Modern Cryptography and Its Applications

Yanwei Yu

E-mail: ywyu@ustc.edu.cn

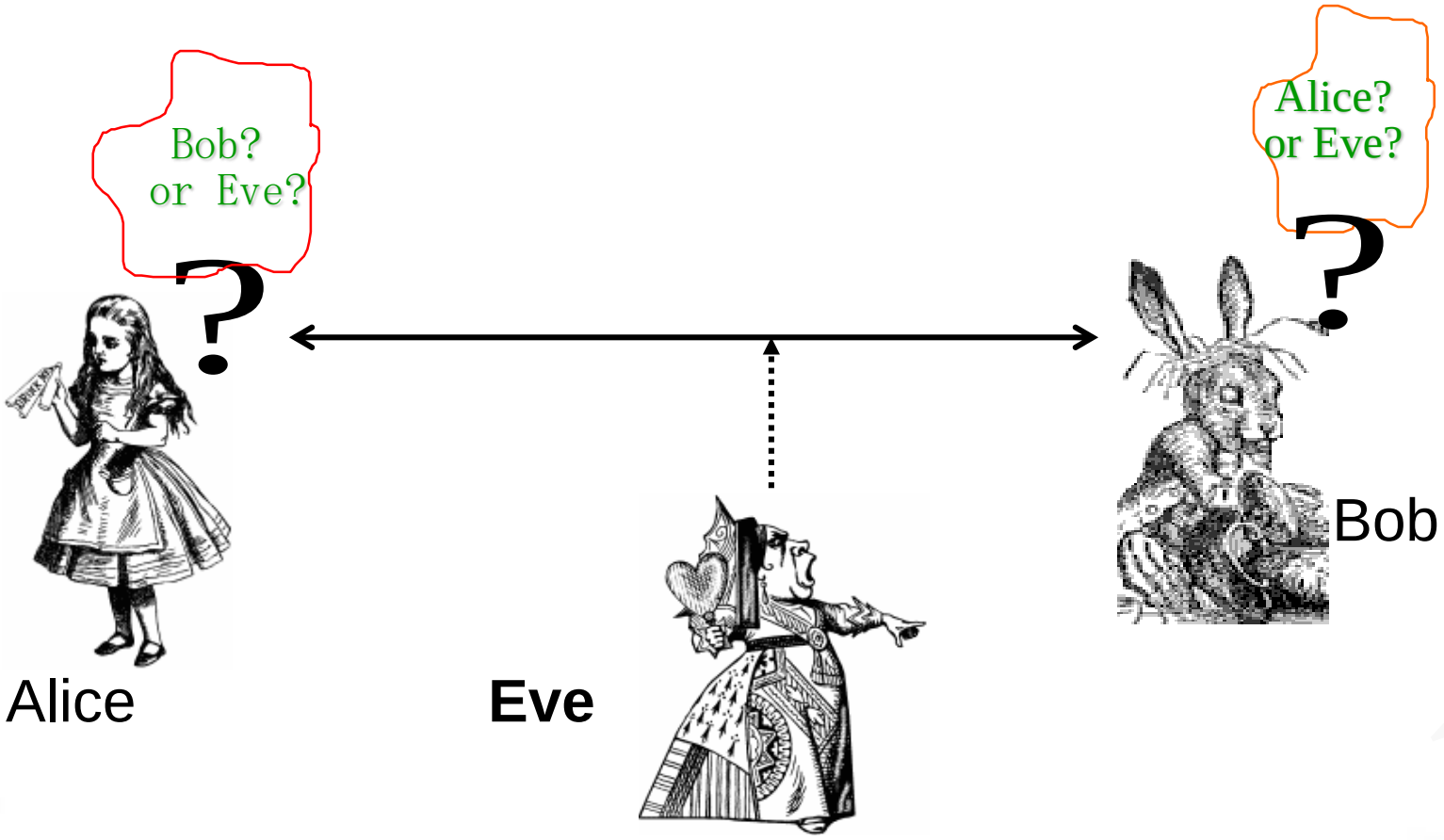
Outline

- **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



- **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
- ……

Scene1: Chat on the Internet

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

“Eve” Anywhere !

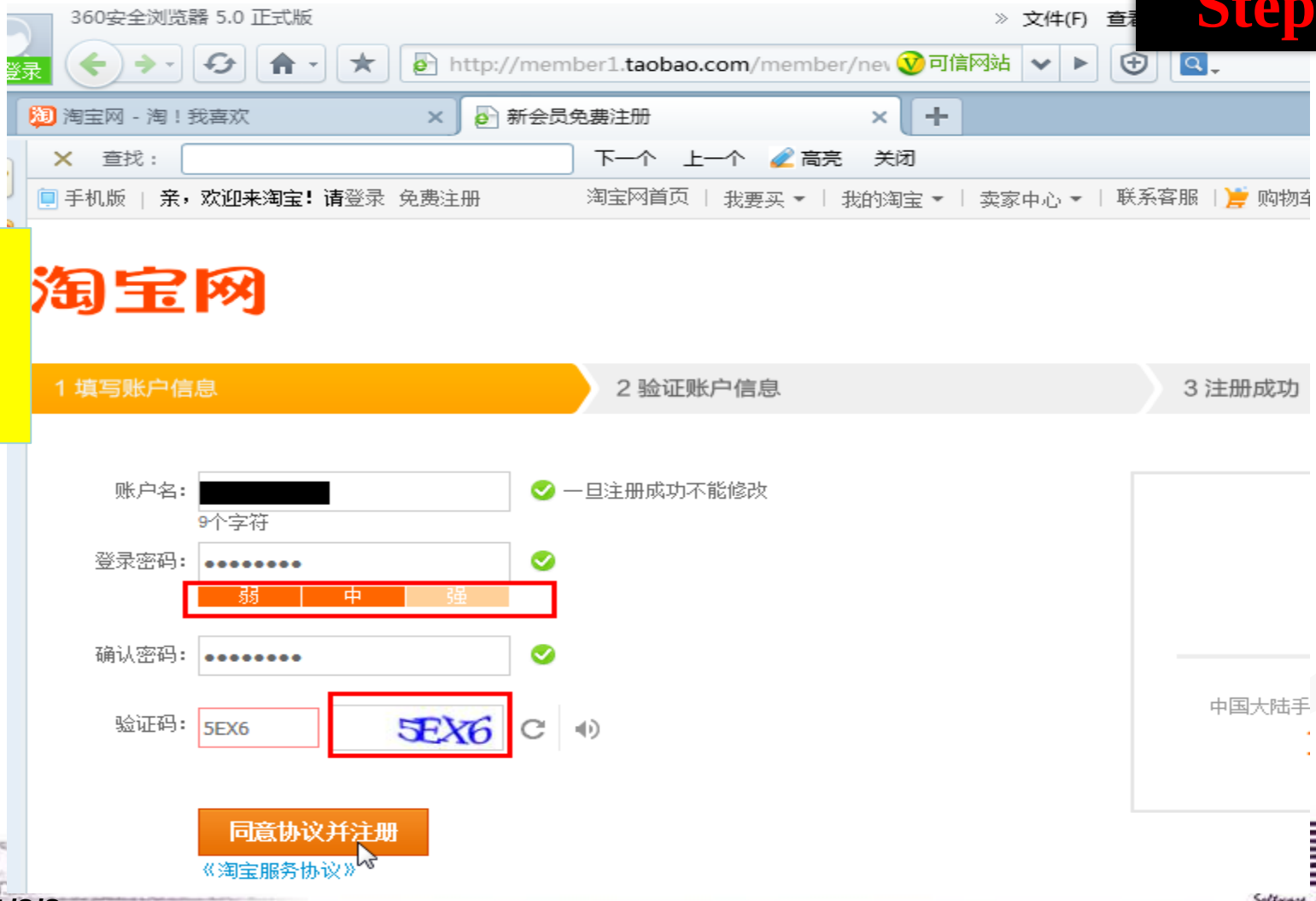
Scene2: Login on web


http://mis.sse.ustc.edu.cn/default.a
章泽天约友人按摩
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
9368
刷新
登录
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



Scene3: Sign in Taobao for new customer

Step2

2010年版本

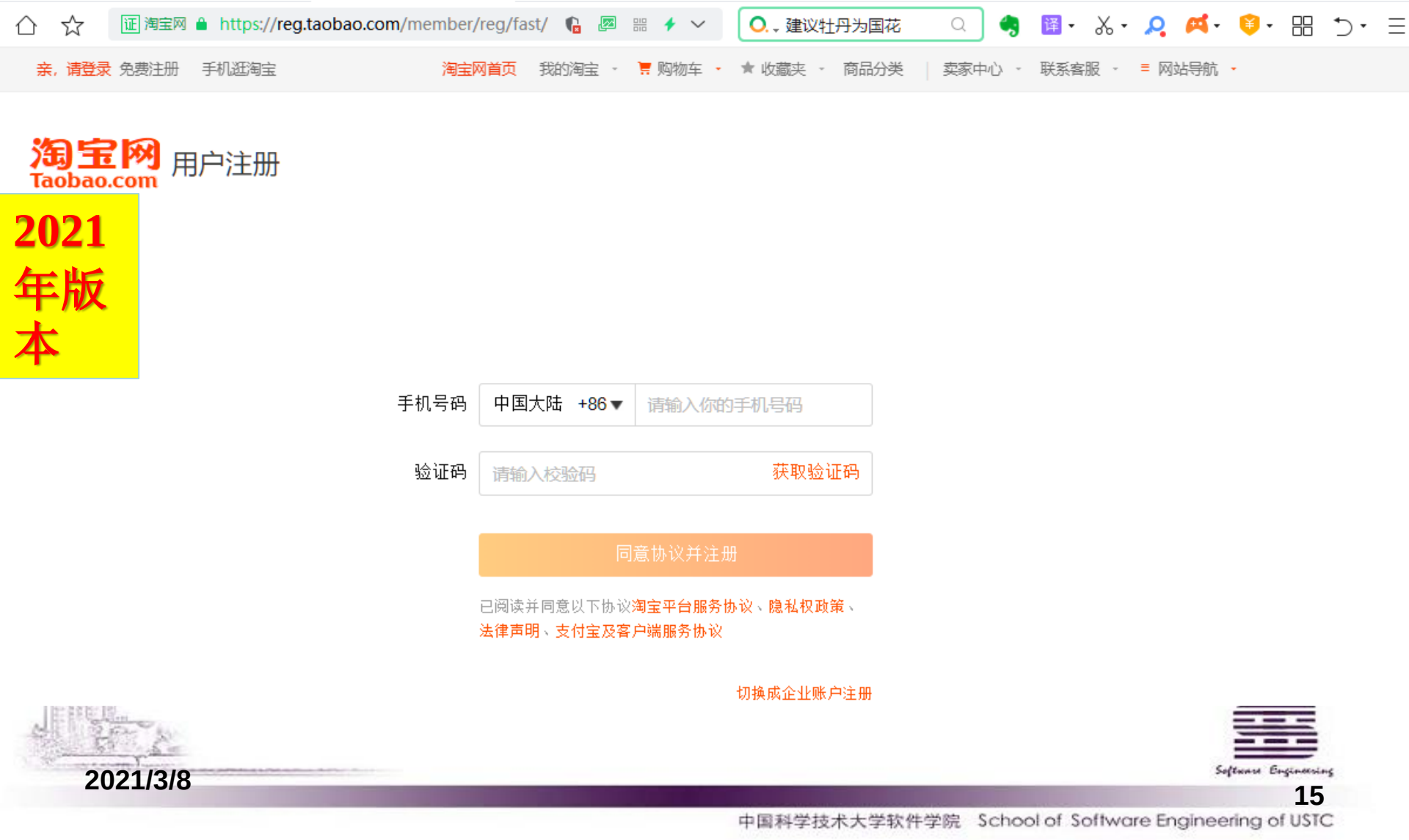
2010年版本


360安全浏览器 5.0 正式版
文件(F) 查看(V)
http://member1.taobao.com/member/nev
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
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
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

Scene3: Sign in Taobao for new customer

Step3

2010年版本

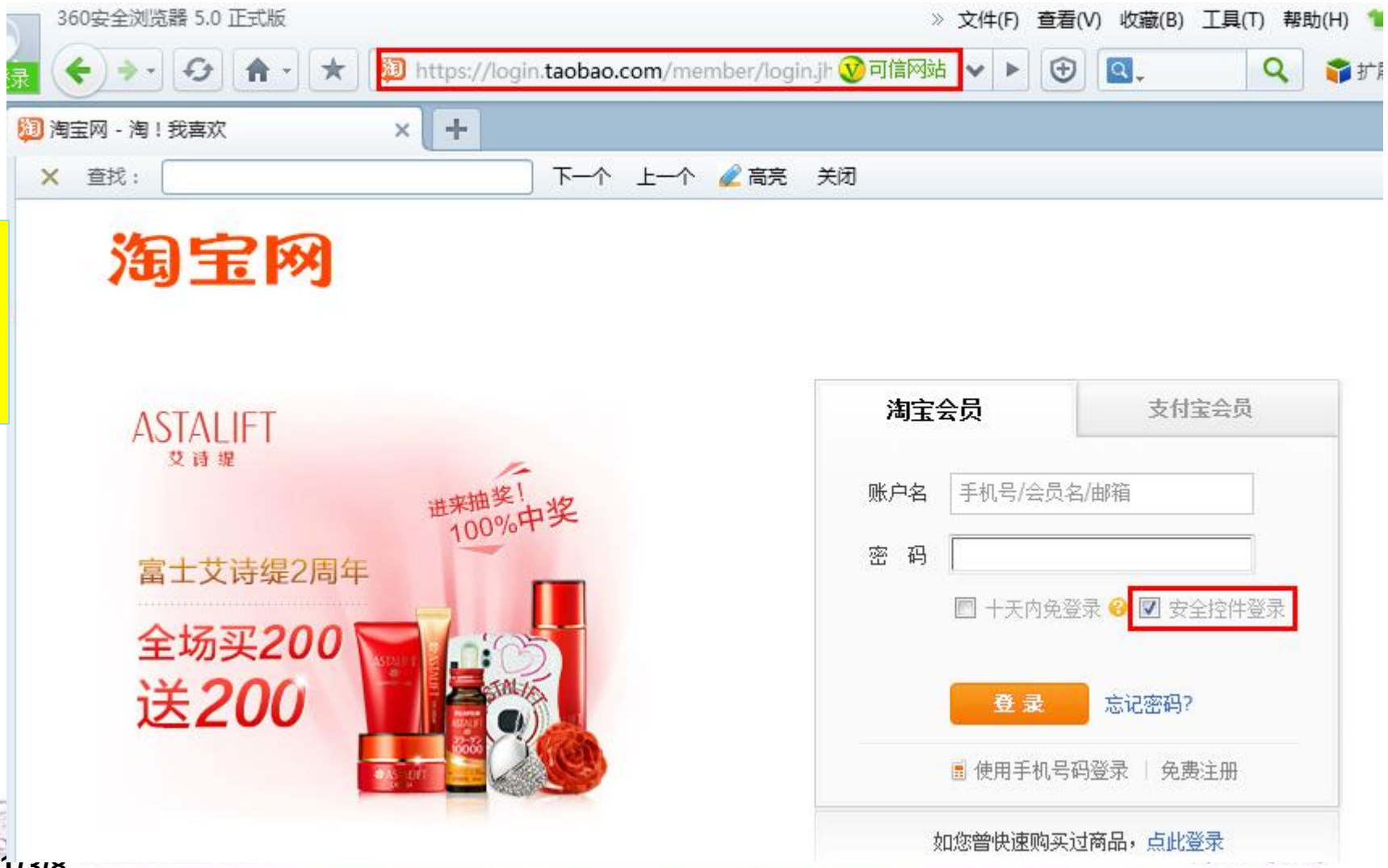

证 淘宝网 https://reg.taobao.com/member/reg/fast/
建议牡丹为国花
亲，请登录 免费注册 手机逛淘宝 淘宝网首页 我的淘宝 购物车 收藏夹 商品分类 卖家中心 联系客服 网站导航
淘宝网 Taobao.com 用户注册
2021年版本
手机号码 中国大陆 +86 请输入你的手机号码
验证码 请输入校验码 获取验证码
同意协议并注册
已阅读并同意以下协议淘宝平台服务协议、隐私权政策、法律声明、支付宝及客户端服务协议
切换成企业账户注册


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
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
设置会员名
登录名
会员名一旦设置成功，无法修改
提交
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?
手机（停机、丢失等）收不到验证码，怎么办?
手机、邮箱正常使
360安全键盘，可以防止键盘记录器窃取您的密码，让您安全放心登录网站。是否开启此功能？
暂不开启
立即开启

2021年版本

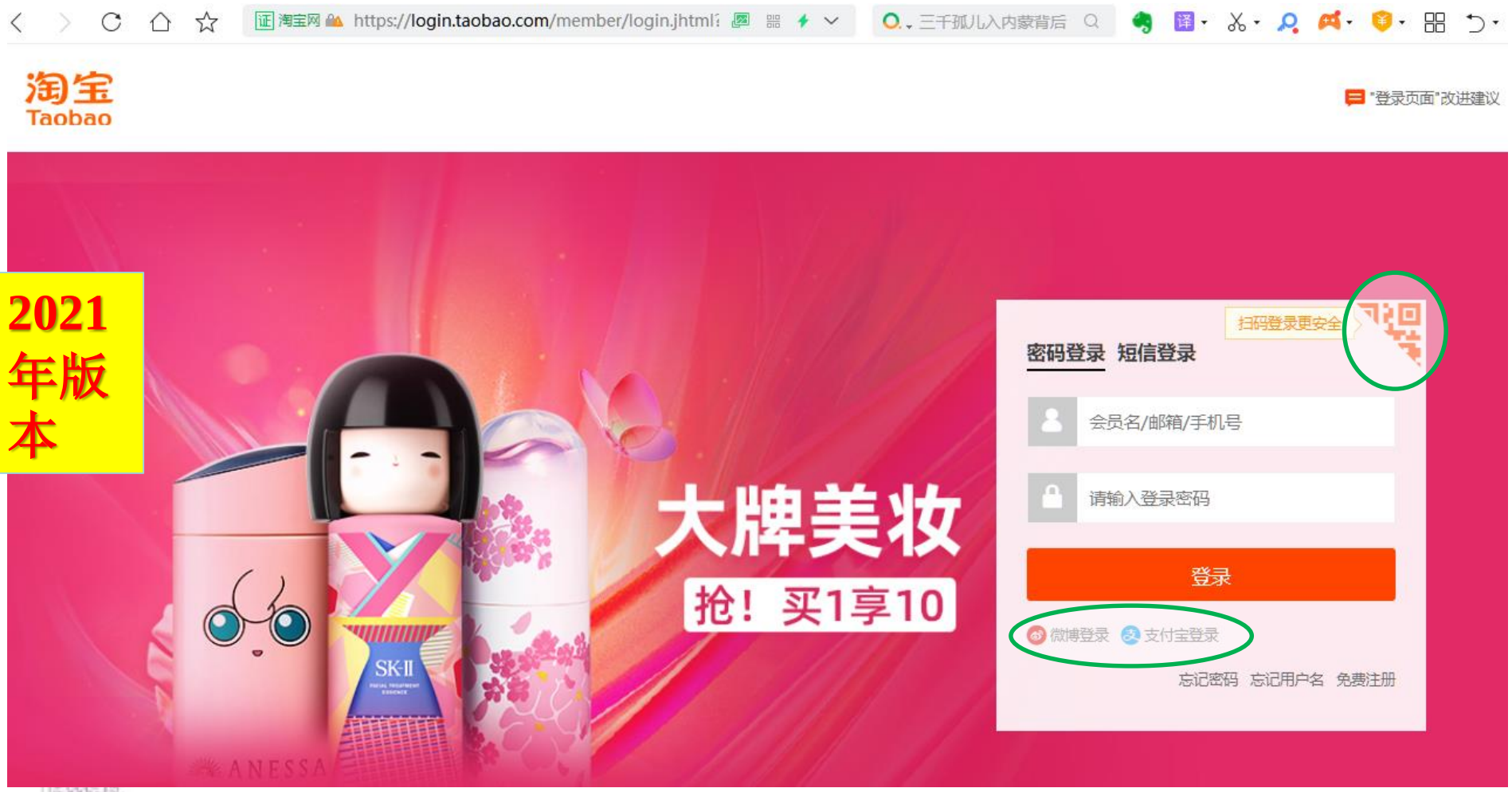
Scene4: Login on Taobao

2012年版本



淘宝网 After 3~5 continuous unsuccessful login attempt

2012年版本


https://login.taobao.com/member/login.jhtml
淘宝
Taobao
"登录页面"改进建议
2021年版本
大牌美妆
抢！买1享10
SK-II
ANESSA
扫码登录更安全
密码登录
短信登录
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


中国工商银行
电子银行口令卡正面
电子银行口令卡背面
（覆膜刮开后的示意图）

2012年版本


EXPO 2010 SHANGHAI CHINA
交通银行
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
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
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

Bank of Communicatio... https://pbar 袁立外籍前夫近照

交通银行 BANK OF COMMUNICATIONS
始于1908 您的财富管理银行

个人网上银行

在线客服 | 网银向

我的账户 转账 贷款 支付缴费 信用卡 理财存款 基金 保险 黄金 外汇 证券期货 预约与设置

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

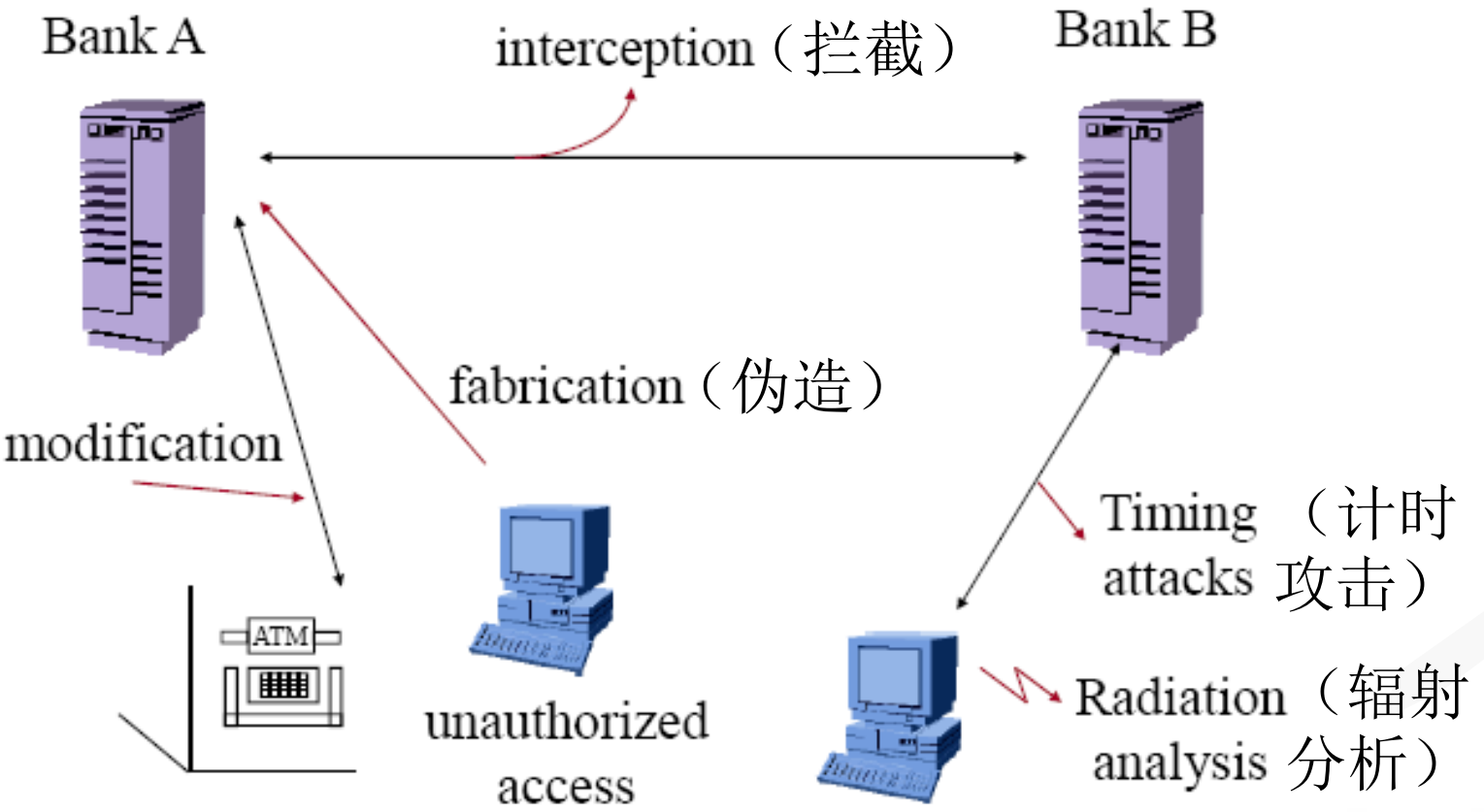
用户指南

2019年版本

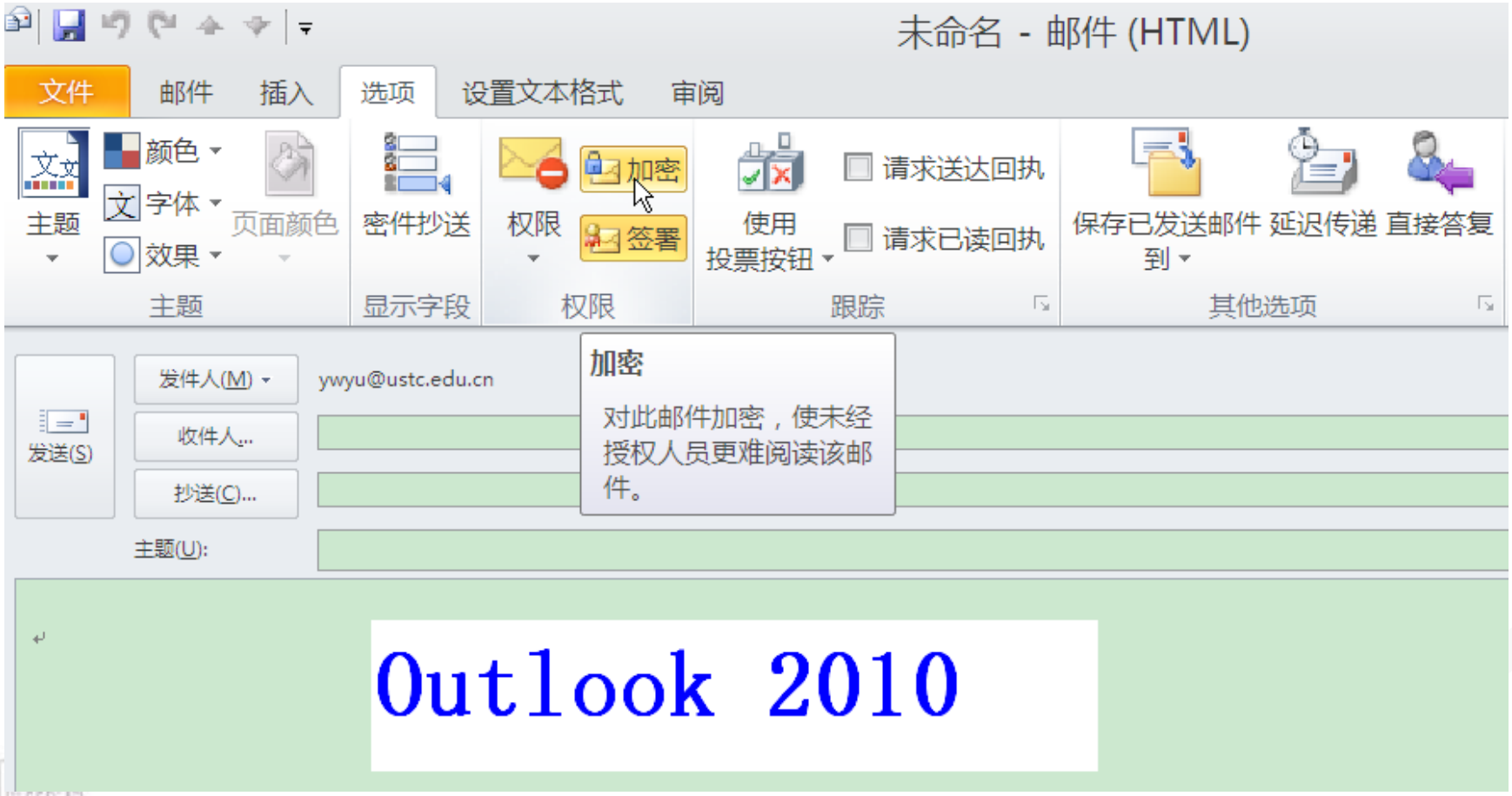
Scene6: Home-Shopping

- 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)

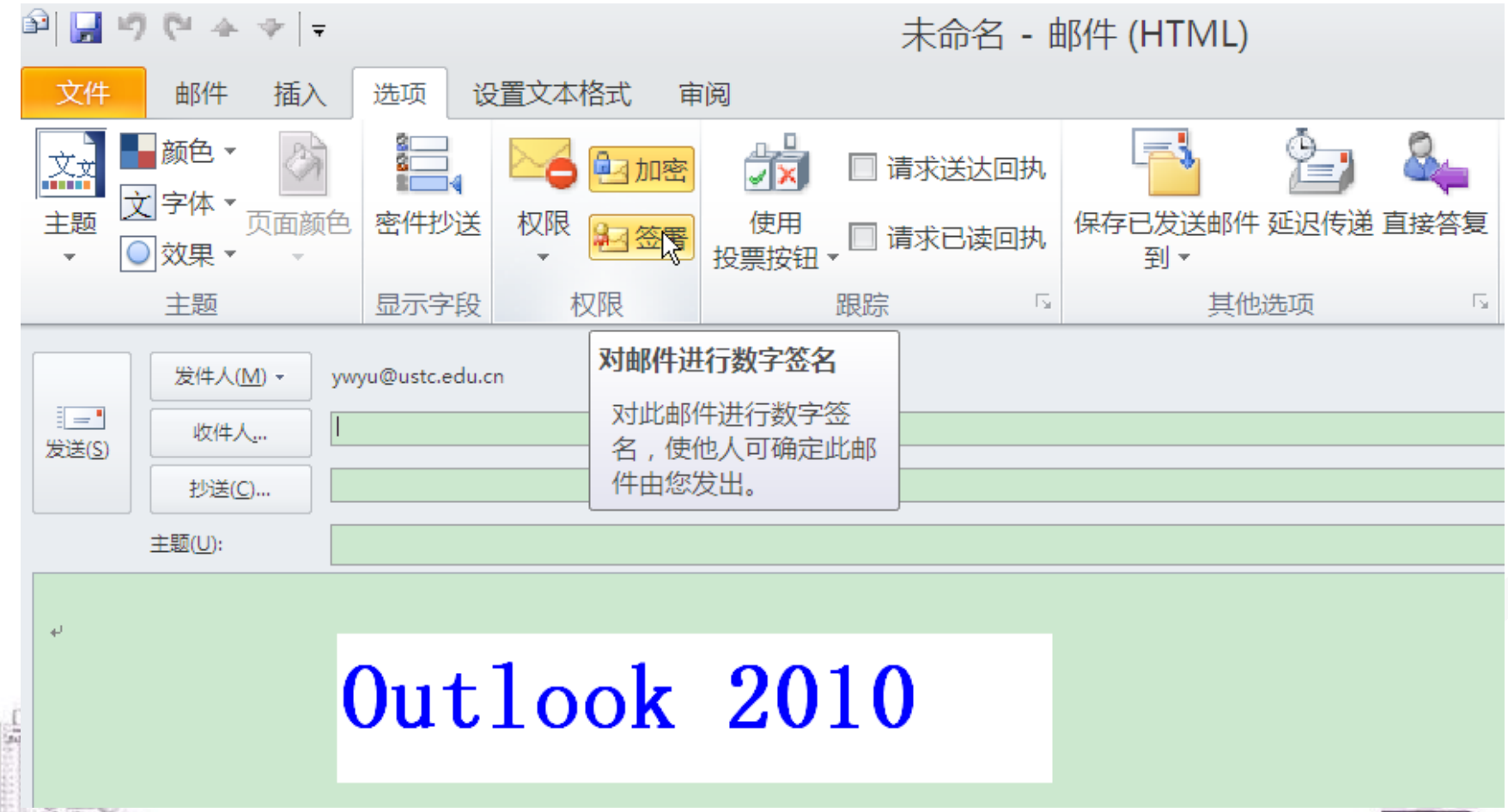
Security Threats in Banking Systems



Scene7: Email: Encryption



Scene7: Email: Digital Signature



Scene8: Download softwares

Scene8: Download softwares

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

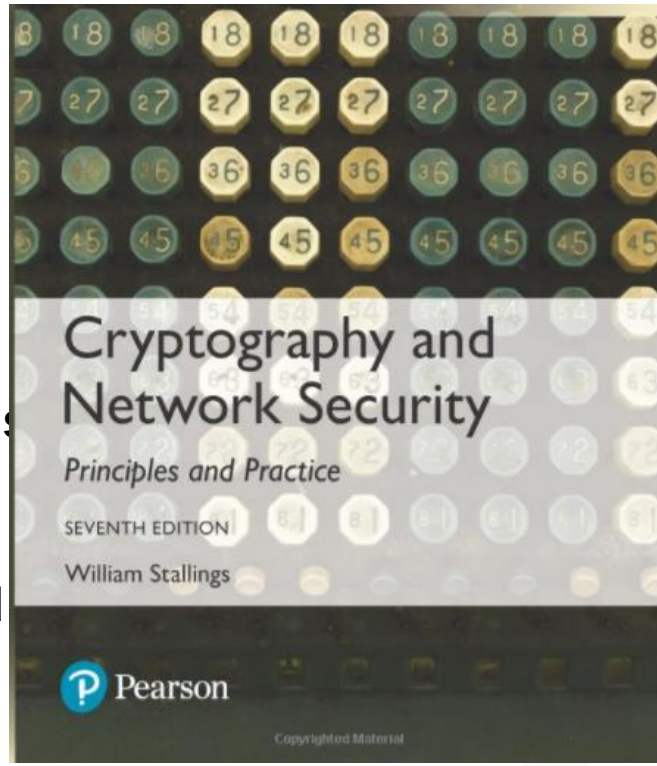
- Understand Basic principle of cryptographic techniques and Use them safely
  - Encryption, Hash, Digital signature
  - Authentication(Message Authentication, Identification)
- Understand applications of cryptographic techniques
  - Authenticaiton: X.509
  - Cloud security
  - Web Security: Secure storage 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, Algorthms 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**

Grading Scheme

- Labs 50%
  - 5 lab

参与八强淘汰！

- Midterm Test / Paper: 10%
- Final Exam: 40%, half-open

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

Contact us

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

Thanks!