
- **References:**
  - **Applied Cryptography: Protocols, Algorithms and Source code in C, 2nd Edition.** Bruce Schneier, John Wiley & Sons, 1996.
  - **Handboook of applied Cryptography.** Alfred J. Menezes, CRC Press, 1996.
- **Web resources:**  
<http://williamstallings.com/Cryptography/>





# Course Schedule

- Week1: Organization, Introduction; Classical Encryption
- Week 2: DES, 3DES; Finite Fields
- Week 3: AES; Modes of Operation
- Week 4: stream cipher, random number generator, Confidentiality Using Symmetric Encryption
- Week 5: Symmetric Key Management, **midterm Test**
- Week 6: RSA, ECC, Message Authentication and Hash Functions
- Week 7: Message Authentication and Hash Functions, Identification
- Week 8: Digital Signatures, security application



2021/3/8





# Grading Scheme

- Labs 50%
  - 5 lab
- Midterm Test / Paper: 10%
- Final Exam: 40%, half-open

参与八强淘汰！

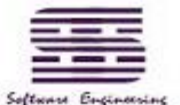


# Laboratory

- 5 labs:
  - Lab1: Many time pad
  - Lab2: discrete log
  - Lab3: AES
  - Lab4: RSA
  - Lab5: data integrity
- Suggest python code
- 小助教机制:
  - 实验开始的至少前一天，找主讲老师检查通过，才有资格申请。
  - Bonus: extra 1 point per lab



2021/3/8



# Contact us

- **Instructor:**
  - Yanwei Yu
  - E-mail: [ywyu@ustc.edu.cn](mailto:ywyu@ustc.edu.cn)
  - Tel: 0512-68839304
  - Office room: Room 501-7, SiXian Building



# Thanks!



2021/3/8



Software Engineering

36