

- 作业讲解

- TJ第2章练习13、14、15、16、19、22、28、29、30、31

- ~~– TJ第2章编程练习1、3~~

- CS第2.2节问题2、4、6、8、15、16、17、19

TJ第2章练习13

- 第一数学归纳法
 - 如果 $P(1)$ 是true, 且 $P(n)$ 是true $\rightarrow P(n+1)$ 是true
 - 那么 $P(n)$ 对所有 n 都是true
- 第二数学归纳法
 - 如果 $Q(1)$ 是true, 且 $Q(1).....Q(n)$ 都是true $\rightarrow Q(n+1)$ 是true
 - 那么 $Q(n)$ 对所有 n 都是true
- 第一 \rightarrow 第二 (UD第17章问题14, 去年此时的一道作业题)
 - 令 $P(n)$ 为“ $Q(1).....Q(n)$ 都是true”: 欲证 $Q(n)$ 对所有 n 都是true, 即证 $P(n)$ 对所有 n 都是true
 - Base case: $Q(1)$ 是true $\rightarrow P(1)$ 是true
 - Induction: $P(k)$ 是true $\rightarrow Q(1).....Q(k)$ 都是true $\rightarrow Q(k+1)$ 是true $\rightarrow Q(1).....Q(k+1)$ 都是true $\rightarrow P(k+1)$ 是true $\rightarrow P(n)$ 对所有 n 都是true
- 第二 \rightarrow 第一
 - 令 $Q(n)$ 为“ $P(n)$ 是true”: 欲证 $P(n)$ 对所有 n 都是true, 即证 $Q(n)$ 对所有 n 都是true
 - Base case: $P(1)$ 是true $\rightarrow Q(1)$ 是true
 - Induction: $Q(1).....Q(k)$ 是true $\rightarrow Q(k)$ 是true $\rightarrow P(k)$ 是true $\rightarrow P(k+1)$ 是true $\rightarrow Q(k+1)$ 是true $\rightarrow Q(n)$ 对所有 n 都是true

TJ第2章练习29

- 反证法：假设有限个，即 p_1, \dots, p_k
- 令 $N=p_1 \dots p_k$ ，设 p 为 N^2-N+1 的一个质因子（显然不同于 p_1, \dots, p_k ），则 p 也能整除 $(N^2-N+1)(N+1)=N^3+1$ ，即 $N^3 \equiv -1 \pmod{p}$ ，因此 $N^6 \equiv 1 \pmod{p}$
- 所以， N 在群 Z_p^* 中，且 N 的阶可能是1、2、3、6
 - 由于 $N^3 \equiv -1 \pmod{p}$ ，所以阶不为3，显然也不能为1
 - 如果阶为2：即 $N^2 \equiv 1 \pmod{p}$ ，而 $N^3 \equiv -1 \pmod{p}$ ，因此 $N \equiv -1 \pmod{p}$ ，于是 p 能整除 $N+1$ 和 N^2-N+1 ，即 $\gcd(N+1, N^2-N+1) \geq p$ ，而由 $N^2-N+1=(N+1)(N-2)+3$ 可知 $\gcd(N+1, N^2-N+1) = \gcd(N+1, 3) \leq 3$ ，所以 $p \leq 3$ ，即 p 为2或3，但是，由 N 形如 $6n+1$ 可知 N^2-N+1 也形如 $6n+1$ ，作为其因子的 p 不可能是2或3，矛盾
 - 所以阶只能为6
- 因此，6能整除 $|Z_p^*| = p-1$ ，于是 p 也形如 $6n+1$ ，与假设矛盾

TJ第2章练习30

- 反证法：假设有限个，即 p_1, \dots, p_k
- 令 $N=(p_1 \dots p_k)^2+2$ ，则 $N \equiv_4 3$
- 而 N 是奇数且不含任何形如 $4n-1$ 的因子，因此 N 的质因子都形如 $4n+1$ ，则 $N \equiv_4 1$ ，矛盾

CS第2.2节问题15

- $k=jq+r$
relationship between $\gcd(j,k)$ and $\gcd(r,k)$?
- $\gcd(j,k)=\gcd(r,j)$
→ $j=x_j\gcd(r,j)$, $k=x_k\gcd(r,j)$
以及 $r=x_r\gcd(r,j)$
→ $\gcd(r,k)=\gcd(x_r,x_k)\gcd(r,j)$
→ $\gcd(r,j) \mid \gcd(r,k)$
即 $\gcd(j,k) \mid \gcd(r,k)$

- 教材讨论
 - TJ第7章
 - TC第31章第7、9节

问题1： 对称密钥加密和公开密钥加密

- 太公曰：“主与将，有阴符，凡八等。有大胜克敌之符，长一尺。破军擒将之符，长九寸。降城得邑之符，长八寸。却敌报远之符，长七寸。警众坚守之符，长六寸。请粮益兵之符，长五寸。败军亡将之符，长四寸。失利亡士之符，长三寸。诸奉使行符，稽留，若符事闻，泄告者，皆诛之。八符者，主将秘闻，所以阴通言语，不泄中外相知之术。敌虽圣智，莫之能识。”
- 你理解这种加密方法了吗？

问题1: 对称密钥加密和公开密钥加密 (续)

- 斯巴达司令派人给前线送一条这样的腰带:
KGDEINPKLRIJLFGOKLMNISOJNTVWG
- 你能猜到使用的加密方法吗?
- **KGDEINPKLRIJLFGOKLMNISOJNTVWG**

问题1: 对称密钥加密和公开密钥加密 (续)

- 一条战场快讯: WECRLTEERDSOEFEAOCAVDEN
- 你能猜到使用的加密方法吗?

```
W . . . E . . . C . . . R . . . L . . . T . . . E  
. E . R . D . S . O . E . E . F . E . A . O . C .  
. . A . . . I . . . V . . . D . . . E . . . N . .
```

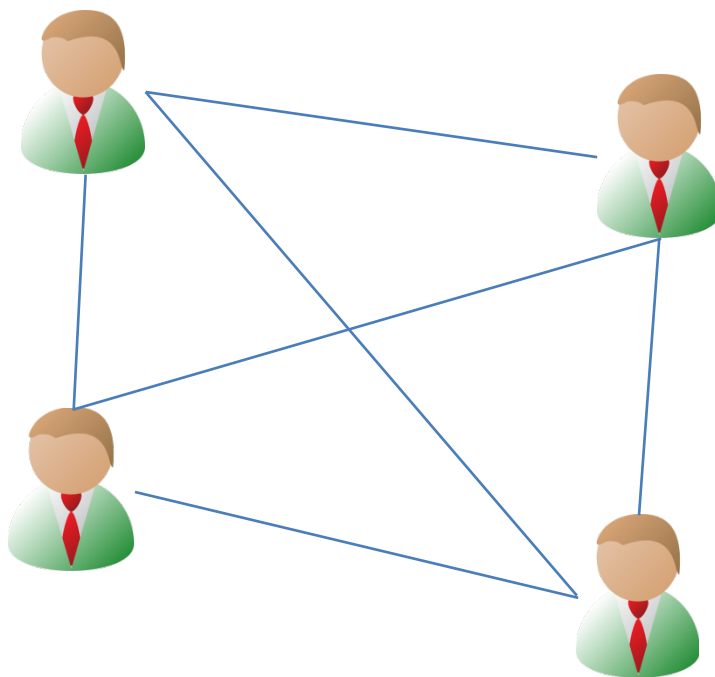
问题1： 对称密钥加密和公开密钥加密 (续)

- 对称密钥加密(private/symmetric key cryptography)
- 公开密钥加密(public/asymmetric key cryptography)

- 它们分别是什么含义？
- 各有什么优缺点？
- 你能设计一种新的方式，结合两者的优点吗？
 - Because symmetric key algorithms are nearly always much less computationally intensive than asymmetric ones, it is common to exchange a key using a key-exchange algorithm, then transmit data using that key and a symmetric key algorithm.

问题1： 对称密钥加密和公开密钥加密 (续)

- 四个人之间采用对称密钥加密两两间的通讯，你认为需要几个密钥？
- 如果采用公开密钥加密呢？



问题1： 对称密钥加密和公开密钥加密 (续)

- 你能简述如何生成RSA的公钥和私钥吗？

1. Select at random two large prime numbers p and q such that $p \neq q$. The primes p and q might be, say, 1024 bits each.
2. Compute $n = pq$.
3. Select a small odd integer e that is relatively prime to $\phi(n)$, which, by equation (31.20), equals $(p - 1)(q - 1)$.
4. Compute d as the multiplicative inverse of e , modulo $\phi(n)$. (Corollary 31.26 guarantees that d exists and is uniquely defined. We can use the technique of Section 31.4 to compute d , given e and $\phi(n)$.)
5. Publish the pair $P = (e, n)$ as the participant's *RSA public key*.
6. Keep secret the pair $S = (d, n)$ as the participant's *RSA secret key*.

- 如何加密、解密？

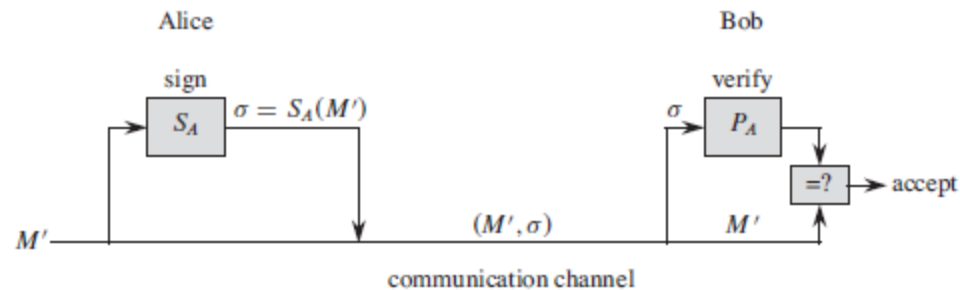
$$P(M) = M^e \bmod n$$

$$S(C) = C^d \bmod n$$

- 如果先解密、再加密，会怎么样？
- 破解RSA的关键是什么？为什么？

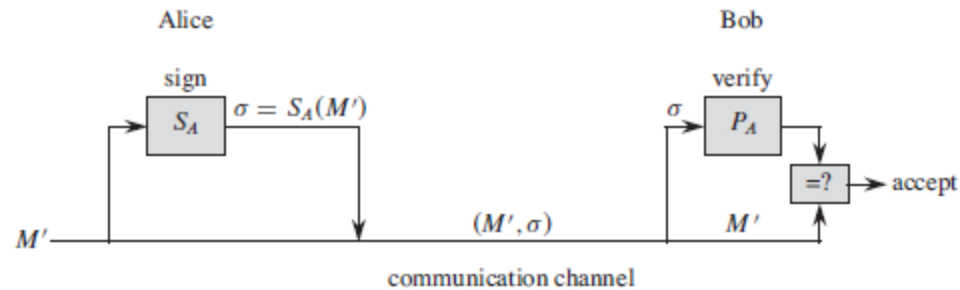
问题2： 数字签名

- 如何利用数字签名分别实现这些目的？
 - 验证发送者身份
 - 验证数据完整性
 - 发送者不可抵赖
- 如何基于公开密钥加密实现数字签名？ 和之前的加密/解密过程最大的区别是什么？



问题2：数字签名

- 如何利用数字签名分别实现这些目的？
 - 验证发送者身份
 - 验证数据完整性
 - 发送者不可抵赖
- 如何基于公开密钥加密实现数字签名？和之前的加密/解密过程最大的区别是什么？



- 你有没有办法设计一种基于对称密钥加密的数字签名？

问题2：数字签名 (续)

- 这种身份验证的过程靠谱吗？



$S_A(\text{我是A})$



$P_A(S_A(\text{我是A})) = \text{我是A}$
所以他真是A!

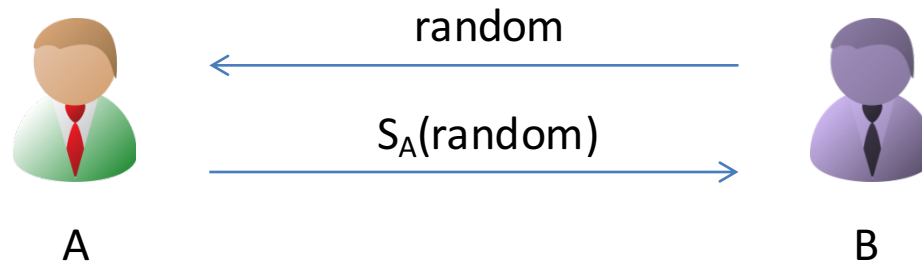
作为一个坏人，你能想出什么办法来冒充A？

从A获取“ $S_A(\text{我是A})$ ”，向B重放

怎么改进？

问题2：数字签名 (续)

- 改进



$P_A(S_A(\text{random})) = \text{random}$
所以他真是A!

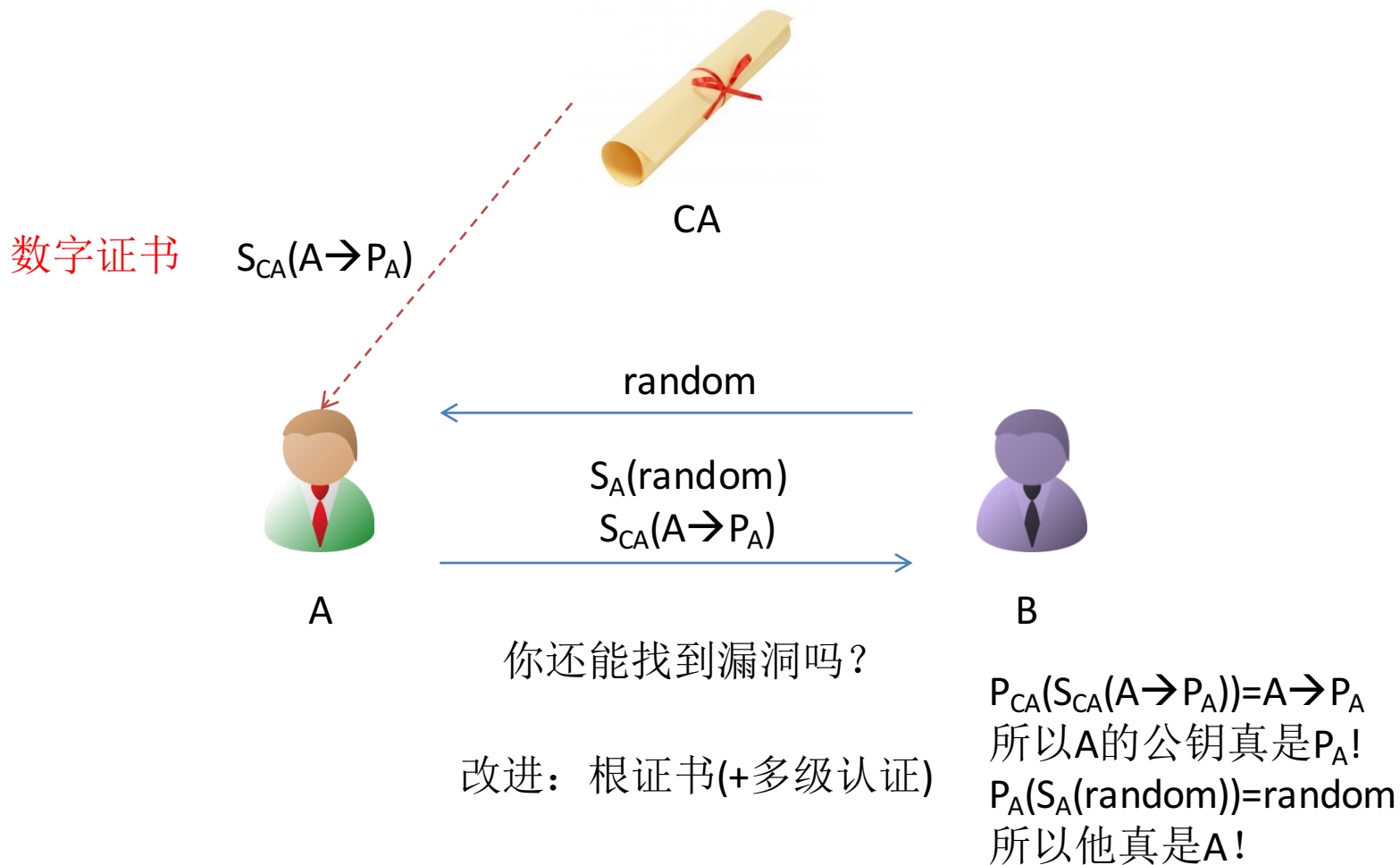
作为一个坏人，你又能想出什么办法来冒充A?

换掉B保存的 P_A

怎么改进?

问题2：数字签名 (续)

- 继续改进



问题2：数字签名 (续)

- 为了验证数据完整性，除RSA以外，还有更简单的方法吗？
 - 奇偶校验、MD5.....
- 与RSA相比，这些方法的优缺点是什么？
 - 数据量小
 - 安全性差
- 如何结合两者的优点？