北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

《现代密码学》第十章

# 身份鉴别

BUPT ISC 信息安全中心

# 上讲内容回顾

- 密钥管理简介
- 密钥分配
- 密钥协商
- PKI及数字证书简介

# 本讲主要内容

- 身份鉴别的定义
- 口令身份鉴别
  - 固定口令
  - 一次口令
- 身份鉴别协议
  - 挑战应答协议
  - 零知识证明协议

# 本讲主要内容

- 身份鉴别的定义
- 口令身份鉴别
  - 固定口令
  - 一次口令
- 身份鉴别协议
  - 挑战应答协议
  - 零知识证明协议

# 身份鉴别的定义

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

定义：身份鉴别，又称为身份识别、身份认证。它是证实客户的真实身份与其所声称的身份是否相符的过程。

身份鉴别手段：

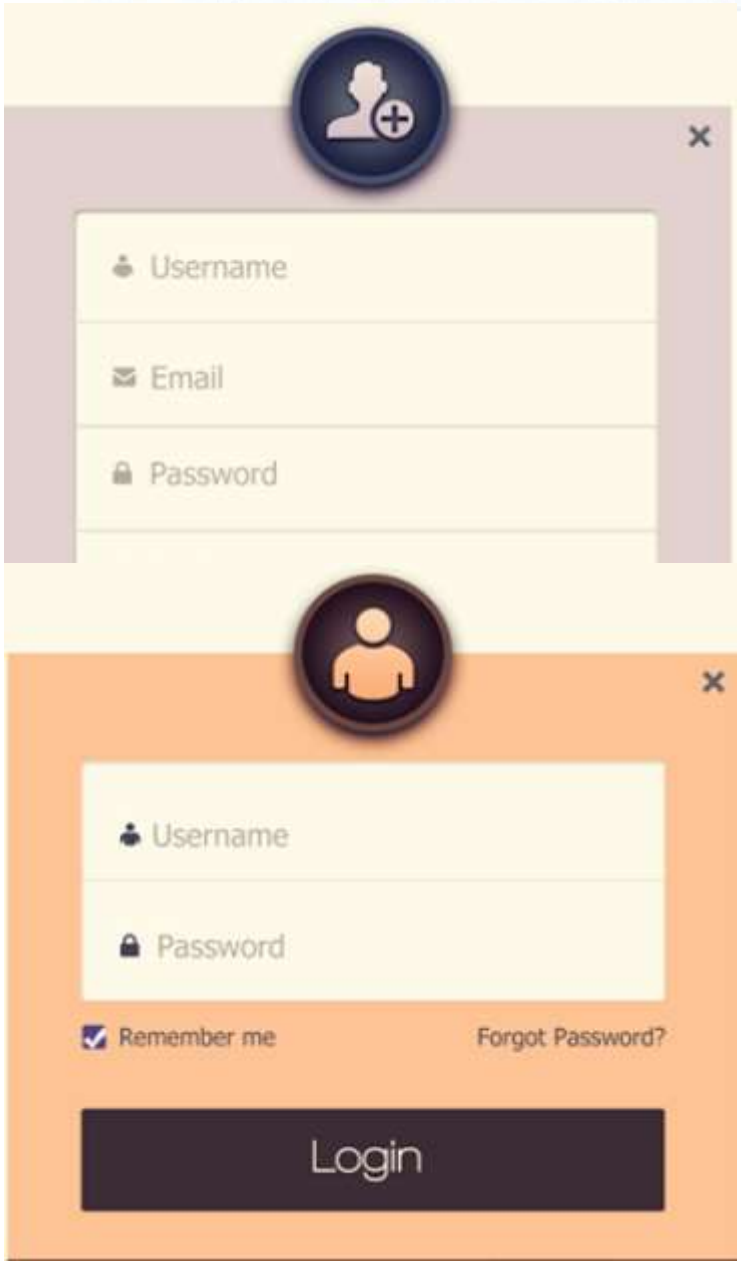
- 已拥有的事物：通常是物理配件。如，磁卡、智能卡(或IC卡)、证件。
- 固有事物(对某个人)：利用人类物理特征和无意行为。如，手写签名、指纹、声音、视网膜模式、手的几何形状等。
- 已知事物：口令、个人识别码(PIN)、挑战-应答协议中已被证实的秘密或私钥。

# 本讲主要内容

- 身份鉴别的定义
- 口令身份鉴别
  - 固定口令
  - 一次口令
- 身份鉴别协议
  - 挑战应答协议
  - 零知识证明协议

# 口令身份鉴别

- 口令生成
- 口令分配（注册）
- 口令保存
- 口令使用（登录）
- 口令备份/恢复（忘记口令）
- 口令撤销/更新（修改密码）
- 口令销毁




北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS
BUPT ISC 信息安全中心

# 口令身份鉴别

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 用户的脆弱口令行为

表 1　本文使用口令集的基本信息

| Password Dataset | Service Type | Language | Leaked Time | Total Passwords | Unique Password | Personal Info | Typical Reference |
|---|---|---|---|---|---|---|---|
| Dodonew | Gaming, Ecommerce | Chinese | 2011-12 | 16 258 891 | 10 135 260 | | Ref[23-26] |
| CSDN | Programmer Forum | Chinese | 2011-12 | 6 428 277 | 4 037 605 | | Ref[23-26] |
| 126 | Email | Chinese | 2011-12 | 6 392 568 | 3 778 168 | | Ref[28] |
| 12306 | Train Ticketing | Chinese | 2014-12 | 129 303 | 117 808 | √* | Ref[29] |
| Rockyou | Social Networks | English | 2009-12 | 32 581 870 | 14 326 970 | | Ref[23-24,30] |
| 000webhost | Web Hosting | English | 2015-10 | 15 251 073 | 10 583 709 | | Ref[28] |
| Yahoo | Web Portal | English | 2012-07 | 442 834 | 342 510 | | Ref[23-25] |
| Rootkit | Hacker Forum | English | 2011-02 | 69 419 | 56 900 | √** | Ref[27] |

Notes: * The 12306 dataset includes five types of personal information: name, birthday, email, phone number and national identity card number.

** The Rootkit dataset includes four types of personal information: name, birthday, user name and email.

# 口令身份鉴别



- 口令构造的偏好性选择

1．国民口令

表 2　各个网络服务中最流行的 10 个口令

| Rank | Dodonew | CSDN | 126 | 12306 | Rockyou | 000webhost | Yahoo | Rootkit |
|---|---|---|---|---|---|---|---|---|
| 1 | 123456 | 123456789 | 123456 | 123456 | 123456 | abc123 | 123456 | 123456 |
| 2 | a123456 | 12345678 | 123456789 | a123456 | 12345 | 123456a | password | password |
| 3 | 123456789 | 11111111 | 111111 | 5201314 | 123456789 | 12qw23we | welcome | rootkit |
| 4 | 111111 | dearbook | password | 123456a | password | 123abc | ninja | 111111 |
| 5 | **5201314** | 00000000 | 000000 | 111111 | **iloveyou** | a123456 | abc123 | 12345678 |
| 6 | 123123 | 123123123 | 123123 | **woaini1314** | **princess** | 123qwe | 123456789 | qwerty |
| 7 | a321654 | 1234567890 | 12345678 | 123123 | 1234567 | secret666 | 12345678 | 123456789 |
| 8 | 12345 | 88888888 | **5201314** | 000000 | rockyou | YfDbUfNjH10305070 | sunshine | 123123 |
| 9 | 000000 | 111111111 | 18881888 | qq123456 | 12345678 | asd123 | **princess** | qwertyui |
| 10 | 123456a | 147258369 | 1234567 | 1qaz2wsx | abc123 | qwerty123 | qwerty | 12345 |
| Percetage/% | 3.28 | 10.44 | 3.52 | 1.28 | 2.05 | 0.79 | 1.01 | 3.94 |

# 口令身份鉴别

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 口令构造的偏好性选择

## 1．国民口令

- ✓ 除了选择单词作口 令，用户常常将单词进行简单变换，以满足网站口令 设置策略的要求． 比如“１２３４５６ａ”可以满足“字母＋数 字”的 策 略 要求．
- ✓ 中文国民口令多为纯数字，而英文 国民口令多含字母
- ✓ 爱情这一主题在国民口令中占据了重 要地位．
- ✓ 高 达１．０１％～１０．４４％的 用 户 选 择 最 流 行 的１０个口令

攻击者只要尝试１０个最 流行的口令，其成功率就会达到１．０１％～１０．４４％

# 口令身份鉴别

- 口令构造的偏好性选择

2. 字符组成结构

表 3　中英文用户口令的字符组成结构　%

| Datasets | ^[a-z]+$ | [a-z] | ^[A-Za-z]+$ | [a-zA-Z] | ^[0-9]+$ | [0-9] | ^[a-zA-Z0-9]+$ | ^[a-z]+[0-9]+$ | ^[a-zA-Z]+[0-9]+$ | ^[a-z]+1$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Dodonew | 10.30 | 66.32 | 10.92 | 69.05 | **30.76** | **88.52** | 98.33 | 43.50 | 45.74 | 1.40 |
| CSDN | 11.64 | 51.39 | 12.35 | 54.33 | **45.01** | **87.10** | 96.31 | 26.14 | 28.45 | 0.24 |
| 126 | 32.66 | 66.63 | 34.86 | 68.87 | **30.66** | **63.24** | 95.92 | 21.99 | 23.15 | 2.35 |
| 12306 | 5.26 | 72.52 | 5.42 | 72.94 | **27.03** | **94.56** | 99.87 | 50.85 | 51.50 | 0.93 |
| Rockyou | 41.71 | **80.58** | 44.07 | 83.89 | 15.94 | 54.04 | 96.25 | 27.70 | 30.18 | **4.55** |
| 000webhost | 0.04 | **98.04** | 0.26 | 99.57 | 0.02 | **98.41** | 93.08 | **54.42** | 60.95 | **4.66** |
| Yahoo | 33.09 | **92.83** | 34.64 | 94.06 | 5.89 | 64.74 | 97.15 | 38.27 | 41.85 | **4.80** |
| Rootkit | 41.60 | **84.64** | 43.84 | 85.84 | 13.88 | 53.97 | 93.90 | 19.19 | 21.55 | 1.81 |

# 口令身份鉴别



- 口令构造的偏好性选择

## 2. 字符组成结构

- ✓ 当网站设置了口令生成策略时，口令的字符组成很大程度上由口令策略所决定.
  - ✓高达99.57%的000webhost口令由字母和数字共同构成，这意味着该网站在运行不久后就执行了“字母+数字”的口令策略.
  - ✓用户也显示了偏好：54.42%的000webhost口令符合“一串小写字母+一串数字”的结构.
- ✓ 当网站未设置口令构成策略时，用户口令的结构直接体现了用户的偏好.
  - ✓绝大多数中文口令包含数字，且27%～45%仅由数字构成
  - ✓英文口令喜欢包含字母，低于16%的口令仅由数字构成，有相当一部分由一串小写字母后面跟1组成.

# 口令身份鉴别



- 口令构造的偏好性选择

3. 基于个人信息构造口令

✓ 早在 1979 年，Morris和 Thompson就 发现 用户构造口令时喜欢使用姓名等个人信息，在猜测 字典中加入姓名库可以显著提高口令猜测成功率.

✓ 除了姓名、生 日、用 户 名、Email前 缀、身 份 证 号 、电 话号码，甚至地名这些个人相关信息都可能 被用户使用

用户使用个人信息构造口令的习惯严重降低了口令强度，定向攻击者可依此大大增强其效率.

# 口令身份鉴别

- 口令构造的偏好性选择

## 3. 基于个人信息构造口令

相当比例的用户使用姓氏或“名的缩写＋姓氏”作为口令的构成部分.

英文网站Rootkit用户使用个人信息相较中文网站12306较少，但这并不能得到“中文用户更倾向于在口令中使用个人信息”的结论，这是因为Rootkit网站是黑客论坛，其中的用户具有比普通用户更高的安全意识。

表6 12306网站口令中个人信息使用频率 %

| Types of Personal Info | 12306[29] | Rootkit |
|---|---|---|
| Name | 22.35 | 3.12 |
| Birthdate | 24.10 | 1.19 |
| Account Name | 23.60 | 1.59 |
| Email Prefix | 12.66 | 0.77 |
| ID Number | 3.00 | |
| Phone Number | 2.73 | |

表7 各类姓名的使用频率 %

| Types of Name Usages | 12306 | Rootkit |
|---|---|---|
| Full Name | 4.68 | 1.38 |
| Family Name | 11.15 | 2.28 |
| Given Name | 6.49 | 0.49 |
| Abbreviate Full Name | 13.64 | 0.15 |

# 口令身份鉴别

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 口令构造的偏好性选择

## 4. 口令长度

用户口令长度也直接受网站策略影响.

✓ 比如，000webhost提供建站服务，该网站34.7%的口令长度不低于11，这一比例是其他任意网站的2倍以上.

✓ 对于普通网站来说，90%以上口令的长度介于6－11之间.

表4 中英文用户口令的长度分布 %

| Datasets | 1~5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | ≥15 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Dodonew | 2.46 | 12.31 | 15.87 | 20.86 | 22.89 | 16.37 | 5.21 | 1.76 | 0.89 | 0.56 | 0.83 |
| CSDN | **0.63** | **1.29** | **0.26** | 36.38 | 24.15 | 14.48 | 9.78 | 5.75 | 2.61 | 2.41 | 2.26 |
| 126 | **0.00** | 26.16 | 19.33 | 22.67 | 11.26 | 8.17 | 4.60 | 1.76 | 0.90 | 0.68 | 0.12 |
| 12306 | 3.58 | 11.21 | 15.08 | 26.32 | 23.35 | 18.13 | 3.43 | 1.51 | 0.55 | 0.31 | 0.88 |
| Rockyou | 1.93 | 26.05 | 19.29 | 19.98 | 12.12 | 9.06 | 3.57 | 2.10 | 1.32 | 0.86 | 0.47 |
| 000webhost | **0.02** | 5.70 | 7.92 | 21.81 | 15.41 | 14.51 | **10.49** | **7.67** | **4.14** | **3.14** | **9.20** |
| Rahoo | 6.39 | 17.98 | 14.82 | 26.90 | 14.90 | 12.37 | 4.79 | 4.91 | 0.60 | 0.34 | 0.80 |
| Rootkit | **0.00** | 24.37 | 16.84 | 25.80 | 11.01 | 7.39 | 3.50 | 2.25 | 1.02 | 0.62 | 0.00 |

# 口令身份鉴别

表 5　口令重用统计数据

| References | Year | Research Method | Direct Reuse/% | In-direct Reuse/% |
|---|---|---|---|---|
| Ref [27] | 2014 | User survey | 51 | 26 |
| Ref [27] | 2014 | Empirical | 43 | 30 |
| Ref [46] | 2014 | Empirical | 21 | 26 |
| Ref [28] | 2016 | User survey | 45 | 33 |
| Our statistics | 2016 | Empirical | 34 | 31 |

- 口令构造的偏好性选择

## 5. 口令重用

✓ 面对如此多的需要管理的帐号，重用口令是用户理智的做法，关 键在 于如何重用.

✓ 跨不同安全级（或重要程度）帐户重用口令，是应努力避免的

２０１４年，Ｄａｓ等人研究了口令间接重 用时新口令和原口令间的相似度，结果 表 明，

✓ 只 有 约３０％的 用 户 重 用 口 令时简单修改（即新旧口令相似度在［０．８，１］），绝大多 数用户的新旧 口 令 相 似 度 小于０．８，表 明 修 改 幅 度 较大.

✓ 中文用户口令重用的问 题要更严重：约有４０％以上间接重用的中文口令相 似度在［０．７，１］，而英文口令仅有２０％.

# 口令身份鉴别

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

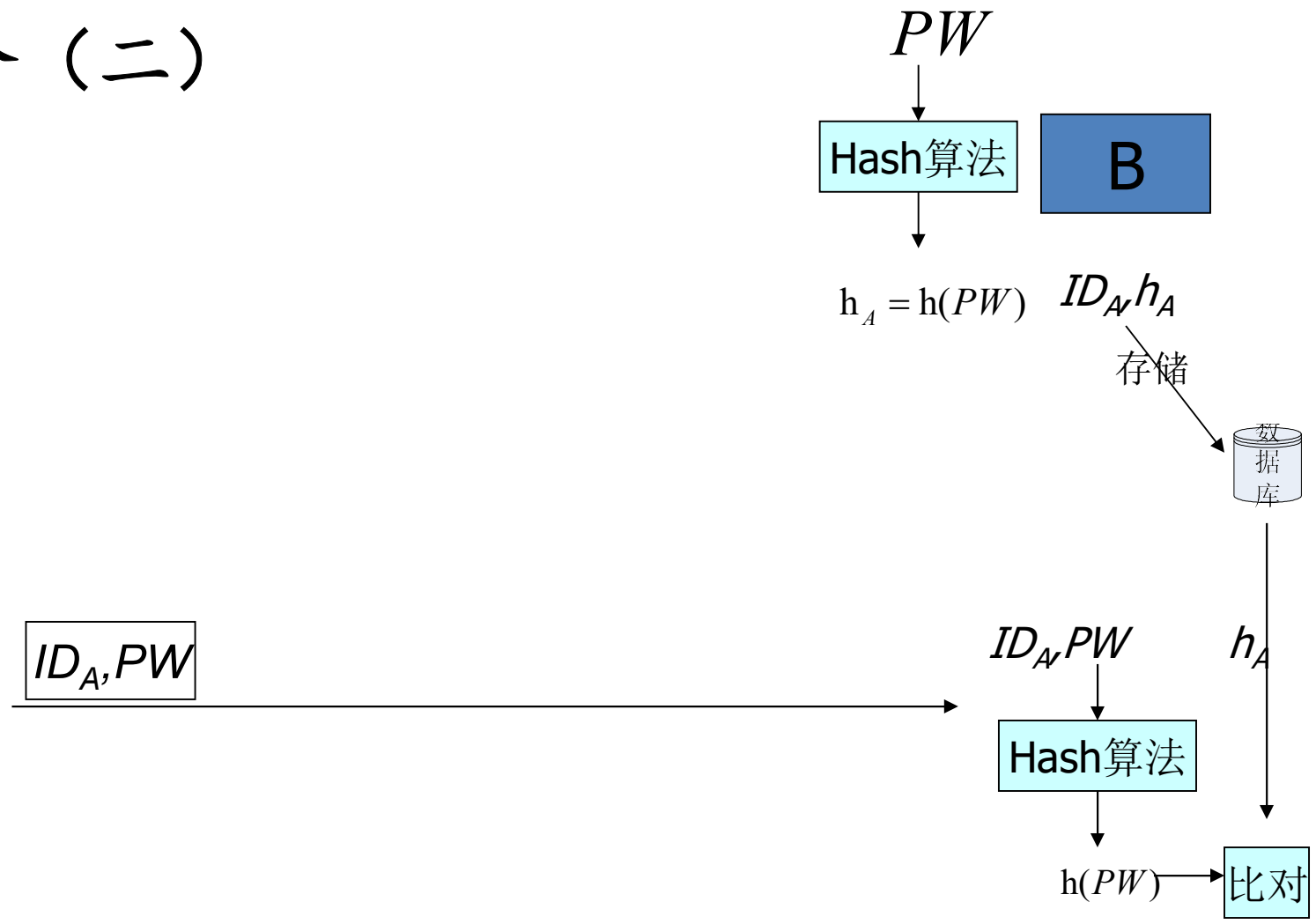
## 固定口令（一）

# 口令认证

## 固定口令（二）

A

$PW$



# 口令认证

攻击--Mallory找到（任意）某个用户口令

- 假设口令是六位数（银行密码）；
- Mallory可以创建一个六位数(000000~999999)的列表；
- 然后对每一个数使用散列函数，结果就是一个一百万个散列的列表；
- 她窃取得到口令档案并搜索条目中的口令字段列，找出一个与之相匹配的；
- 找到匹配以后， Mallory就可以再上线，用口令来访问系统。

# 口令认证

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

## 固定口令（三）

### 注册环节：口令加盐(Salting Passwords)

① 接收用户提供的口令$pw$;

② 生成一个盐值：$Dsalt = Arandom(\ )$;

③ 生成口令信息：$s = Agen(Dsalt, pw)$;

④ 把口令信息$s$和$Dsalt$存入数据库的口令字段中。

### 登录环节：

① 接收用户提供的帐户名$Dname$和口令$pw$;

② 在帐户信息数据库中检查$Dname$的合法性，如果合法，则找出其对应的$s$和$Dsalt$;

③ 生成临时口令信息：$sr = Agen(Dsalt, pw)$;

④ 如果$sr$与$s$相等，则认证成功，否则，认证失败。

# 口令认证

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

## 固定口令（三）

生成口令信息$s = Agen(Dsalt, pw)$--例：

① 给口令$pw$撒盐：$Dpw = Asalt\ (Dsalt,\ pw)$;

② 用撒盐结果做密钥：$K = Dpw$;

③ 用一个64位的全0位串构造一个数据块$Dp$;

④ 设循环次数：$i = 0$;

⑤ 对数据块加密：$Dc = Acrypt(K, Dp)$;

⑥ $Dp = Dc,\ i = i + 1$;

⑦ 如果$i < 25$，则回到第⑤步;

⑧ 把数据块变换成字符串：$s = Atrans(Dc)$;

⑨ 返回$s$。

# 口令认证



- 攻击--Mallory找到（任意）某个用户口令
  - 如果原口令是六位数，盐是四位数，那么撒盐处理的结果就是十位数。
  - Mallory需要制作一个有10，000，000，000个条目的列表，并为每一个条目创建一个s。这个列表也有10，000，000，000个条目，比较这些条目要花费很长时间。

# 口令认证

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

## 固定口令（四）

### 注册环节：双因子认证

① 接收用户提供的口令*pw*（PIN）；

② 生成用户的其它信息（证书等），存入磁卡(或芯片卡、门卡）等，发放给用户；

③ 把口令信息*pw*等信息存入数据库的口令字段中。

### 登录环节：

① 接收用户提供的帐户名*Dname*、口令*pw*和证书等信息；

② 在帐户信息数据库中检查*Dname*的合法性，如果合法，则找出其对应的*pw*等信息；

③ 如果收到信息和存储数据相等，则认证成功，否则，认证失败。

# 口令认证

## 固定口令（四）

例：自动取款机认证--带有PIN(个人身份号码)的卡

- 银行卡属于“拥有某事”这一类，PIN属于“知道某事”这一类。

- 使用两种认证方式，故称为双因子认证：如果卡丢失了，不知道PIN的话，也不能使用。同样，看到用户输入的PIN，拿不到银行卡，也无法通过认证。

# 口令认证

加强固定（时不变）口令安全性的措施：

- 避免“弱”口令
- 口令扩展为通行短语

- 口令加盐
- 双因子认证

- 放慢口令映射
- 限制口令的尝试次数

# 本讲主要内容

- 身份鉴别的定义
- 口令身份鉴别
  - 固定口令
  - 一次口令
- 身份鉴别协议
  - 挑战应答协议
  - 零知识证明协议

# 口令认证

## （一）共享列表一次口令

### 注册环节：

① 接收用户提供的口令列表$\{pw_1, pw_2, ..., pw_t\}$；

② 每个口令分别生成口令信息：$\{s_i=\mathrm{F}(pw_i) \mid i=1,2,...,t\}$；

③ 把口令信息$\{s_i \mid i=1,2,...,t\}$存入数据库的口令字段中。

### 登录环节：第*i*次登录

① 接收用户提供的帐户名*Dname*和口令$pw_i$；

② 在帐户信息数据库中检查*Dname*的合法性，如果合法，则找出其对应的$s_i$；

③ 生成临时口令信息：$sr_i=\mathrm{F}(pw_i)$；

④ 如果$sr_i$与$s_i$相等，则认证成功，从列表中删除$s_i$；否则，认证失败。

# 口令认证

## （二）顺序更新一次口令

**注册环节：**

① 接收用户提供的初始口令 $pw_1$；

② 把口令信息$pw_1$存入数据库的口令字段中。

**登录环节：第*i*次登录**

① 接收用户提供的帐户名*Dname*和口令$pw_i$；以及下次认证口令的密文$c_{i+1} = \mathrm{E}_{pw_i}[pw_{i+1}]$；

② 在帐户信息数据库中检查*Dname*的合法性，如果合法，则找出其对应的$pw_i$；

③如果两个口令相等，则认证成功，执行步骤④；否则，认证失败。

④ 解密得$pw_{i+1} = \mathrm{D}_{pw_i}[c_{i+1}]$，覆盖数据库的口令字段中的$pw_i$。

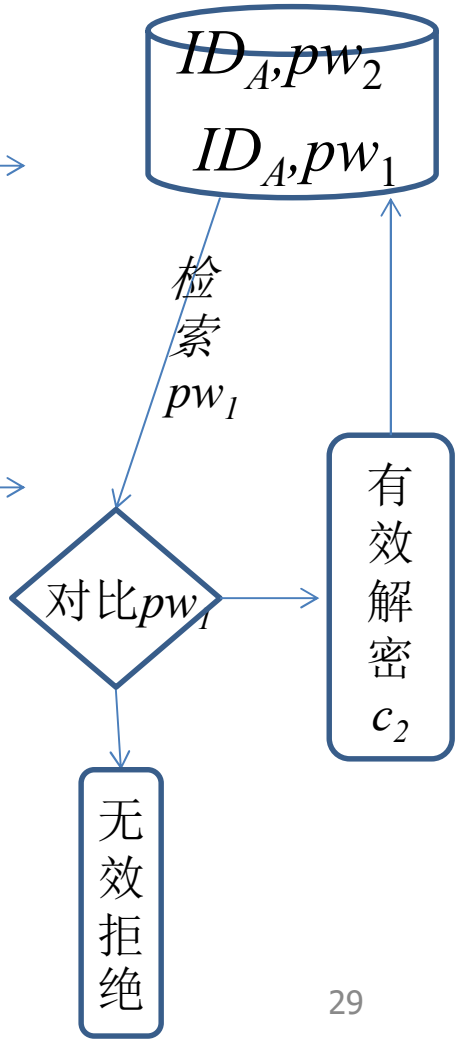
# 口令认证



A　　B

**注册阶段**　选$pw_1$　　$ID_A$ ， $pw_1$

**首次登录**　　$ID_A, pw_1, c_2=E_{pw_1}(pw_2)$



# 口令认证

## （三） Lamport一次口令

**注册环节：** 用户选初始口令w和一个计数器$t$，算出$h^t(w)$，这里$h^t$表示hash函数h散列$t$次：$w, h(w), h(h(w)), \ldots, h^t(w)$；

①接收用户提供的初始口令信息$h_t = h^t(w)$；

② 把口令信息$h_t$存入数据库的口令字段中。

**登录环节：第*i*次登录**

① 接收用户提供的帐户名$Dname$和口令$h_{t-i}$；

② 在帐户信息数据库中检查$Dname$的合法性，如果合法，则找出其对应的口令信息$h_{t-i+1}$；计算$h(h_{t-i}) = s$

③如果$s$和$h_{t-i}$相等，认证成功，执行步骤④；否则，认证失败。

④ 令$h_{t-i}$覆盖数据库的口令字段中的$h_{t-i+1}$。

# 口令认证



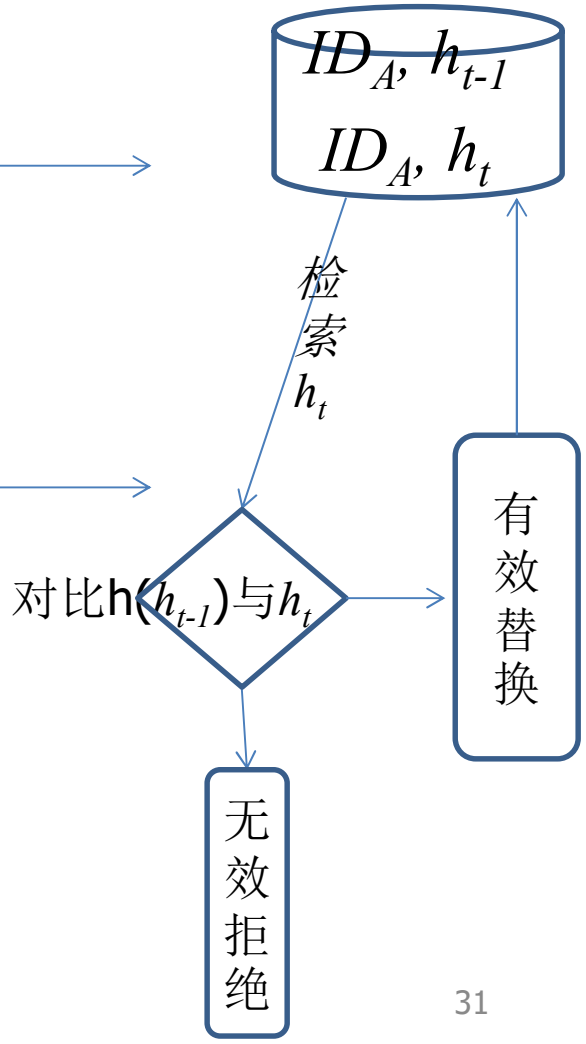
A　　B

**注册阶段**　选$w$
计算
$h^t(w)=h_t$

$ID_A$ ， $h_t$

**首次登录**

$ID_A$ , $h_{t-1}$



# 口令认证

- 共享口令列表一次口令
  - 安全：口令两两独立且随机
  - 效率：注册和更新过程计算量（随机数生成）和通信量大
  - 客户端需要安全存储设备，共享口令列表需要安全存储
- 顺序更新一次口令
  - 安全：不满足后向安全，即当前口令泄露，未来口令仍然安全；
  - 效率：无需额外的更新环节；每次身份鉴别计算量（随机数生成）和通信量略大；

# 口令认证

- 顺序更新一次口令
  - 客户端或许需要安全存储设备（或计算设备），因为口令频繁更换
- Lamport一次口令
  - 安全：不满足前向安全，即当前口令泄露，历史口令仍然安全（威胁不大）；
  - 效率：注册和更新过程计算量（hash迭代）大
  - 客户端或许需要安全存储设备（或计算设备），，因为口令熵要足够大

# 本讲主要内容

- 身份鉴别的定义
- 口令身份鉴别
  - 固定口令
  - 一次口令
- **身份鉴别协议**
  - **挑战应答协议**
  - 零知识证明协议

# 身份鉴别协议

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 协议：是一系列步骤，它包括两方和多方，设计它的目的是要完成一项任务。
  - 协议是从开始到结束的一个序列，每步必须依次执行
  - 完成协议至少需要两个人
  - 协议的目的是为了做一些事情

# 身份鉴别协议

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- Alice通过向Bob展示与秘密相关的知识来证明自己的身份，但在协议中并没有向Bob泄露秘密本身。

- 包括：
  - 基于对称密码技术的挑战-应答身份鉴别协议
  - 基于公钥密码技术的挑战-应答身份鉴别协议

# 身份鉴别协议

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

## 1）对称密码技术的挑战应答协议

每对用户可预先共享一个密钥，Alice证明他知道共享密钥的方式有两种：

- Alice可以对明文挑战加密，得到正确密文（或对密文挑战解密，得到正确明文）；
- Alice可以对挑战得到正确的认证码.

# 身份鉴别协议



- 基于对称加密系统的挑战-应答

$$A \leftarrow B: \quad r_B \qquad (1)$$

$$A \rightarrow B: \quad \mathbf{E}_K(r_B, B^*) \quad (2)$$

- 基于消息认证码系统的挑战-应答

$$A \leftarrow B: \quad r_B \qquad (1)$$

$$A \rightarrow B: \quad \mathbf{h}_K(r_B, B^*) \quad (2)$$

# 身份鉴别协议

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

## 2）公钥密码技术的挑战-应答协议

Alice拥有一对公钥$pk_A$和私钥$sk_A$，以及CA对其公钥的认证证书CA($A$), 她证明自己知道对应私钥的方法有两种：

- Alice可以解密一个（用$pk_A$加密的）密文挑战，得到正确明文
- Alice可以对一个挑战进行数字签名，使其可以通过签名验证算法Ver($pk_A$, .).

# 身份鉴别协议



- 基于公钥加密系统的挑战-应答

$$A \leftarrow B: \quad \mathbf{E}_{PKA}(r_B, A^*) \qquad (1)$$

$$A \rightarrow B: \quad r_B \qquad (2)$$

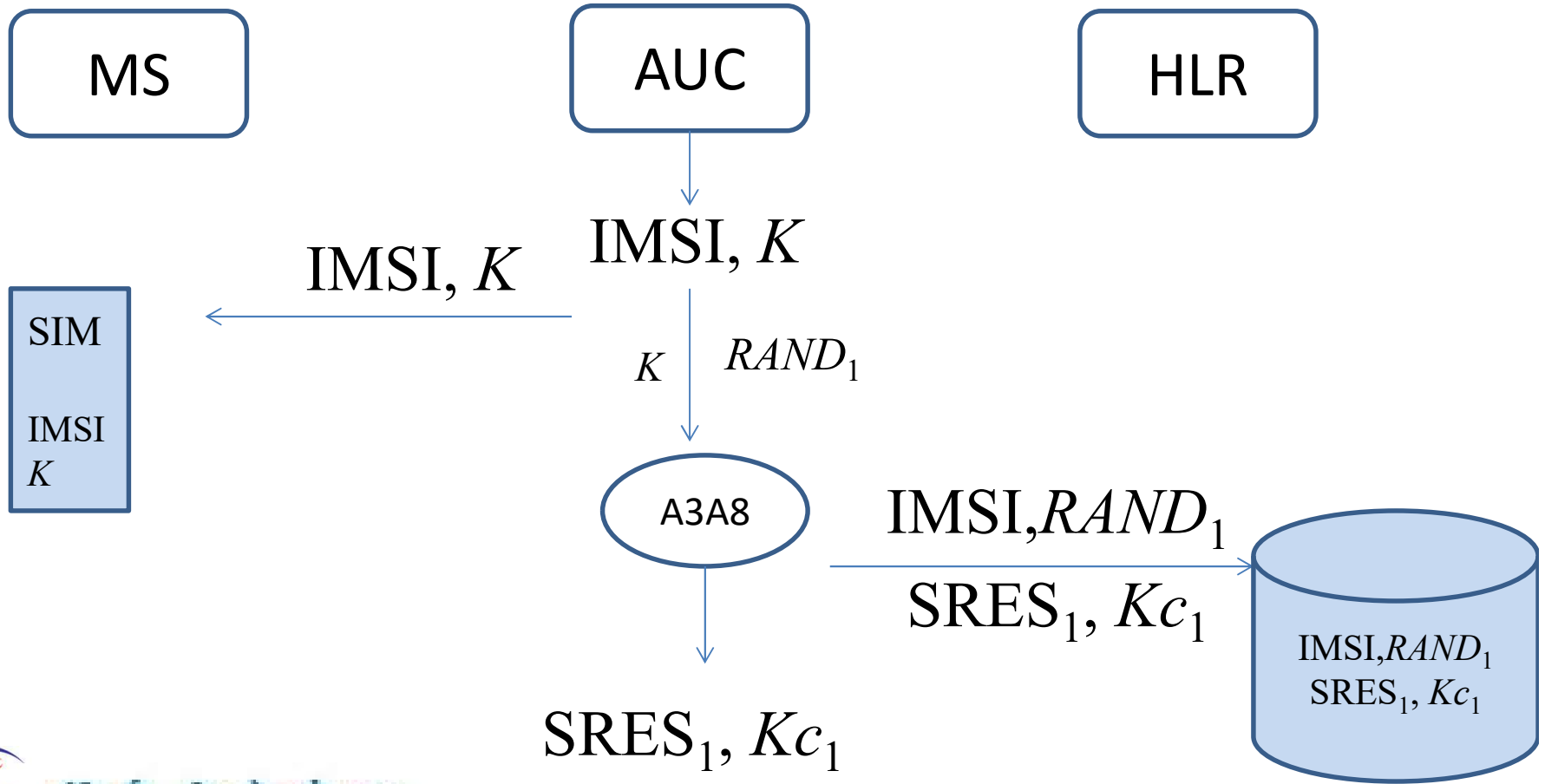
- 基于数字签名系统的挑战-应答

$$A \leftarrow B: \quad r_B \qquad (1)$$

$$A \rightarrow B: \quad cert_A, \mathbf{S}_{SKA}(r_B, B^*) \qquad (2)$$

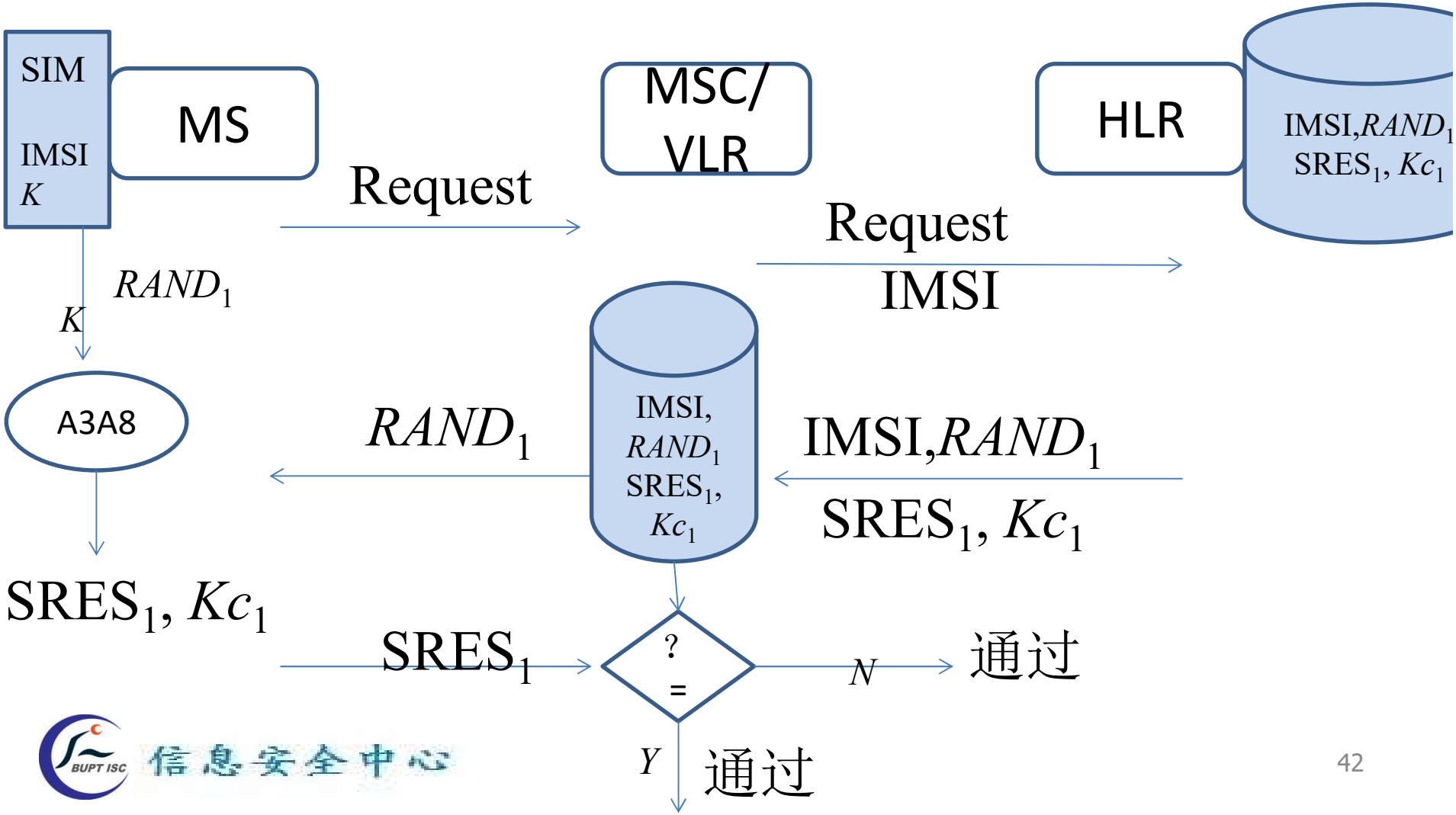
# 身份鉴别协议

## 例（一）　注册


MS
AUC
HLR
IMSI, K
IMSI, K
SIM
IMSI
K
K
RAND1
A3A8
IMSI,RAND1
SRES1, Kc1
IMSI,RAND1
SRES1, Kc1
SRES1, Kc1

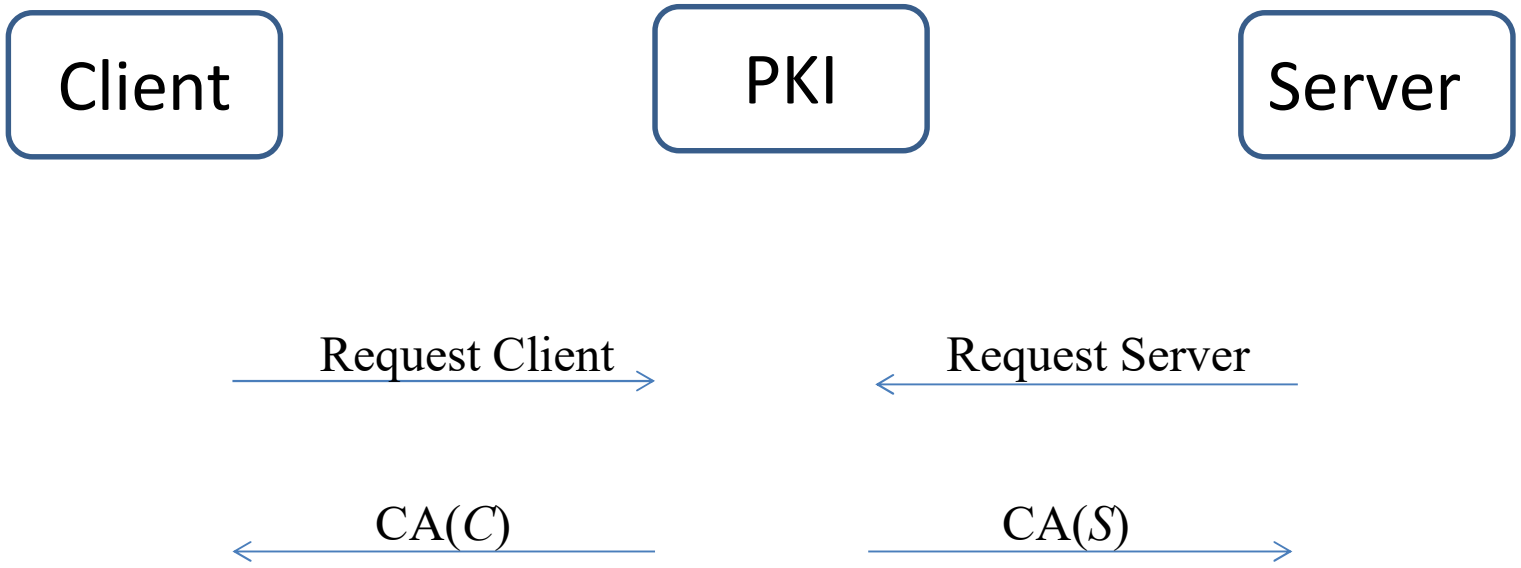
# 身份鉴别协议

## 例（一） 鉴别


SIM
IMSI
K
MS
MSC/
VLR
HLR
IMSI,RAND1
SRES1, Kc1
Request
Request
IMSI
RAND1
K
A3A8
RAND1
IMSI,
RAND1
SRES1,
Kc1
IMSI,RAND1
SRES1, Kc1
SRES1, Kc1
SRES1
?
=
N
通过
Y
通过

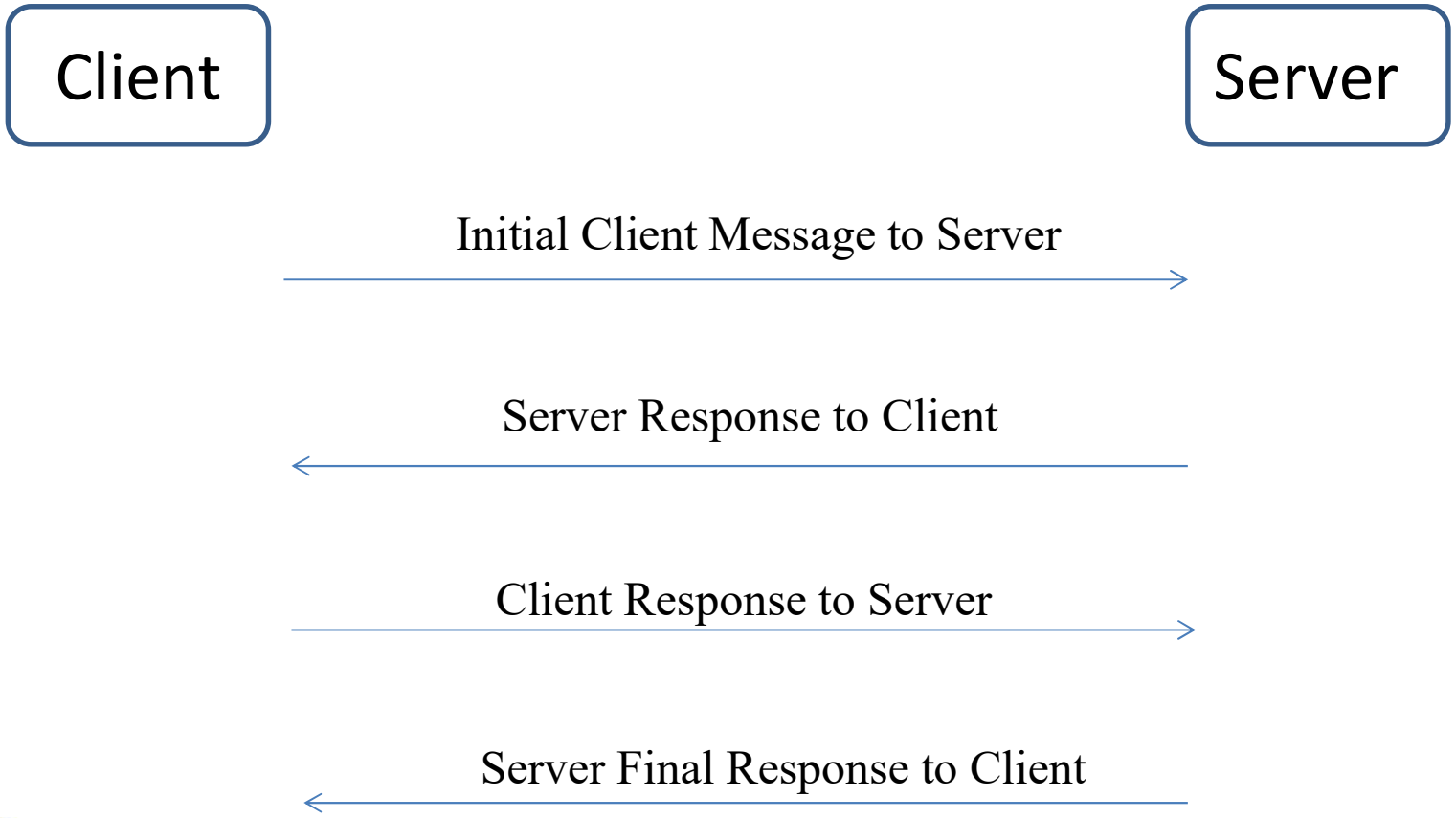
# 身份鉴别协议

## 例（二）　注册



# 身份鉴别协议

## 例（二）　鉴别


Client
Server
Initial Client Message to Server
Server Response to Client
Client Response to Server
Server Final Response to Client

# 身份鉴别协议



Client　　Server

**ClientHello** ——————→

**ServerHello**

**Certificate***

**ServerKeyExchange***

**CertificateRequest**

←—————— **ServerHelloDone**

# 身份鉴别协议



Client

Server

**Certificate***

**ClientKeyExchange**

**CertificateVerify***

**[ChangeCipherSpec]**

**Finished** ——————→

**[ChangeCipherSpec]**

←—————— **Finished**

# 本讲主要内容

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 身份鉴别的定义
- 口令身份鉴别
  - 固定口令
  - 一次口令
- 身份鉴别协议
  - 挑战应答协议
  - 零知识证明协议

# 身份鉴别协议



- 零知识(Zero-knowledge)(ZK)证明的起源

Alice：我知道肯德基的土豆泥的配方以及做法。

Bob：不，你不知道。

Alice：我知道。

Bob：你不知道。

Alice：我确实知道！

Bob：请你证实这一点！

Alice：好吧，我告诉你！(她悄悄说出土豆泥的秘方)

Bob：太有趣了！现在我也知道了。我要告诉《华盛顿邮报》

Alice：啊呀！

# 身份鉴别协议

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

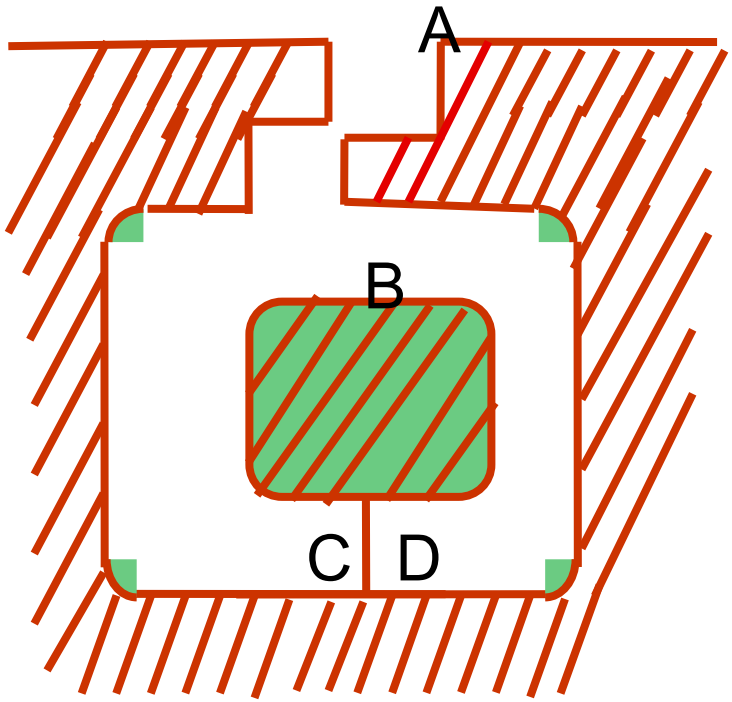
- 零知识证明的思想

  Alice要向Bob证明她知道某些秘密：

  - Bob：问Alice一系列问题
  - Alice：若知道那个秘密，她就能正确回答所有问题。如果她不知道，她仍有50%的机会回答每一个问题。但要猜对每个问题的机会实在太小了（几乎不可能）。
  - 大约10个问题之后，Bob确信Alice是否知道那个秘密。然而所有回答都没有给Bob提供Alice所知道的秘密的任何信息。

# 身份鉴别协议






设Alice知道咒语，可打开C和D之间的秘密门，不知道者都将走向死胡同中。

# 身份鉴别协议

(1)Bob站在 A 点;

(2)Alice进入洞中任一点 C 或 D;

(3)当Alice进洞之后，Bob走到 B 点;

(4)Bob叫Alice: (a)从左边出来，或(b)从右边出来;

(5)Alice按要求实现;

(6)Alice和Bob重复执行 (1)～(5)共n次。

# 身份鉴别协议



- 若 Alice 不知咒语，则在 B 点，只有50 %的机会猜中 Bob的要求，协议执行 $n$ 次，则只有 $2^{-n}$ 的机会完全猜中，若 $n$=16，则若每次均通过 Bob 的检验，B受骗机会仅为1/65536。
- 如果Bob用摄像机记录下他所看到的一切，他把录像给Carol看，Carol会相信这是真的吗？Carol是不会相信这是真的。
- 这说明了两件事情：其一，Bob不可能使第三方相信这个证明；其二，它证明了这个协议是零知识的。Bob在不知道咒语的情况下，显然不能从录像中获悉任何信息。

# 身份鉴别协议

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

身份鉴别协议满足条件：

- 在诚实的情况下，声称者Alice能向验证者Bob证明他确实是Alice ；
- 不同于Alice的实体C以Alice的身份，让Bob相信C是Alice的概率可忽略不计；
- 在声称者Alice向验证者Bob声称他的身份后，验证者Bob不能获得任何有用的信息，Bob也不能模仿Alice向其他第三方证明他就是Alice 。

# 身份鉴别协议

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

## Fiat-Shamir身份鉴别协议

参数生成：

- 可信中心T选择两个素数$p$和$q$(用完销毁)，计算类似RSA的模数$n=p\times q$、并公开$n$。
- 证明者选择与$n$互素的私钥$s(1\leqslant s<n)$，计算$v=s^2 \bmod n$
- 证明者在可信中心T中注册公钥$v$，私钥$s$秘密保存。

# 身份鉴别协议

若$t$轮都成功，则Bob就接收Alice的身份

协议执行：（连续地、独立地）迭代$t$轮

(1) Alice 取随机数 $r(<n)$，计算$x= r^2 \bmod n$，并发送给Bob；

(2) Bob将一随机比特 $e$=0或 1 作为挑战发给 Alice；

(3) Alice计算响应值$y$并发给Bob

- 若$e$=0，则Alice 将$y=r$送给Bob；
- 若$e$=1，则Alice将$y=r\times s \bmod n$送给Bob；

(4) 若$y$=0，则Bob拒绝证明；反之，验证$y^2\equiv x\times v^e \bmod n$？

- 若$e$=0，则Bob 证实$y^2 = x \bmod n$
- 若$e$=1，则 Bob 证实 $y^2 = x\times v \bmod n$

# 身份鉴别协议

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 完备性
  - 如果Alice和Bob遵守协议，且Alice知道$s$，则响应值 $y^2=(r\times s^e)^2 \bmod n \equiv x\times v^e \bmod n$，Bob接收Alice的证明，所以协议是完备的。
- 正确性
  - Alice不知道$s$，他也可取$r$，送$y^2=r^2 \bmod n$给Bob；Bob送$e$给Alice；Alice将$r$作为响应值；当$b$=0时则Alice可通过检验使得Bob受骗，当$b$=1时，则Bob可发现Alice不知$s$。Bob受骗概率为1/2;
  - 连续$t$轮受骗的概率将仅为$2^{-t}$.

# 本讲主要内容

- 身份鉴别的定义
- 口令身份鉴别
  - 固定口令
  - 一次口令
- 身份鉴别协议
  - 挑战应答协议
  - 零知识证明协议

# THE END !