中山大學
SUN YAT-SEN UNIVERSITY

Module I. Fundamentals of Information Security

Chapter 3
Authentication Technologies

Information Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- **3.1 Overview**
  - Introduction to Authentication Technologies
  - The Weak/Strong Authentication Scheme
  - The Application of Authentication Technologies
  - The Attack to Authentication
  - The Security Guidelines to Protect Authentication Schemes
- **3.2 Public Key Infrastructure**
  - Introduction to PKI
  - PKIX
  - The Management of PKIX
  - Public Key Certificate
  - Trust Hierarchy Model

Outline

- **3.3 Kerberos**
  - What is Kerberos
  - Description
  - Kerberos Process
  - Drawbacks & Limitations
- **3.4 X.509**
  - What is X.509
  - History and Version
  - Certificate
  - Security problems
  - Application

3.1 Overview

3.1.1 Introduction to Authentication Technologies

- **Identification, Authorization and Authentication** (身份识别、授权与认证)
  - Identification
    - ✧ Identification aims at determining whether an individual is known to the system.
  - Authorization
    - ✧ Authorization is the process of granting the user access to specific system resources based on his/her profile and local/global policy controlling the resource access.
  - Authentication
    - ✧ Authentication is to prove or show (something, especially a claim or an artistic work) to be true or genuine.

3.1 Overview

3.1.1 Introduction to Authentication Technologies

- **Prover** and **Verifier**
  - Prover and verifier are two parties involved in authentication
    - Prover
      - A claimant 申请者/声称者
      - A prover presents its identity and a proof of that identity.
    - Verifier
      - A recipient 接受者/验证方
      - A verifier checks the prover's proof to ensure the identity of the prover.

3.1 Overview

3.1.1 Introduction to Authentication Technologies

- **Entity Authentication** and **Message Authentication**
  - Entity Authentication 实体认证
    - ✧ *Entity Authentication* can be defined as the process through which the identity of an entity (such as an individual, a computer/an operating process, an application, or a network) is demonstrated.
    - ✧ 实体认证是对实体身份的证明过程。实体可以是个人、计算机、操作进程、应用、网络等等。
  - Message Authentication 消息认证
    - ✧ *Message Authentication* provides the assurance that a message has not been modified during its transmission.
    - ✧ 消息认证用于确保消息在其传送过程中没有被窜改。

3.1 Overview

3.1.1 Introduction to Authentication Technologies

- **Entity Authentication** and **Message Authentication**
  - *Differences*
    - ✧ Entity authentication involves no meaningful message except the claim of being an entity.
    - ✧ Message authentication does not provide time-related guarantees with respect to when the message has been created, signed, sent, or delivered to destination.

3.1 Overview

3.1.1 Introduction to Authentication Technologies

- **Goals of an Authentication**
  - An authentication protocol is a process to *achieve* the following goals:
    - ✧ The probability that a third party different from the prover, using the authentication protocol and impersonating the prover, can cause the verifier to authenticate the third party as the prover, is neglectable. (第三方假冒申请人，通过认证协议，使得审议人将第三方身份认证为申请人的概率可以忽略不计)
    - ✧ The verifier should not be able to reutilize the information provided by the prover to impersonate him/her (the prover) to a third party. (审议人不能够重复使用申请人提供的信息向第三方假冒申请人身份)
    - ✧ A signed message cannot be recovered from the signature code during signature verification. (签名验证过程中不能够从签名代码恢复签名保护的消息)

3.1 Overview

3.1.1 Introduction to Authentication Technologies

- **Three Classes of Entity Authentication** 实体认证的三种类型
  - Know-object-based authentication
    - ✧ 基于原始信息的
    - ✧ E.g., password, PIN, ...
  - Passed-object-based authentication
    - ✧ 基于持有证明的
    - ✧ E.g., credit card, smart card, ...
  - Biometric-object-based authentication
    - ✧ 基于生物学特征的
    - ✧ E.g., fingerprints, retinal pattern, voice, hand geometry, keystroke dynamics, ...

3.1 Overview

3.1.2 The Weak/Strong Authentication Scheme

- **The Weak Authentication Scheme**
  - Base on the password
    - ✧ Password authentication is perhaps the most common way of authenticating a user to an electronic system
    - ✧ Entity provides a (login, password) pair; Differ somewhat by the technique used to perform the verification and store the information providing password verification
    - ✧ Non-time-varying password schemes present various security weakness

3.1 Overview

3.1.2 The Weak/Strong Authentication Scheme

- **The Weak Authentication Scheme**
  - Base on PIN
    - ✧ PIN schemas can be classified as special time-invariant passwords.
    - ✧ This scheme represents a vulnerability that should be covered by additional constraints.
    - ✧ Online/Off-line verification.

3.1 Overview

3.1.2 The Weak/Strong Authentication Scheme

- **The Strong Authentication Scheme**
  - Challenge-Response with password
    - ✧ Secret key cryptography 对称密码学方法

      r : a random number generated by *Bob*

      r' : a random number generated by User *Alice*

      K : the secret key shared by the prover and verifier

      C_K : a secret-key cryptographic function with key-K

      m : optional message used to prevent replay attacks

      $H()$: a hash function

      - The authentication of *Alice*: (*Alice* - prover, *Bob* - verifier)

        Bob : $r \Rightarrow A$ (*Bob* sent a random number r to *Alice*)

        Alice : $C_K(<r, m>) \Rightarrow$ *Bob*
      - Mutual authentication:

        Bob : $r \Rightarrow$ *Alice*

        Alice : $C_k(H(<r, r', m>)) \Rightarrow$ *Bob*

        Bob : $C_k(H(<r, r', m'>)) \Rightarrow$ *Alice*

3.1 Overview

3.1.2 The Weak/Strong Authentication Scheme

- **The Strong Authentication Scheme**
  - Challenge-Response with password
    - ✧ Public key cryptography 非对称密码学方法

      r : a random number generated by *Bob*

      K_{PUa}: the public key of *Alice*

      K_{PRa}: the private key of *Alice*

      $C(K, -)$: a public-key encryption function with parameter K

      $D(K, -)$: a public-key decryption function with parameter K

      m : optional message used to prevent replay attacks

      $H()$: a hash function

      - ◌ The authentication of *Alice*: (*Alice* - prover, *Bob* - verifier)

        Bob : $c = C(K_{PUa}, <r, m>, H(r))$; $c \Rightarrow$ *Alice*

        Alice : $D(K_{PRa}, c)$; $r \Rightarrow$ *Bob*

      - ◌ Mutual authentication:

3.1 Overview

3.1.2 The Weak/Strong Authentication Scheme

- **Zero-knowledge Authentication**
  - The zero-knowledge Proof (零知识证明)
    - A zero-knowledge proof must satisfy three properties:
      - **Completeness**: if the statement is true, the honest verifier will be convinced of this fact by an honest prover. (完备性)
      - **Soundness**: if the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability. (有效性)
      - **Zero-knowledge**: if the statement is true, no cheating verifier learns anything other than the fact that the statement is true. That is, just knowing the statement (not the secret) is sufficient to show that the prover knows the secret.
    - The first two properties are of more general interactive proof systems. The third is what makes the proof zero-knowledge.

3.1 Overview

3.1.2 The Weak/Strong Authentication Scheme

- **Zero-knowledge Authentication**
  - The zero-knowledge Proof (零知识证明)
    - ✧ Zero-knowledge proofs are probabilistic "proofs" rather than deterministic proofs. There is some small probability, the *soundness error* (失效), that a cheating prover will be able to convince the verifier of a false statement.
    - ✧ The zero-knowledge authentication (零知识认证) is a form of interactive proof, during which the prover and the verifier exchange various messages and random numbers to achieve authentication.
  - *Example*.
    - ✧ The *Ali Baba* cave
    - ✧ *Alice* claims that she knows a secrete key *s* without showing it to *Bob*
    - ✧ *Fiat-Shamir* algorithm (*Amos Fiat* and *Adi Shamir*, 1986)
    - ✧ *Feige-Fiat-Shamir* identification scheme (*Uriel Feige*, *Amos Fiat,* and *Adi Shamir* 1988)

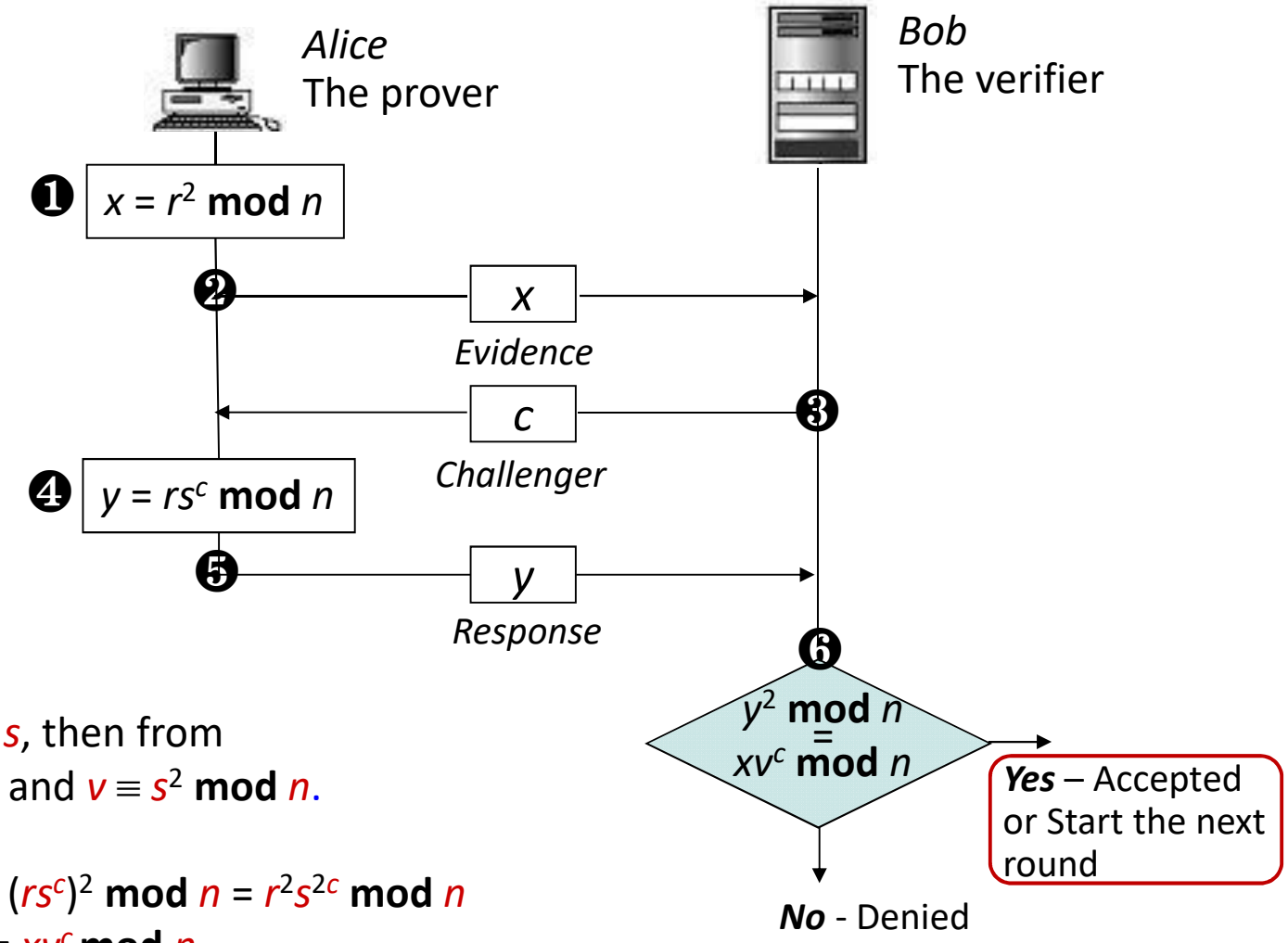
3.1 Overview

3.1.2 The Weak/Strong Authentication Scheme

- **Zero-knowledge Authentication**
  - *Fiat-Shamir* algorithm.
    - n : $n=p\times q$, p, q are big primes. n is generated by a trusted third party and released in public, p, q kept in secret (or destroyed).
    - s : *Alice*'s secrete key, $0<s<n$. *Alice* must proof that she knows s, without showing s to anyone.
    - v : *Alice*'s "public key" satisfying $v \equiv s^2$ **mod** n.
      - *Alice* computes and shows v to *Bob*.
      - It is hard to know s from v. (as hard as the factoring large numbers problem when $n=p\times q$, as selected)
    - r : *Alice* selected a random number r, $0<r<n-1$, and start the process.
    - x : $x = r^2$ **mod** n as an evidence, computed by *Alice* and sent to *Bob*.
    - c : The challenger randomly selected in {1, 0} from *Bob*.
    - y : $y = rs^c$ **mod** n as the response, computed by *Alice* and sent to *Bob*.

3.1 Overview

– *Fiat-Shamir* algorithm.



If *Alice* knows s, then from

$x=r^2 \bmod n$ and $v \equiv s^2 \bmod n$.

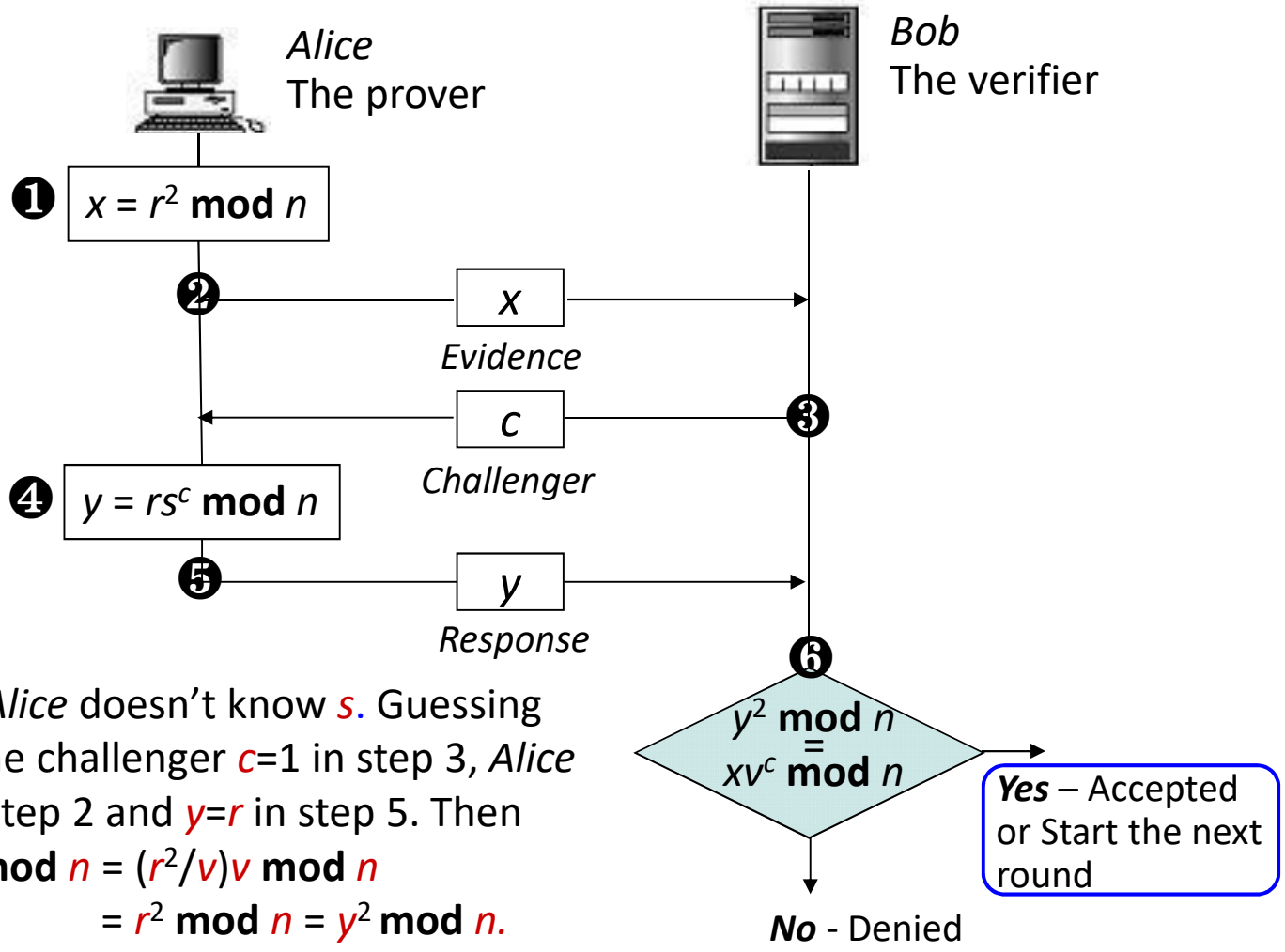
We have

$y^2 \bmod n = (rs^c)^2 \bmod n = r^2 s^{2c} \bmod n$

$= xv^c \bmod n$.

3.1 Overview

– *Fiat-Shamir* algorithm.



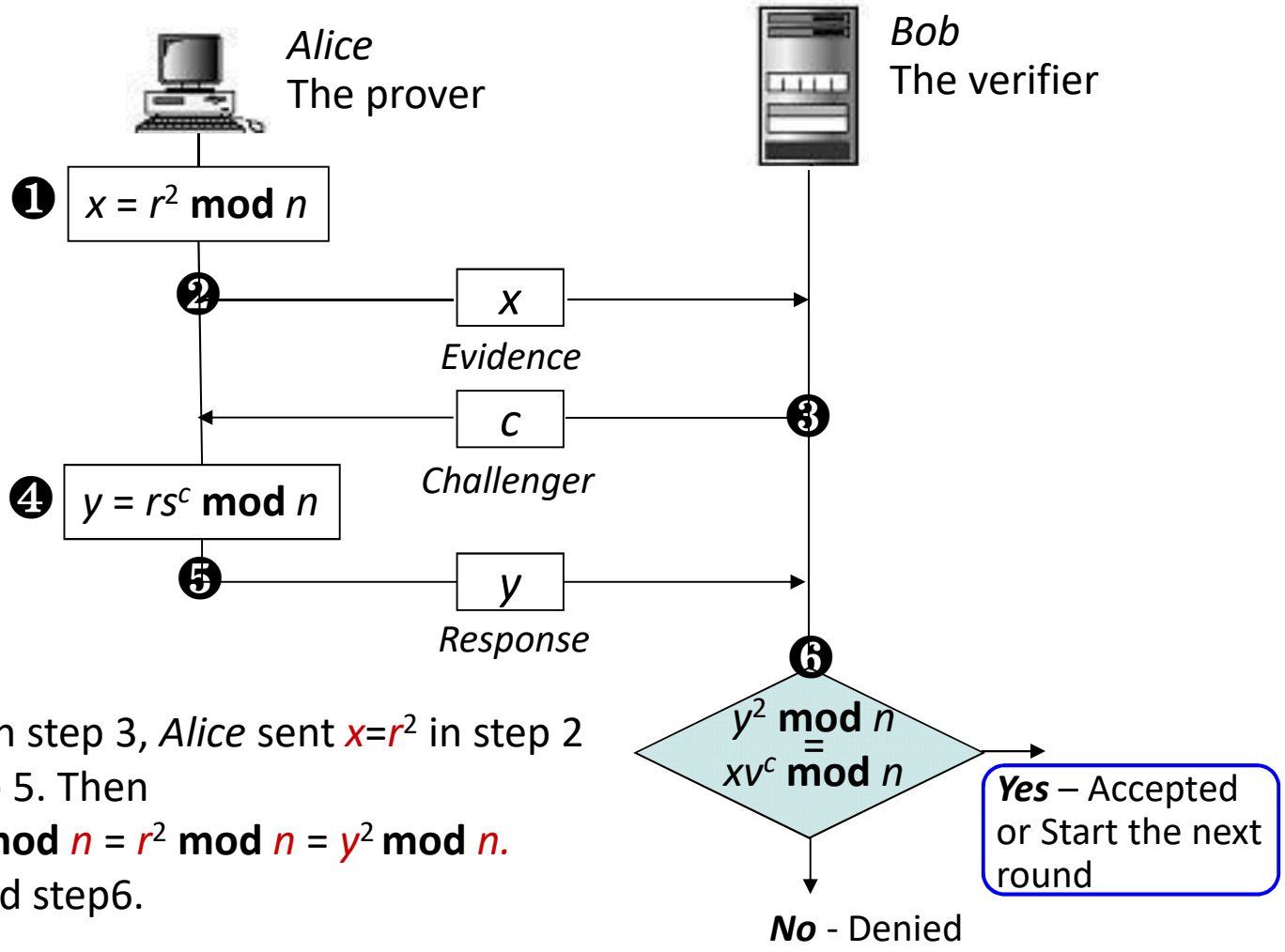
Suppose that *Alice* doesn't know s. Guessing *Bob* sending the challenger c=1 in step 3, *Alice* sent $x=r^2/v$ in step 2 and $y=r$ in step 5. Then

$$xv^c \bmod n = (r^2/v)v \bmod n$$
$$= r^2 \bmod n = y^2 \bmod n.$$

and passed step6.

3.1 Overview

– *Fiat-Shamir* algorithm.



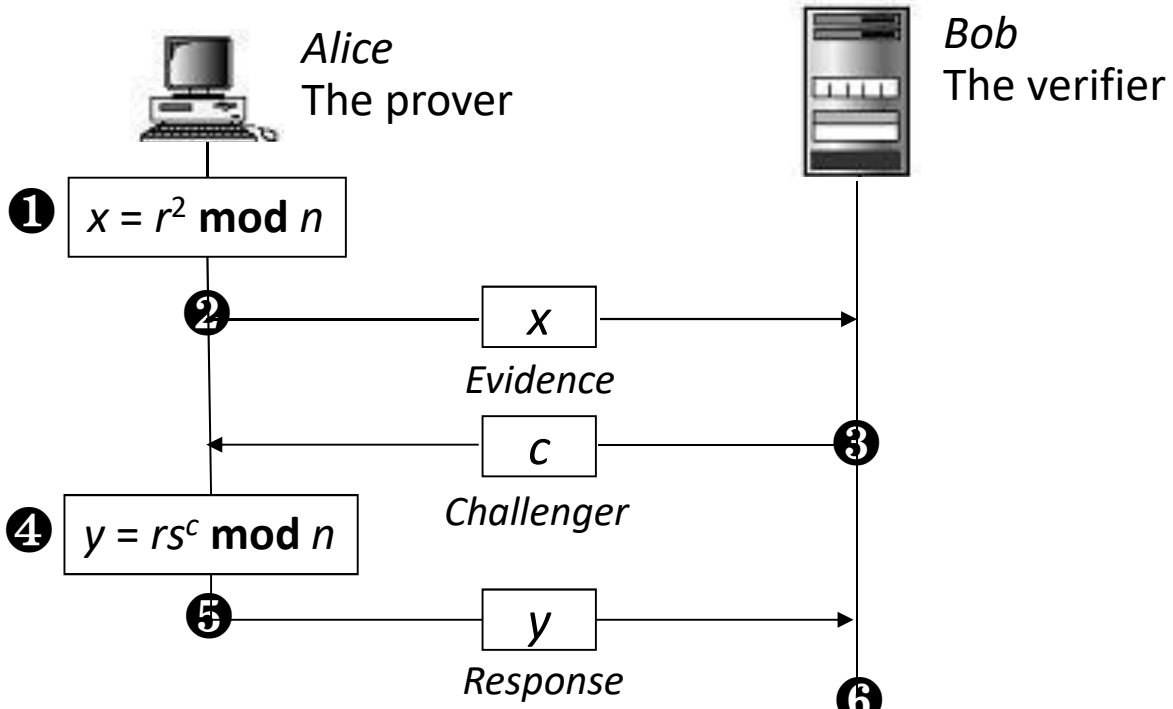
Guessing c=0 in step 3, *Alice* sent $x=r^2$ in step 2 and $y=r$ in step 5. Then

$$xv^c \bmod n = r^2 \bmod n = y^2 \bmod n.$$

and also passed step6.

3.1 Overview

– *Fiat-Shamir* algorithm.



The challenge-response (step1-6) takes *k* rounds (*k*=20 may be). *Alice* will be denied if a dismatch firstly occurs in step 6. The challenger randomly selected in {1, 0} from *Bob* and the probability that *Alice* passed the verification illegally is $1/(2^k)$, 1ppm.

3.1 Overview

3.1.2 The Weak/Strong Authentication Scheme

- **Zero-knowledge Authentication**
  - Base on Device
    - ✧ Using device to help user authentication in a hostile environment (敌对环境).
    - ✧ The device's key is randomly selected out of the key space of the embedded cryptographic algorithm.
    - ✧ Since the key is strong, the probability of success of a brute force attack is almost null.

3.1 Overview

3.1.3 The Application of Authentication Technologies

- **X.509**
  - The ITU-T recommendation X.509 defines a directory service that maintains a database of information about users for the provision of authentication services.
- **Kerberos**
  - Kerberos is an authentication service developed at MIT which allows a distributed system to be able to authenticate requests for service generated from workstations.

3.1 Overview

3.1.4 The Attack to Authentication

- Impersonation attacks
  - 假冒攻击
- Replay attacks
  - 重放攻击
- Forced delay attacks
  - 强迫延时攻击
- Interleaving attacks
  - 交错攻击
- Oracle session attack
  - Oracle 会话攻击
- Parallel session attack
  - 并行会话攻击

3.1 Overview

3.1.5 The Security Guidelines to Protect Authentication Schemes

- Risk Mitigation Strategy (风险降低策略)
  - When a weak authentication based on passwords is used, a pass-policy should be stated and should include rules describe how to manage a user's accounts.
  - Implementation of a risk mitigation strategy
    - ✧ The authentication process and the integrity service should use different keying materials (密钥资料) if necessary.
    - ✧ The working stations procedures should be protected and tightly synchronized, if they are involved in the timestamps' computation and verification.
    - ✧ Anonymous remote attempts of authentication should be unauthorized and limit the number of try.
    - ✧ Security parameters should take the reduction of the probability of successful attacks into consideration.

3.1 Overview

3.1.5 The Security Guidelines to Protect Authentication Schemes

- Risk Mitigation Strategy
  - Implementation of a risk mitigation strategy
    - ✧ In the case where a trust relationship is defined between servers, authentication-related configurations should be reviewed carefully.
    - ✧ Assessing the cryptographic and digital signature.
    - ✧ In assessing an authentication scheme, the potential impact of compromise of keying material should be studied (在作认证方案评估时，对危及密钥资料的潜在威胁须加研究).

End of Chapter 3.1