به نام خدا

دانشکده مهندسی برق،
دانشگاه صنعتی شریف

مبانی رمزنگاری و امنیت شبکه

مدیریت کلید در سیستم‌های رمزنگاری

Key Management and Distribution

مهتاب میرمحسنی

نیم‌سال دوم (بهار) ۹۸-۹۹

مدیریت کلید

- **رمزنگاری متقارن**
  - مبادله کلید مخفی میان دو طرف
  - تغییر کلید جهت حفاظت از داده‌ها در صورت لو رفتن کلید
- **توزیع کلید مخفی (مورد استفاده در رمزنگاری متقارن)**
  - رمزنگاری متقارن
  - رمزنگاری کلید همگانی
- **رمزنگاری کلید همگانی**
  - توزیع کلیدهای همگانی

توزیع کلید مخفی با استفاده از رمزنگاری متقارن

سناریوهای ممکن برای مبادله کلید میان دو کاربر A و B

1. A کلید را انتخاب و به طور فیزیکی در اختیار B قرار دهد
2. شخص سومی کلید را انتخاب و به طور فیزیکی در اختیار A و B قرار دهد
3. اگر A و B در گذشته کلید مخفی مشترکی را در اختیار داشتند، A کلید جدید را با کلید قبلی رمزگذاری کرده و به B بفرستد
4. اگر A و B هر کدام یک ارتباط رمزشده (امن) با شخص سوم C داشته باشند، C کلید را انتخاب و از طریق این ارتباط‌ها در اختیار A و B قرار می‌دهد

توزیع کلید مخفی با استفاده از رمزنگاری متقارن

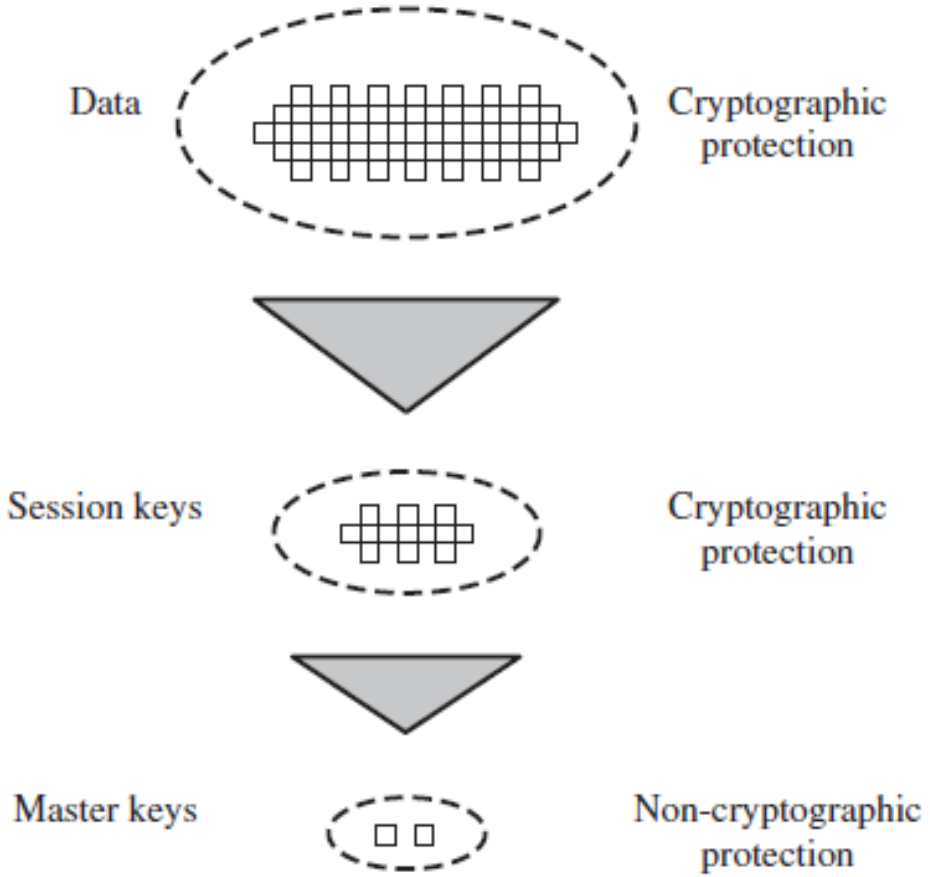
سناریوهای ممکن برای مبادله کلید میان دو کاربر A و B

1. A کلید را انتخاب و به طور فیزیکی در اختیار B قرار دهد
2. شخص سومی کلید را انتخاب و به طور فیزیکی در اختیار A و B قرار دهد
3. اگر A و B در گذشته کلید مخفی مشترکی را در اختیار داشتند، A کلید جدید را با کلید قبلی رمزگذاری کرده و به B بفرستد
4. اگر A و B هر کدام یک ارتباط رمزشده (امن) با شخص سوم C داشته باشند، C کلید را انتخاب و از طریق این ارتباط‌ها در اختیار A و B قرار می‌دهد

- رمزنگاری یال (link): ۱و ۲
- رمزنگاری انتها-به-انتها (end-to-end): تعداد زیادی کلید به صورت پویا اختصاص یابد
  - سیستم‌های توزیع شده
  - در لایه شبکه یا IP: هر زوج کاربر یک کلید ← برای N میزبان تعداد $N(N\text{-}1)/2$ کلید لازم است
  - در لایه کاربرد: هر زوج فرآیند یک کلید ← به مراتب بیشتر از حالت قبل
- ایراد ۳: اگر یک کلید لو رود، همه کلیدهای بعدی لو می‌رود- توزیع اولیه کلیدها
- در رمزنگاری انتها-به-انتها سناریوی ۴ به طور گسترده به کار می‌رود (مرکز توزیع کلید)

مرکز توزیع کلید
key distribution center (KDC)

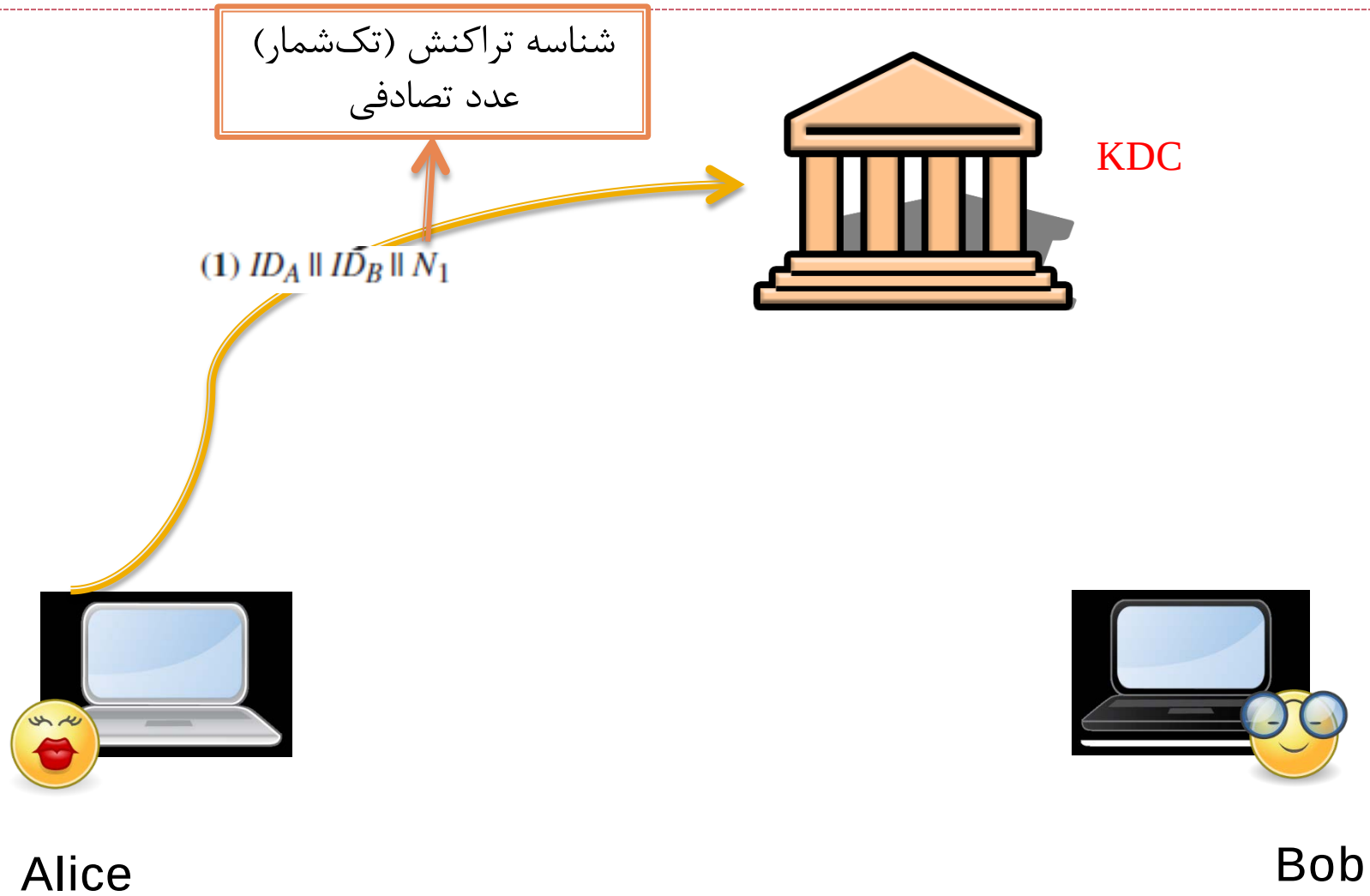
- استفاده از سلسله مراتب کلید (Key Hierarchy)



ارتباط میان دو انتها توسط یک کلید موقت صورت می‌گیرد ← **کلید نشست**
برای هر ارتباط اختصاص یافته و سپس دور ریخته می‌شود
از مرکز توزیع کلید درخواست می‌شود

کلید نشست به صورت رمزگذاری شده با استفاده از یک کلید مخفی میان کاربر انتهایی و مرکز توزیع کلید ارسال می‌شود ← **کلید اصلی یا شاه کلید**
N کلید ← ارسال فیزیکی

یک سناریوی توزیع کلید (KDC)



یک سناریوی توزیع کلید (KDC)

شناسه تراکنش (تک‌شمار)
عدد تصادفی

تنها A می‌تواند بخواند
حتما توسط KDC ارسال شده
درخواست پیش از دریافت توسط
KDC تغییر نیافته
تکرار درخواست قبلی نیست

(1) $ID_A \| ID_B \| N_1$

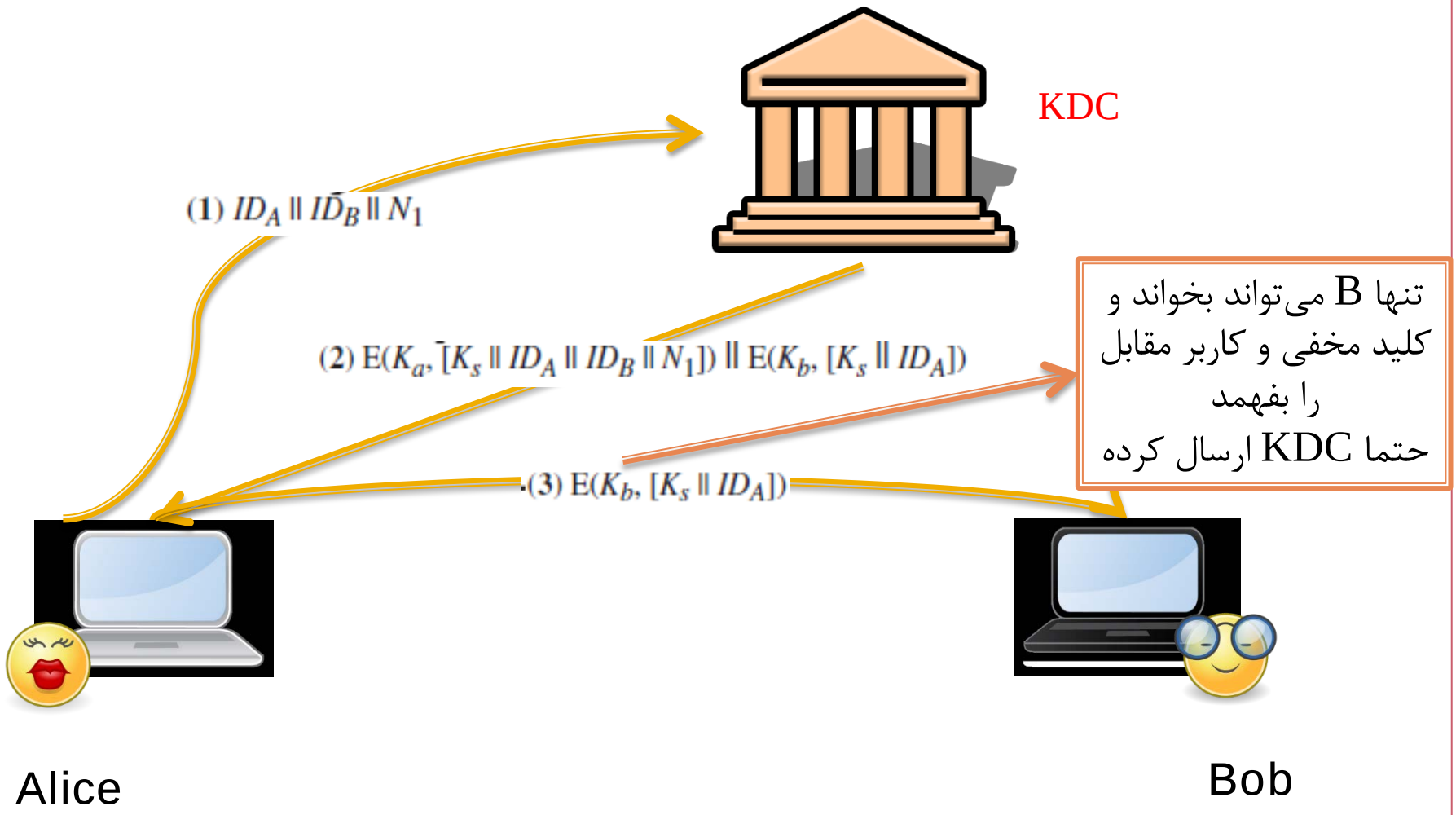
(2) $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s \| ID_A])$

کلید اصلی A

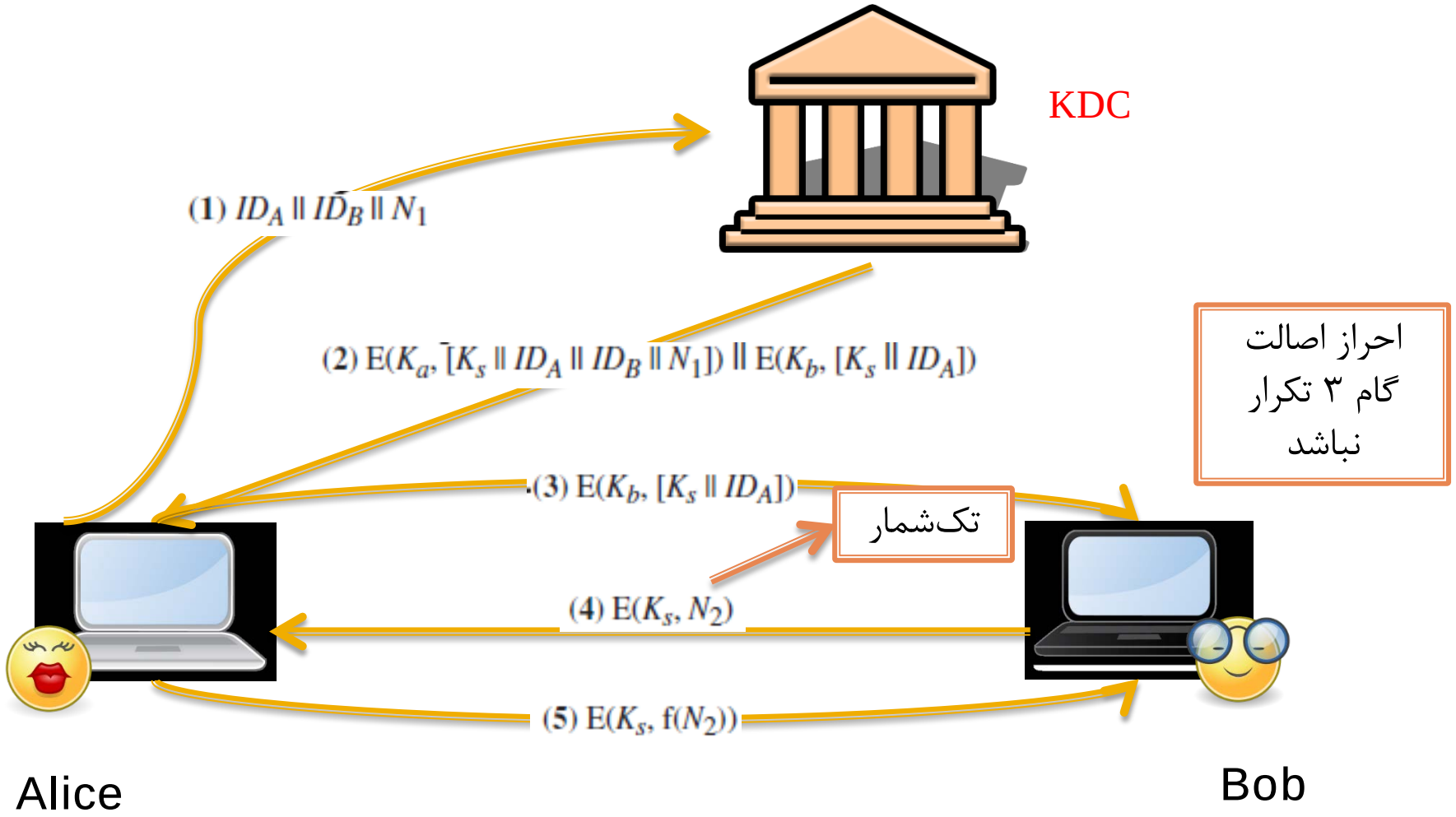
Alice

Bob

یک سناریوی توزیع کلید (KDC)



یک سناریوی توزیع کلید (KDC)



احراز اصالت گام ۳ تکرار نباشد

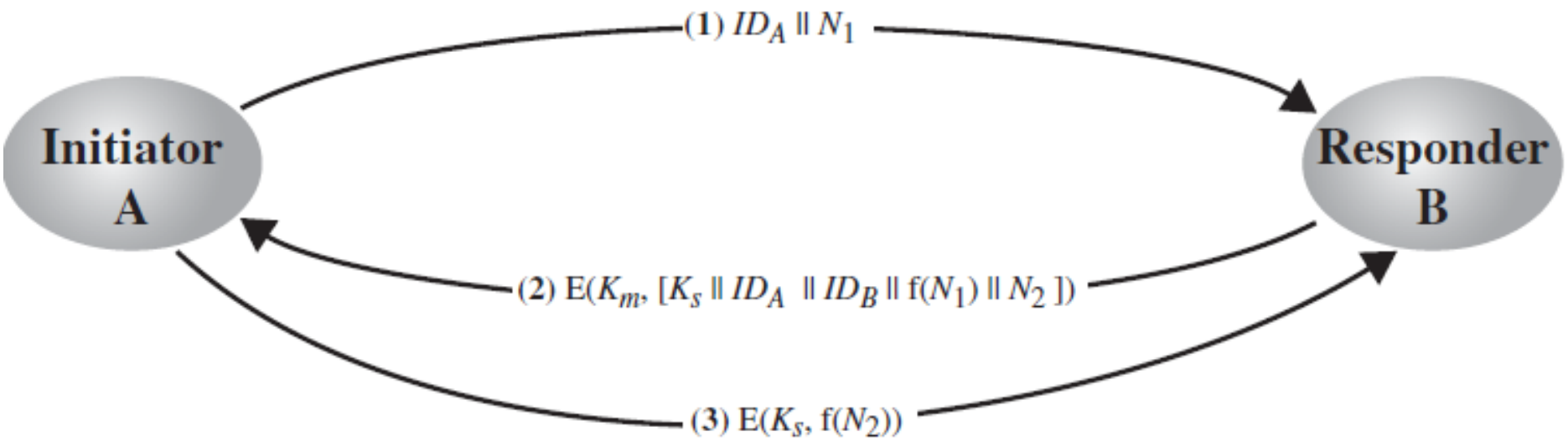
طول عمر کلید نشست

مصالحه‌ای میان کارآیی و امنیت

- طول عمر کمتر ← امنیت بیشتر
  - مهاجم به تعداد کمتری متن رمز شده دسترسی دارد
  - در صورت لو رفتن، خسارت کمی به سیستم وارد می‌شود
- توزیع کلید تاخیر و سربار ارسال و محاسباتی زیادی برای شبکه به همراه دارد
- پروتکل‌های اتصال‌گرا (connection-oriented)
  - یک کلید برای هر اتصال در صورت طولانی نبودن
- پروتکل‌های بدون اتصال (connectionless)
  - تغییر کلید به طور متناوب پس از گذشت زمان مشخص و یا تعداد مشخصی تراکنش

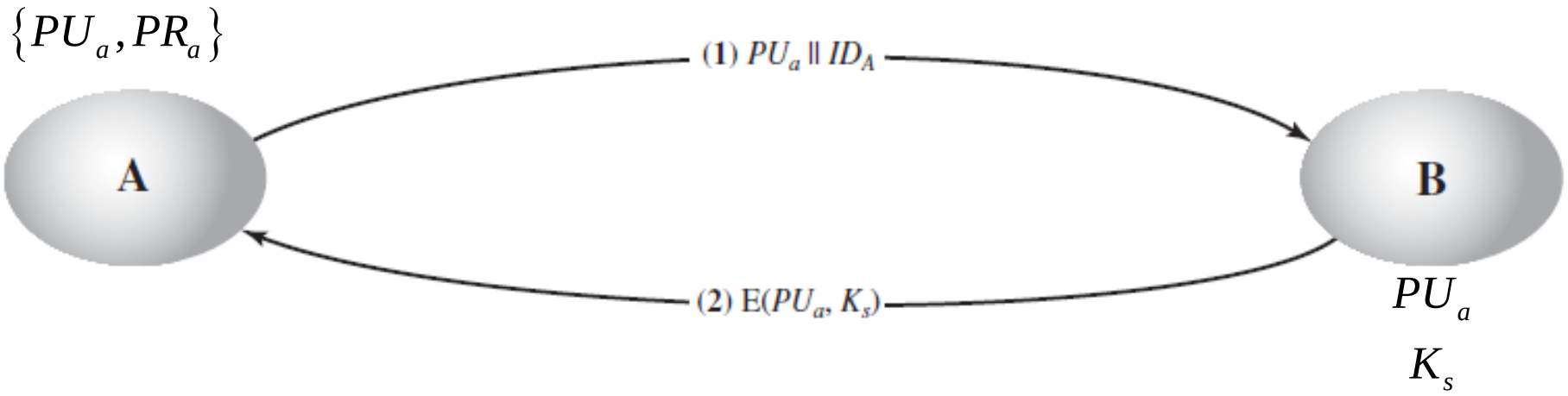
توزیع کلید تمرکززدا (Decentralized)

- مشکل استفاده از KDC: اعتماد به آن و محافظت از آن
  - در شبکه‌های کوچک امکان توزیع کلید بدون مرکز نیز وجود دارد ← نیاز به $N(N-1)/2$ کلید **اصلی** داریم ← هر کاربر باید $N-1$ کلید **اصلی** را محافظت کند



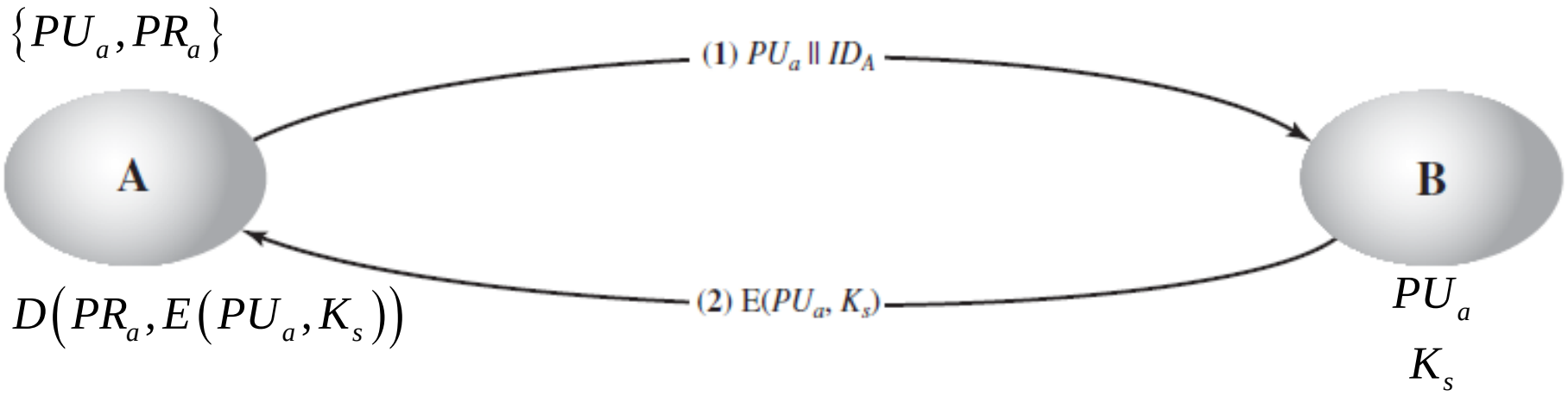
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی

- رمزنگاری کلید همگانی برای ارسال داده‌هایی با طول کم کاربرد دارد
  - رمزگذاری کلید مخفی (رمز متقارن)
- **یک طرح ساده توزیع کلید مخفی (Merkle 79)**



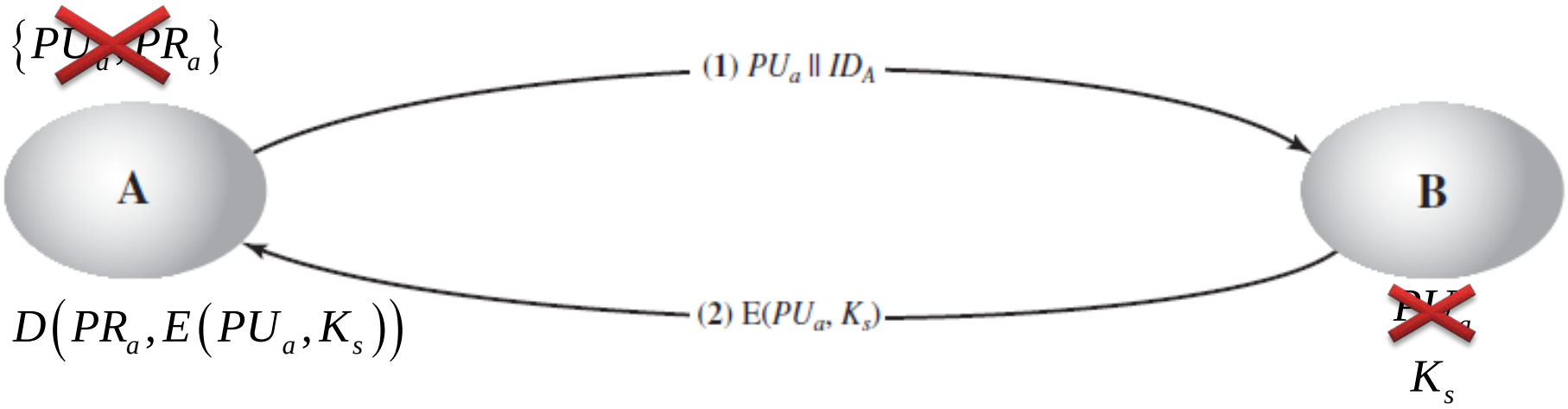
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی

- رمزنگاری کلید همگانی برای ارسال داده‌هایی با طول کم کاربرد دارد
  - رمزگذاری کلید مخفی (رمز متقارن)
- **یک طرح ساده توزیع کلید مخفی (Merkle 79)**



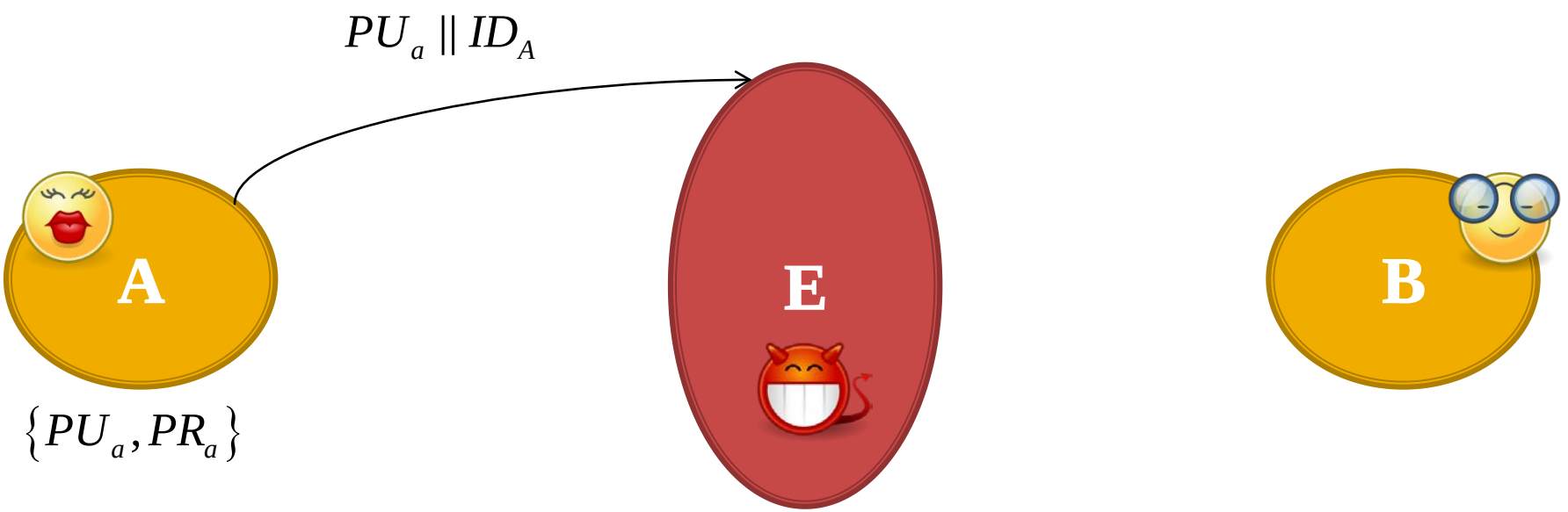
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی

- رمزنگاری کلید همگانی برای ارسال داده‌هایی با طول کم کاربرد دارد
  - رمزگذاری کلید مخفی (رمز متقارن)
- **یک طرح ساده توزیع کلید مخفی (Merkle 79)**
  - هیچ کلیدی پیش از ارتباط لازم نیست و پس از ارتباط نیز باقی نمی‌ماند
  - در برابر شنود (حمله غیر فعال) امن است
  - **در برابر حمله فعال امن نیست ← حمله فرد در میانه**



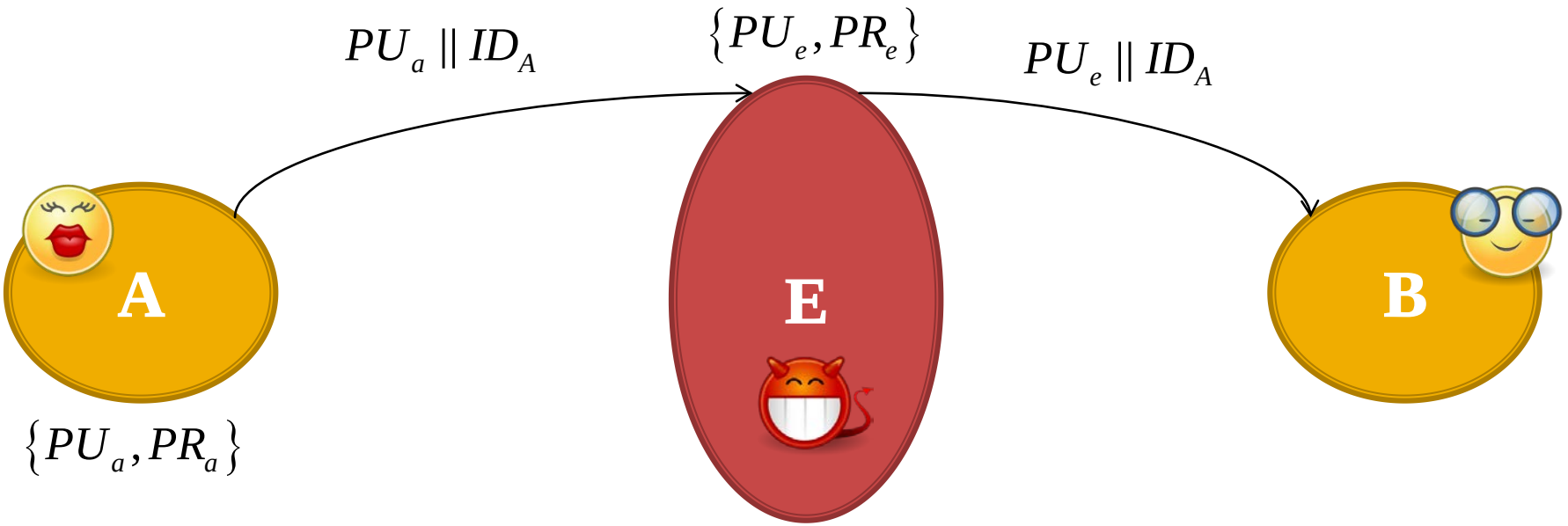
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی

- حمله فرد در میانه



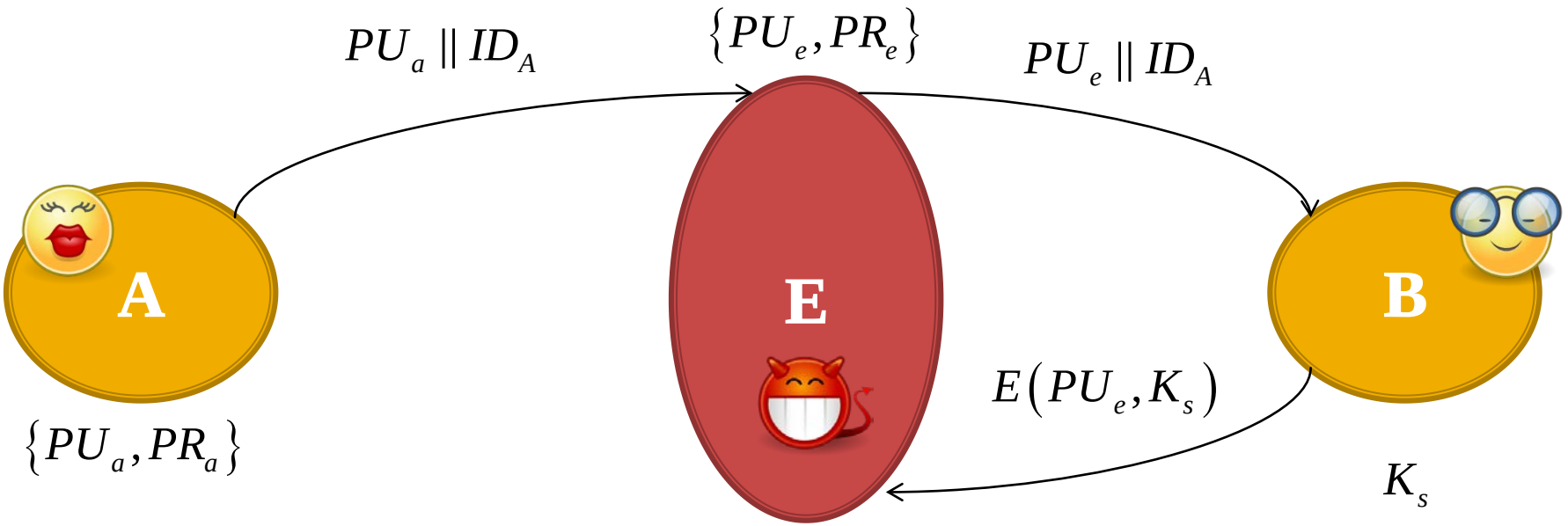
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی

- حمله فرد در میانه



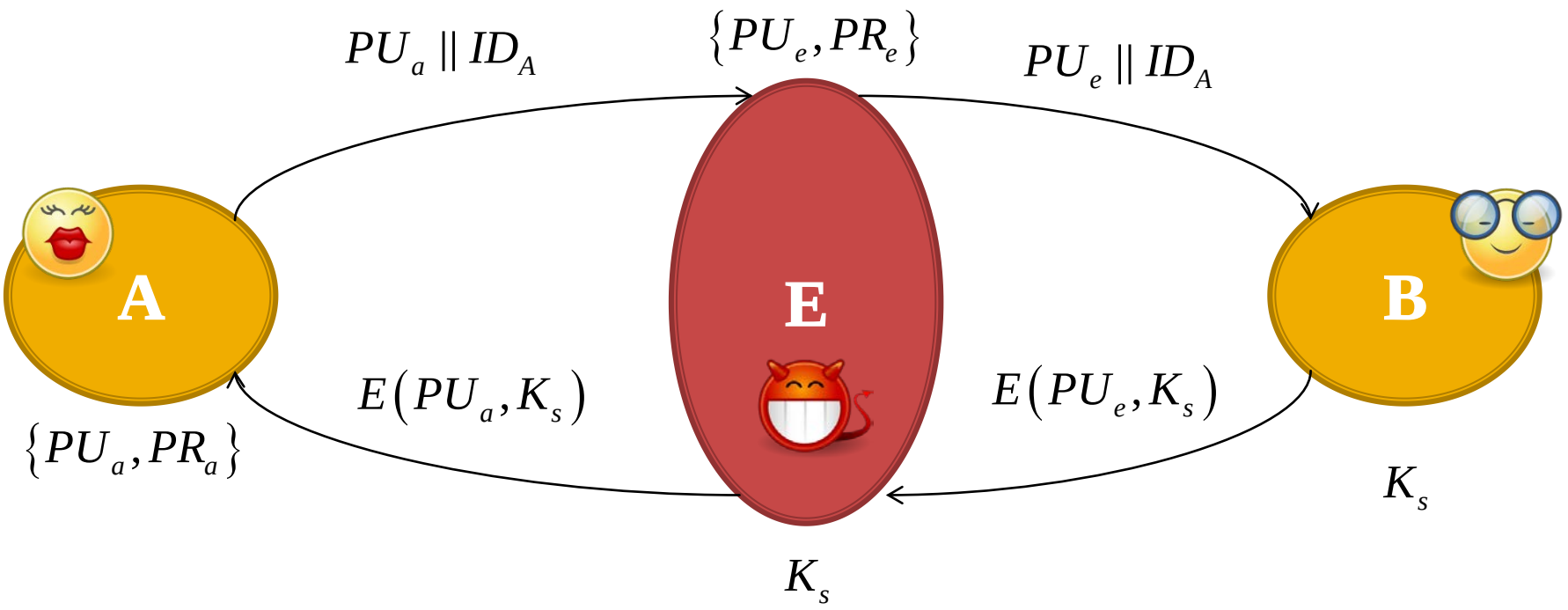
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی

- حمله فرد در میانه



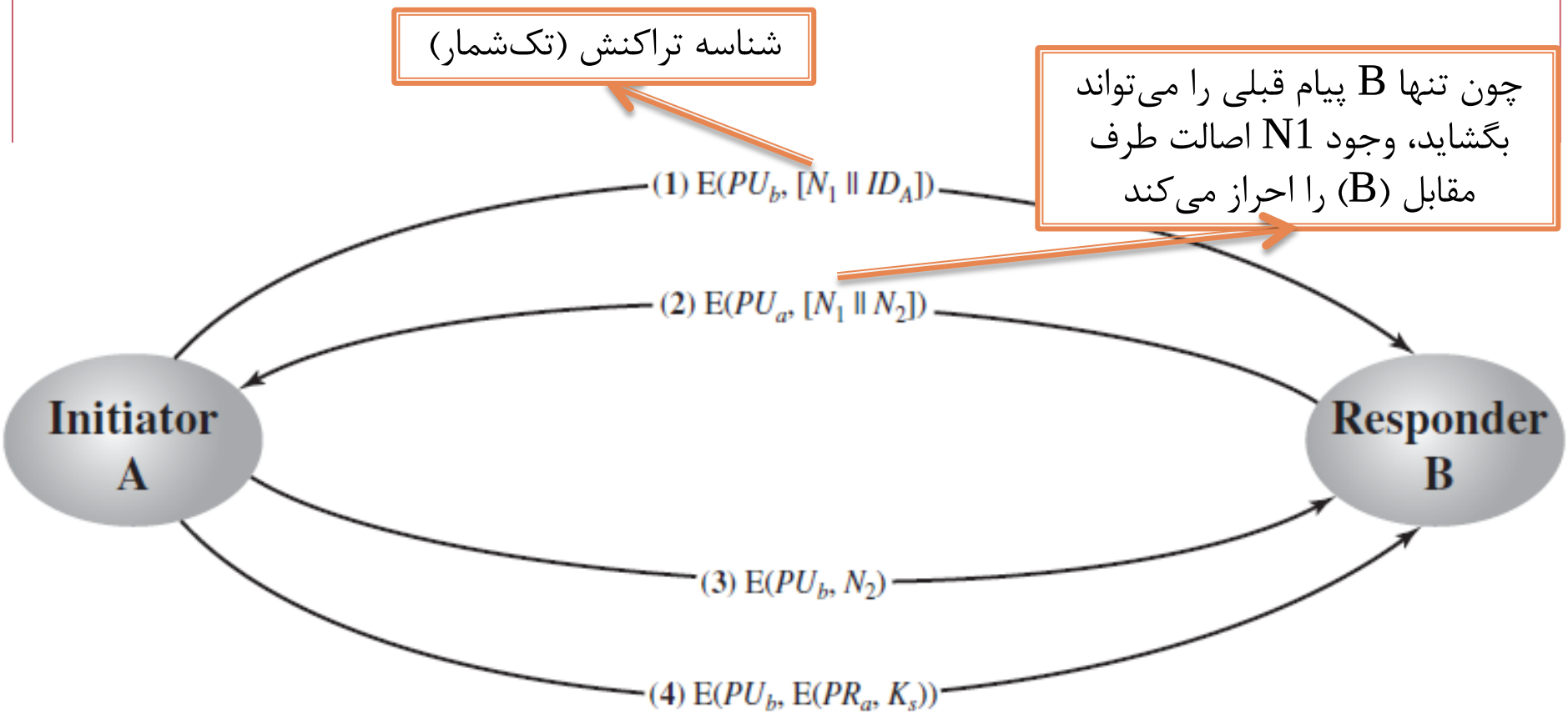
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی

- حمله فرد در میانه
  - پس از آشکار کردن کلید مخفی، دشمن تنها شنود می‌کند



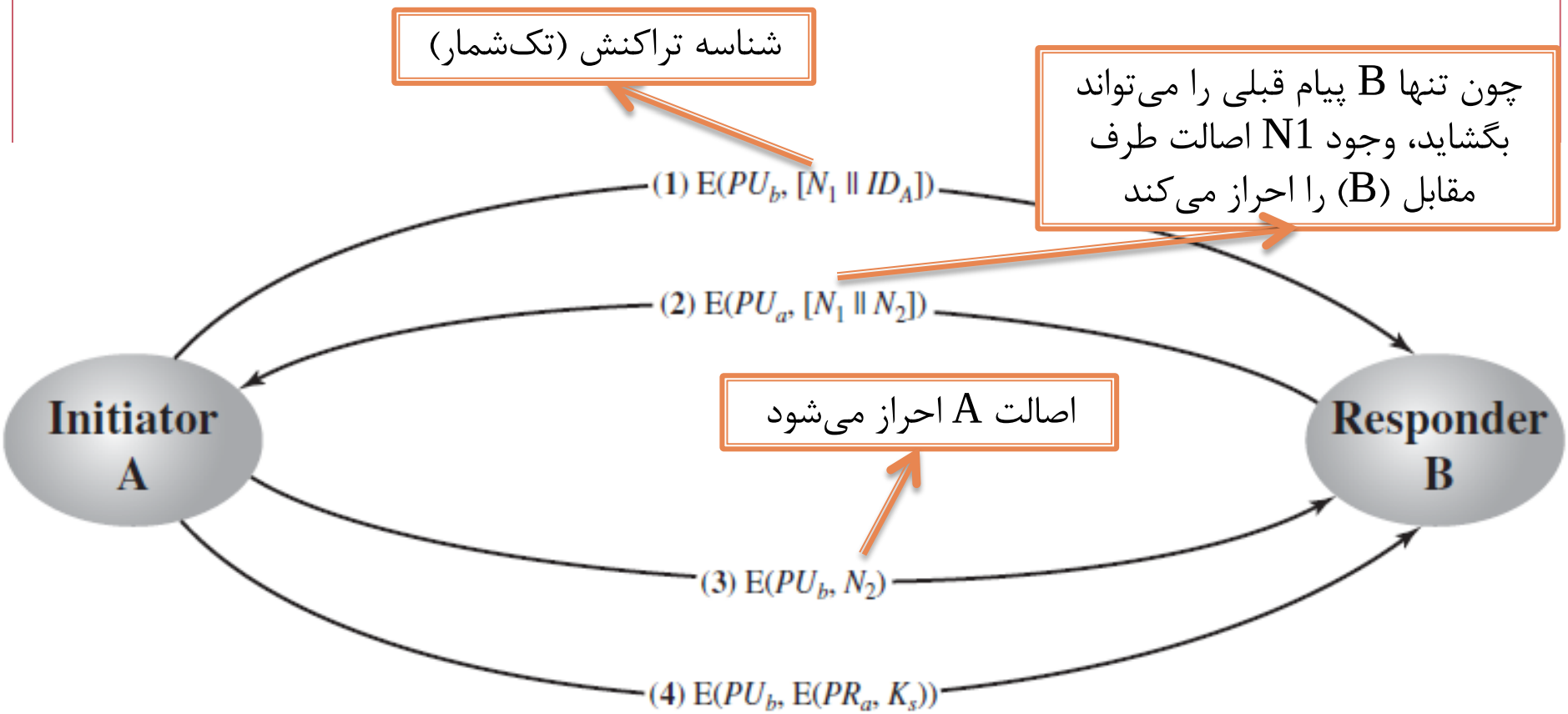
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی
همراه با محرمانگی و احراز اصالت

- مقابله با حملات فعال و غیر فعال
- ابتدا کلیدهای همگانی (PU_a, PU_b) به یک روش امن (در ادامه) توزیع شده‌اند



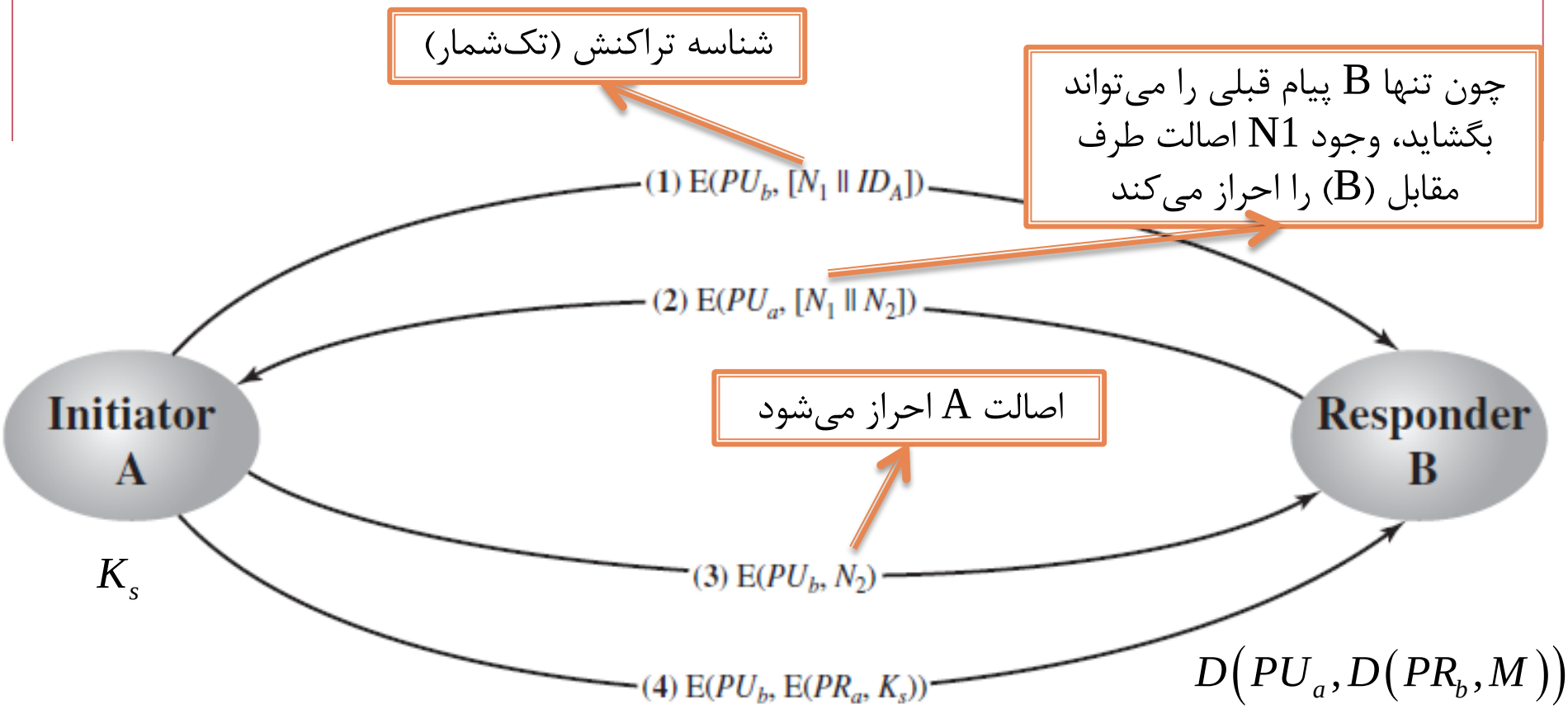
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی
همراه با محرمانگی و احراز اصالت

- مقابله با حملات فعال و غیر فعال
- ابتدا کلیدهای همگانی (PU_a, PU_b) به یک روش امن (در ادامه) توزیع شده‌اند



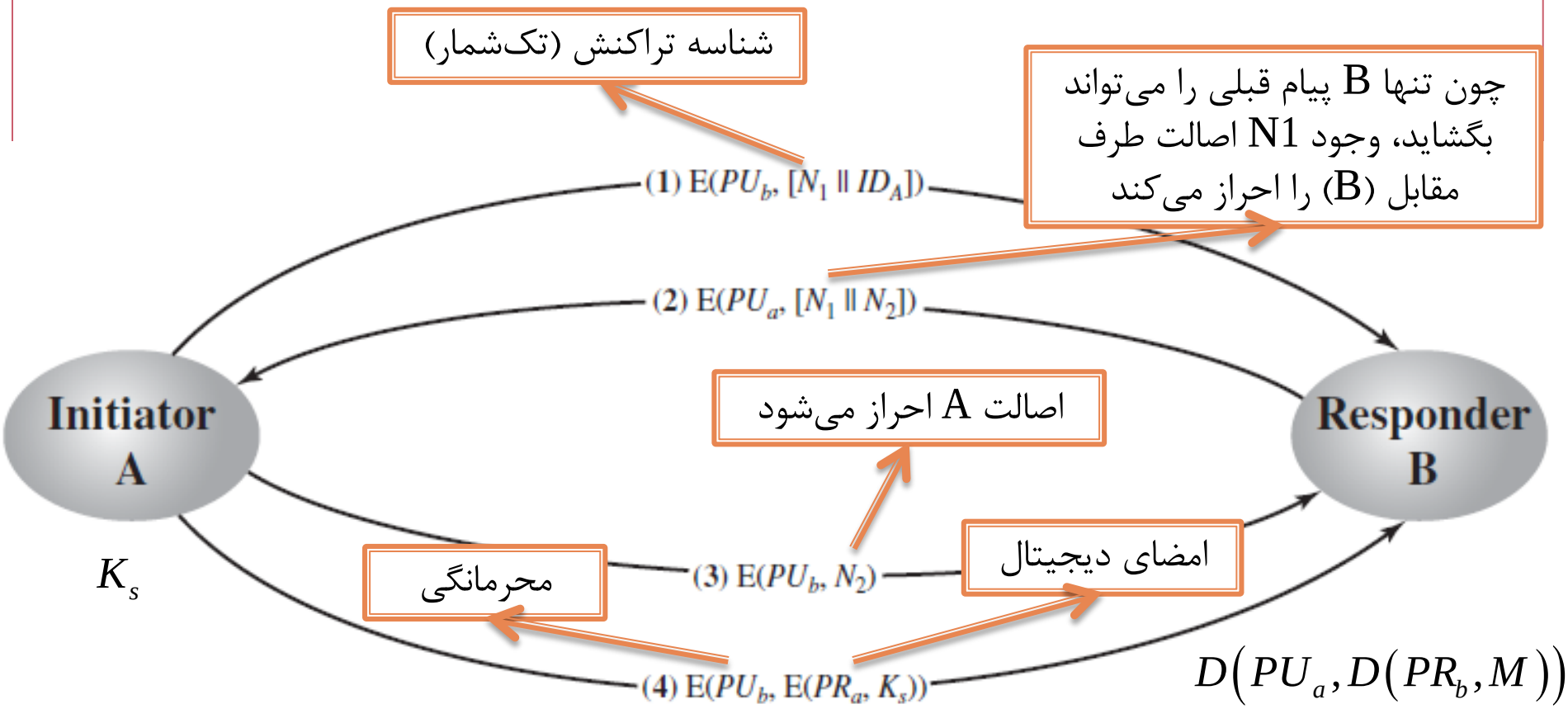
توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی
همراه با محرمانگی و احراز اصالت

- مقابله با حملات فعال و غیر فعال
- ابتدا کلیدهای همگانی (PU_a, PU_b) به یک روش امن (در ادامه) توزیع شده‌اند



توزیع کلید مخفی با استفاده از رمزنگاری کلید همگانی
همراه با محرمانگی و احراز اصالت

- مقابله با حملات فعال و غیر فعال
- ابتدا کلیدهای همگانی (PU_a, PU_b) به یک روش امن (در ادامه) توزیع شده‌اند



روش ترکیبی توزیع کلید مخفی

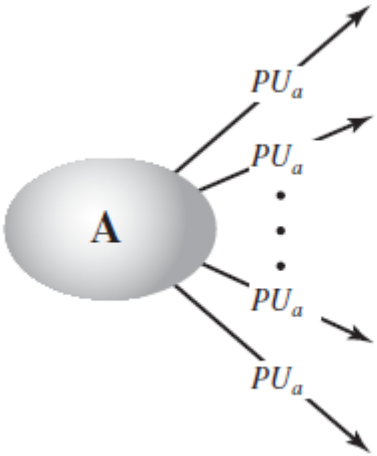
- تعداد کلیدهای نشست مورد نیاز بسیار زیاد است
- با توجه به سربار روش توزیع کلید با استفاده از رمزنگاری کلید همگانی، استفاده از این روش در توزیع کلیدهای نشست، کارآیی سیستم را به شدت کاهش می‌دهد
- روش ترکیبی: استفاده شده در IBM
- توزیع کلیدهای اصلی (میان کاربرها و KDC) با استفاده از رمزنگاری کلید همگانی
- توزیع کلیدهای نشست با استفاده از رمز متقارن و کلیدهای اصلی

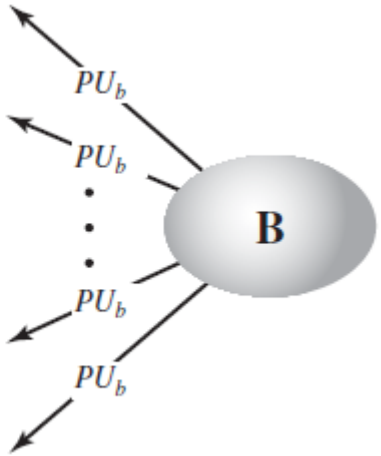
توزیع کلیدهای همگانی

- اعلام همگانی (Public announcement)
- فهرست راهنمای همگانی در دسترس (Publicly available directory)
- مرجع مجازشناس کلید همگانی (Public-key authority)
- گواهی‌نامه کلید همگانی (Public-key certificates)

اعلام همگانی (Public announcement)

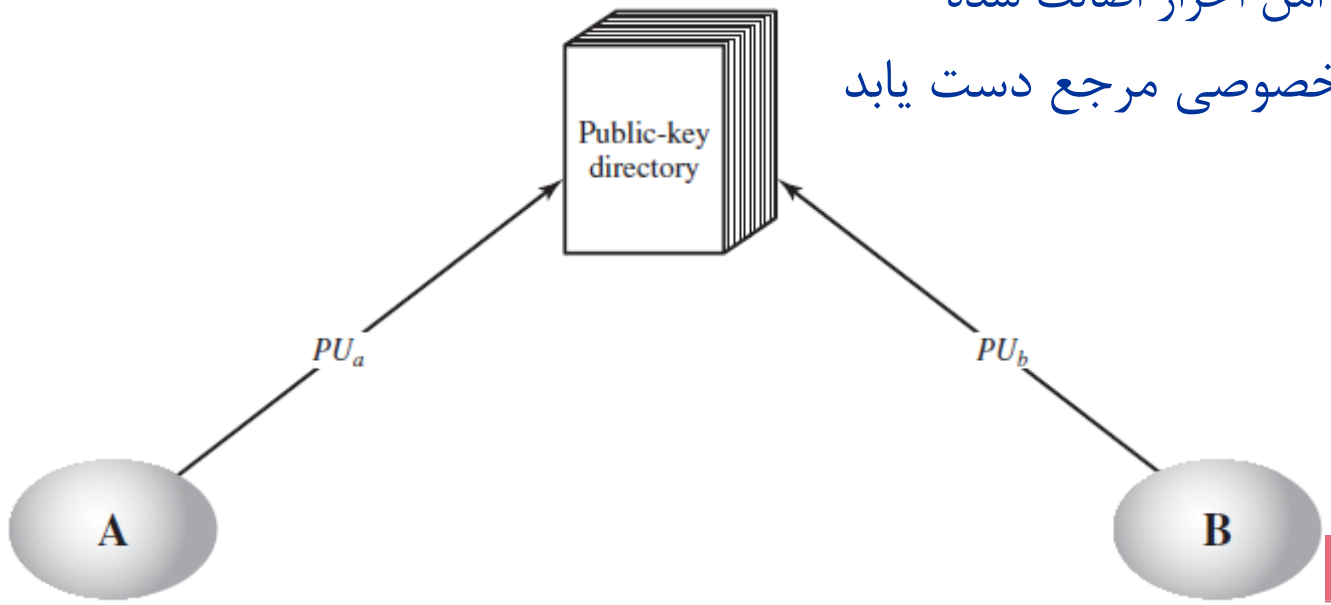
- هدف اولیه طراحی رمزنگاری کلید همگانی
- در پروتکل PGP (بر پایه RSA)، بسیاری از کاربرها کلید همگانی خود را به پیام الصاق و به فروم‌های همگانی ارسال می‌کنند
- مشکل اصلی: هر کسی می‌تواند این اعلام همگانی را جعل کند
  - مثلا کاربری ادعا کند که A است (با اعلام یک کلید همگانی جعلی) و همه پیام‌های رمزشده برای A را بخواند و از امضای A نیز برای احراز اصالت استفاده کند



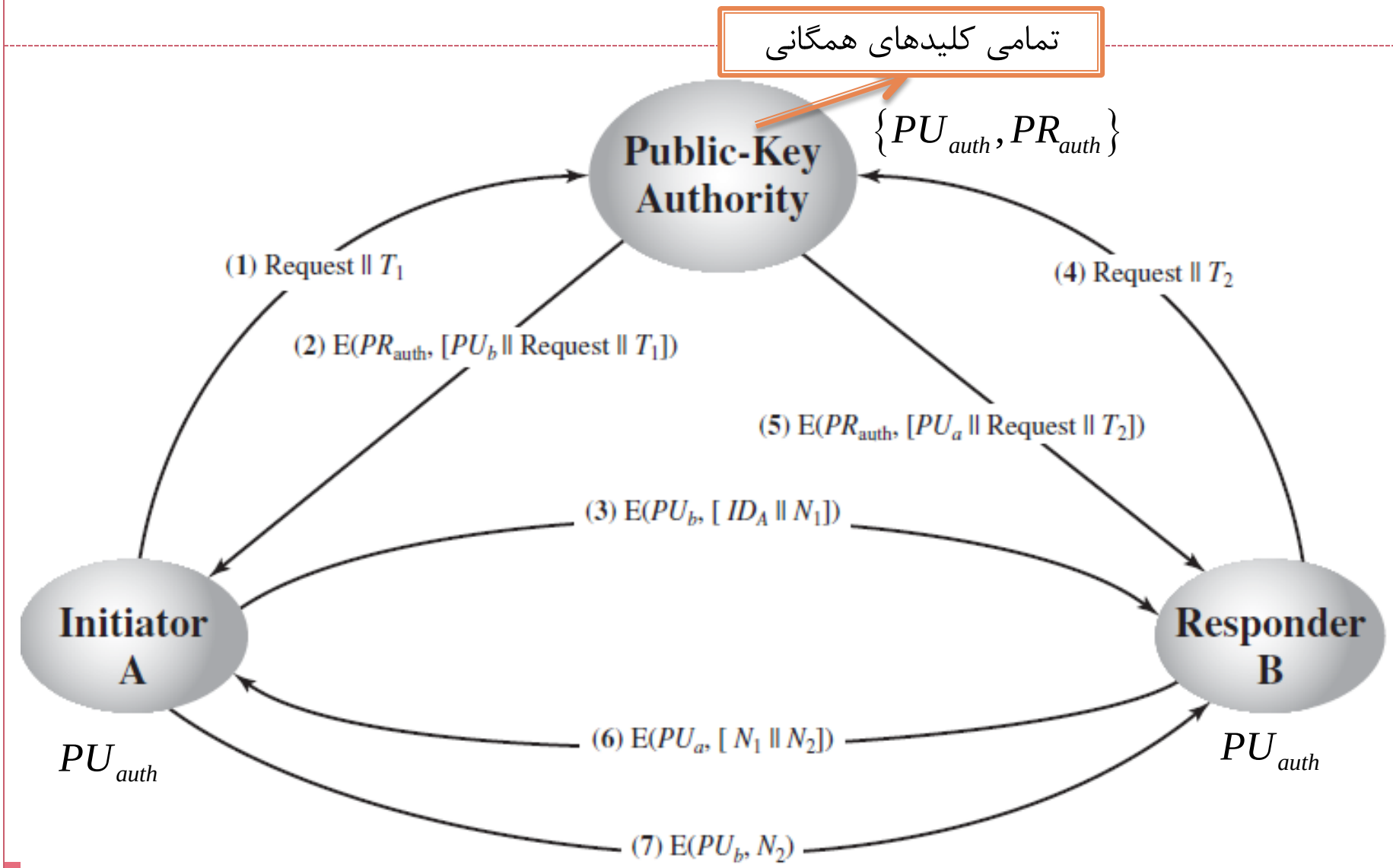


فهرست راهنمای همگانی در دسترس
Publicly available directory

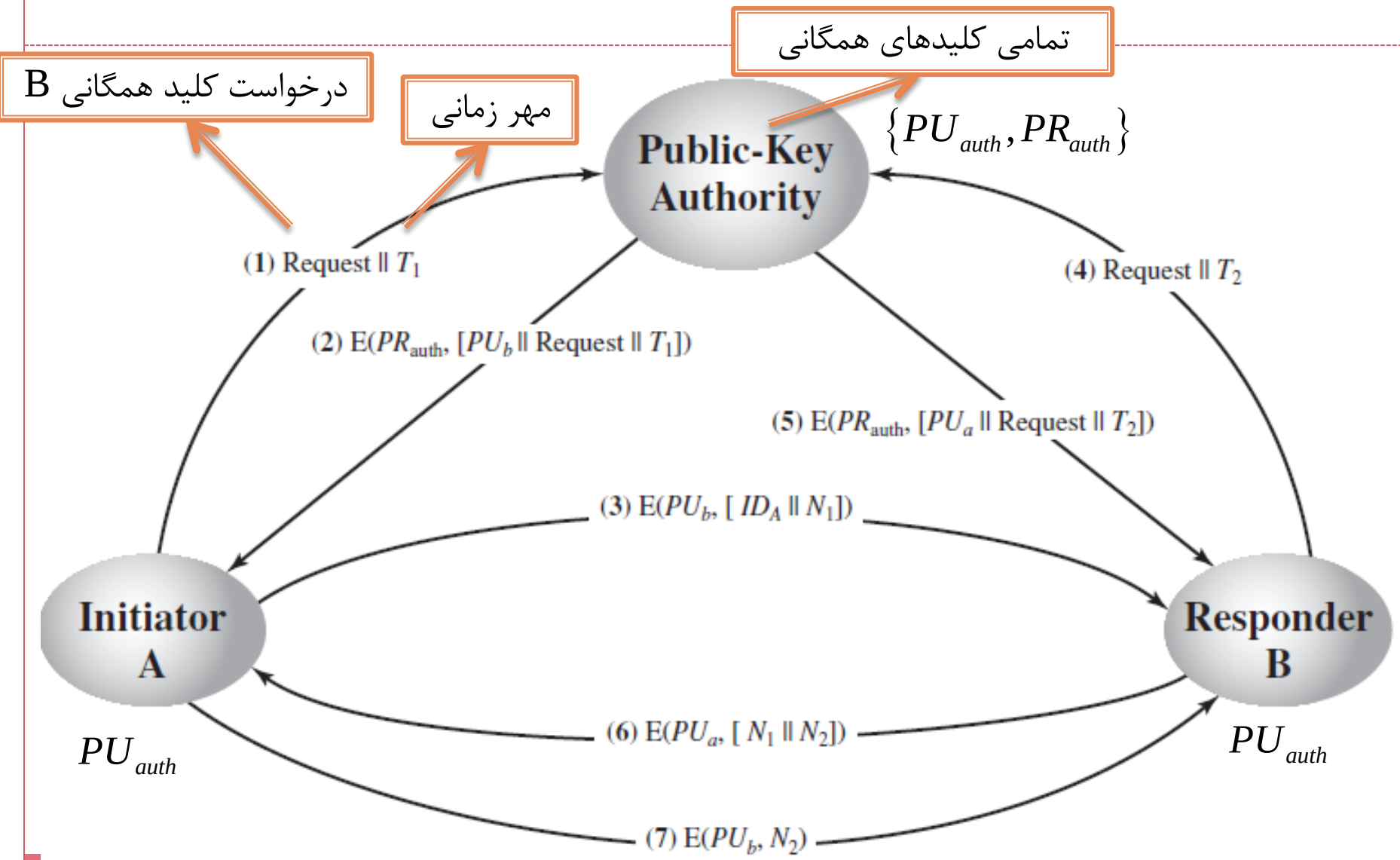
- **امنیت بیشتر از اعلام همگانی**
- کلیدهای همگانی در یک فهرست راهنمای همگانی که نگهداری آن بر عهده یک سازمان معتمد است
- فهرستی از {نام+کلیدهمگانی} برای هر کاربر
  - ثبت نام به صورت فردی یا با یک ارتباط امن احراز اصالت شده
  - دسترسی با یک ارتباط امن احراز اصالت شده
- مشکل: مهاجم به کلید خصوصی مرجع دست یابد



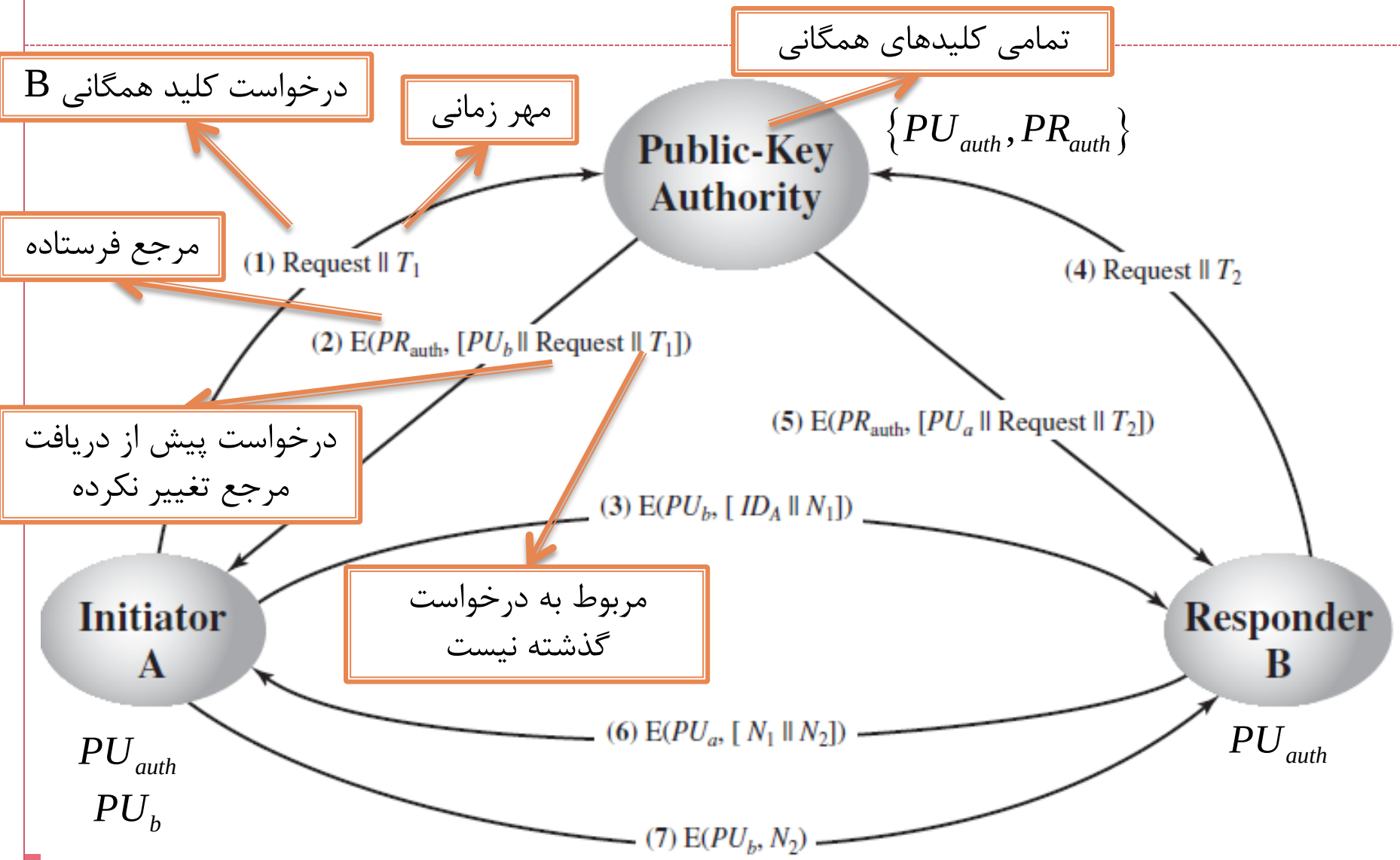
مرجع مجازشناس کلید همگانی (Public-key authority)



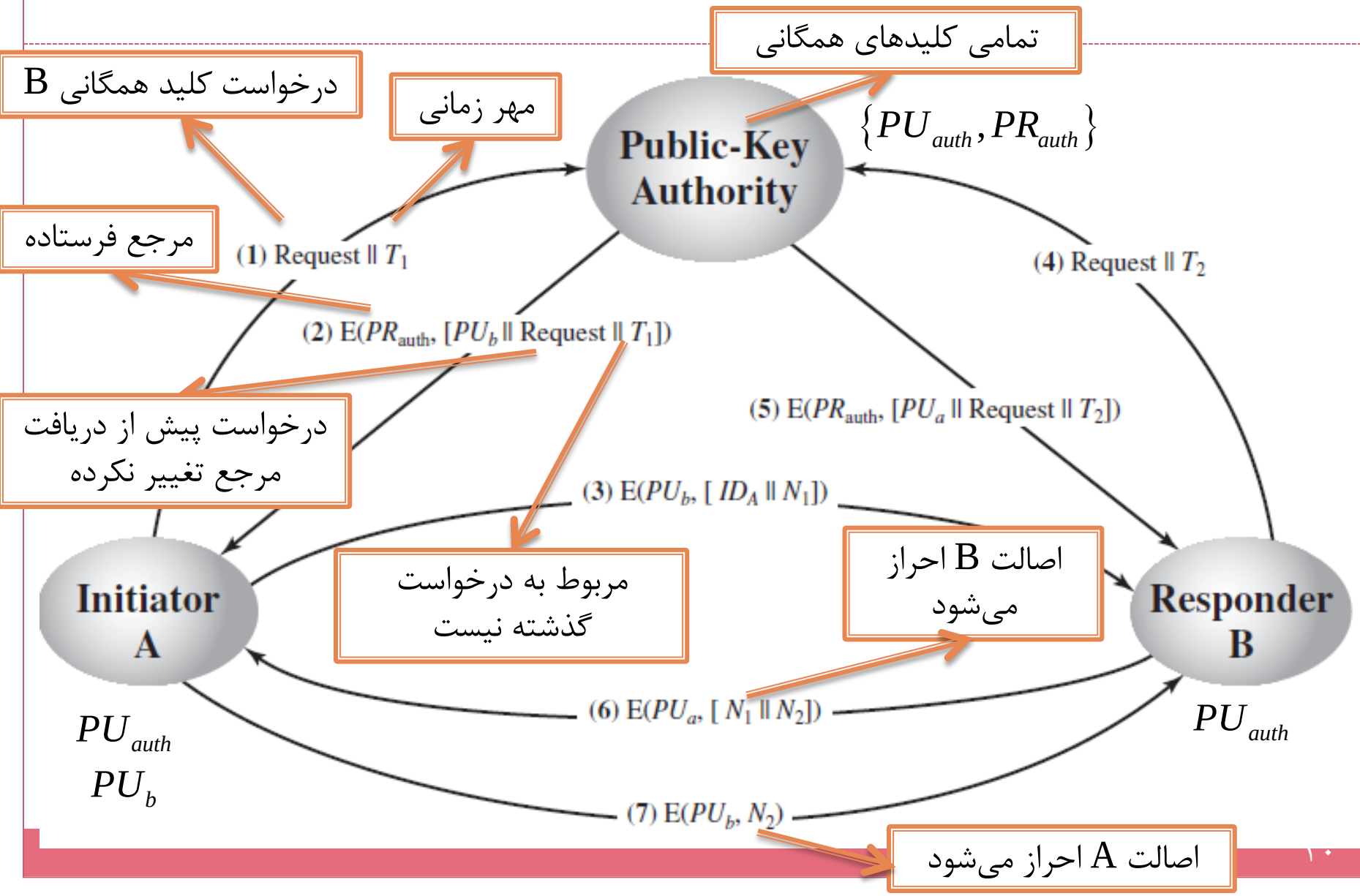
مرجع مجازشناس کلید همگانی (Public-key authority)



مرجع مجازشناس کلید همگانی (Public-key authority)



مرجع مجازشناس کلید همگانی (Public-key authority)

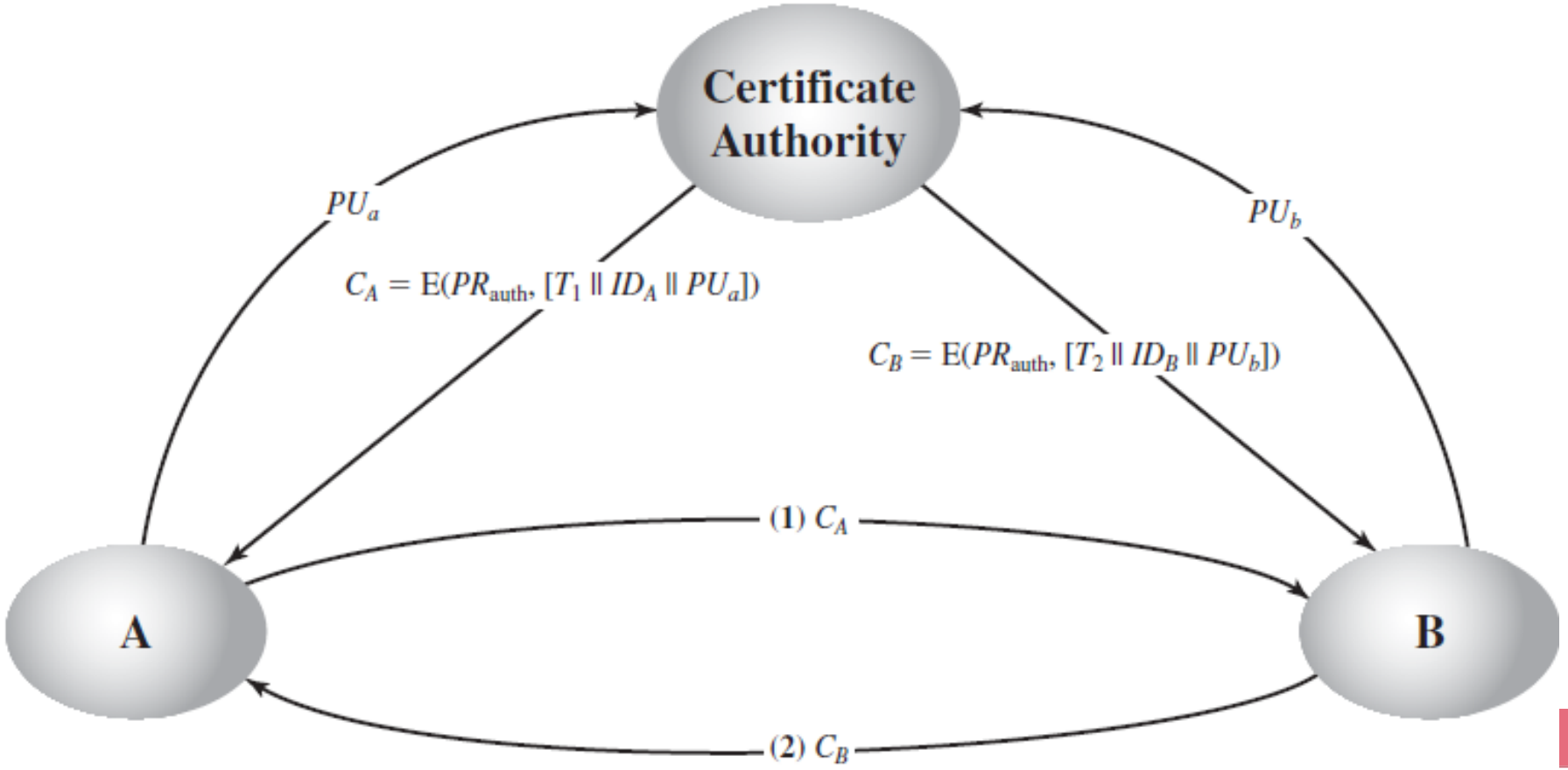


گواهی‌نامه کلید همگانی (Public-key certificates)

- در روش قبلی: مرجع مجازشناس گلوگاه سیستم است
  - هر دو کاربر پیش از ارتباط به آن مراجعه می‌کنند
- راه حل: استفاده از گواهی‌نامه کلید همگانی
- **مشخصات گواهی‌نامه**
  - هر کاربری بتواند آن را خوانده و نام و کلید همگانی صاحب کلید همگانی را بفهمد
  - هر کاربری بتواند صدور آن توسط مرجع مجازشناس را تایید کند
  - تنها مرجع مجازشناس (Certificate Authority (CA)) بتواند آن را صادر و به‌روزرسانی کند
  - هر کاربری بتواند به روز بودن آن را تایید کند
- برای باطل کردن پیش از پایان اعتبار
  - فهرست گواهی‌های باطل شده (certificate revocation list (CRL))

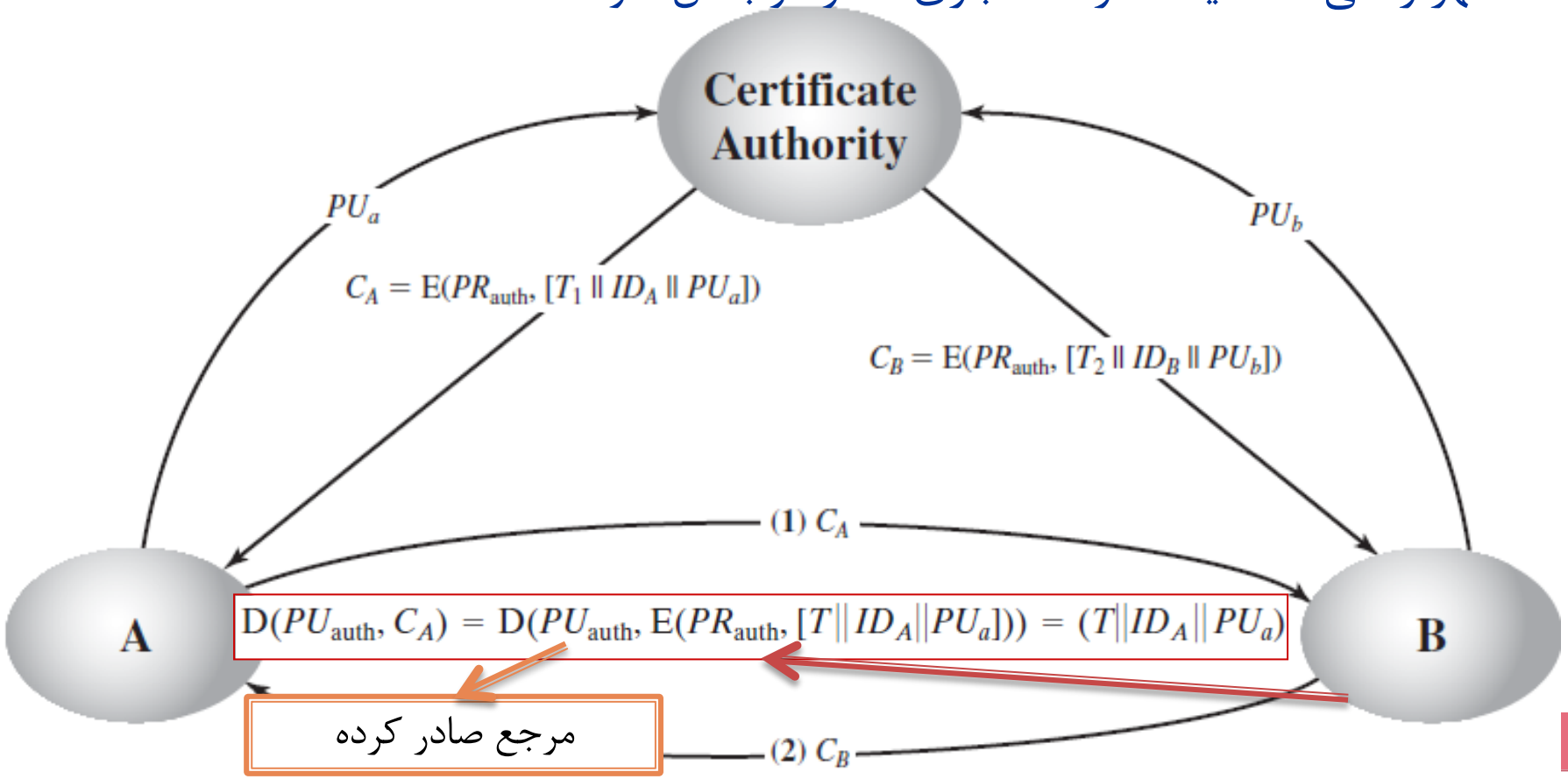
گواهی‌نامه کلید همگانی (Public-key certificates)

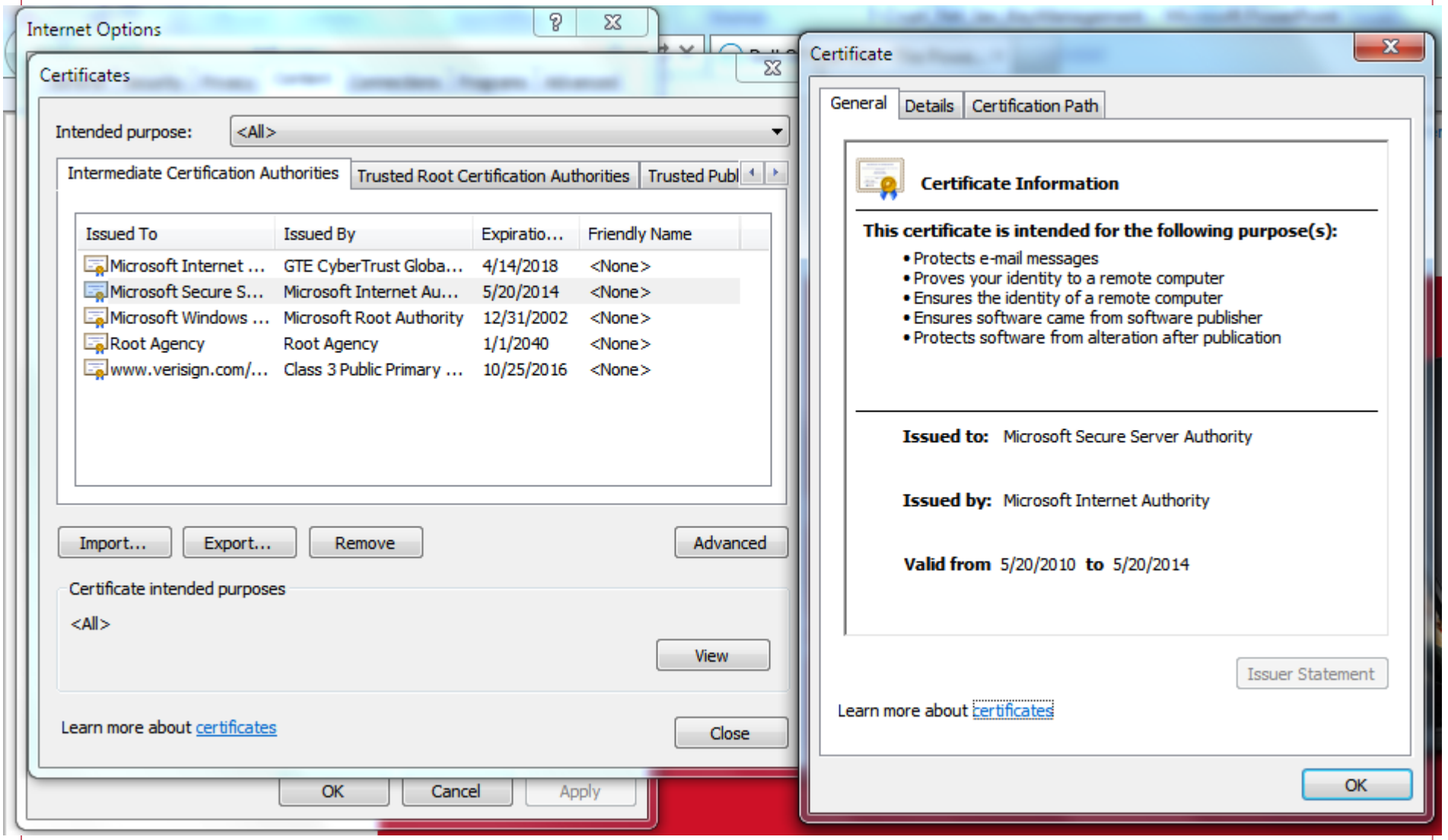
- هر کاربر با ارسال کلید همگانی خود، درخواست گواهی‌نامه می‌کند
  - به صورت فردی یا با یک ارتباط امن احراز اصالت شده

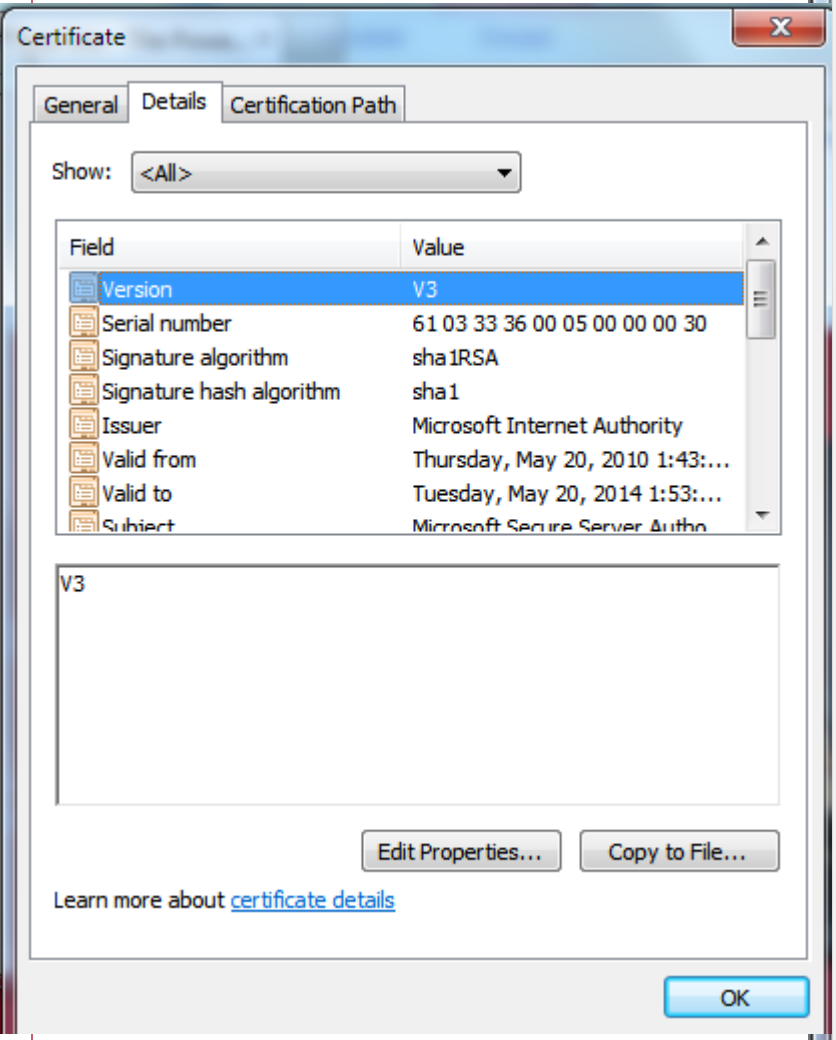


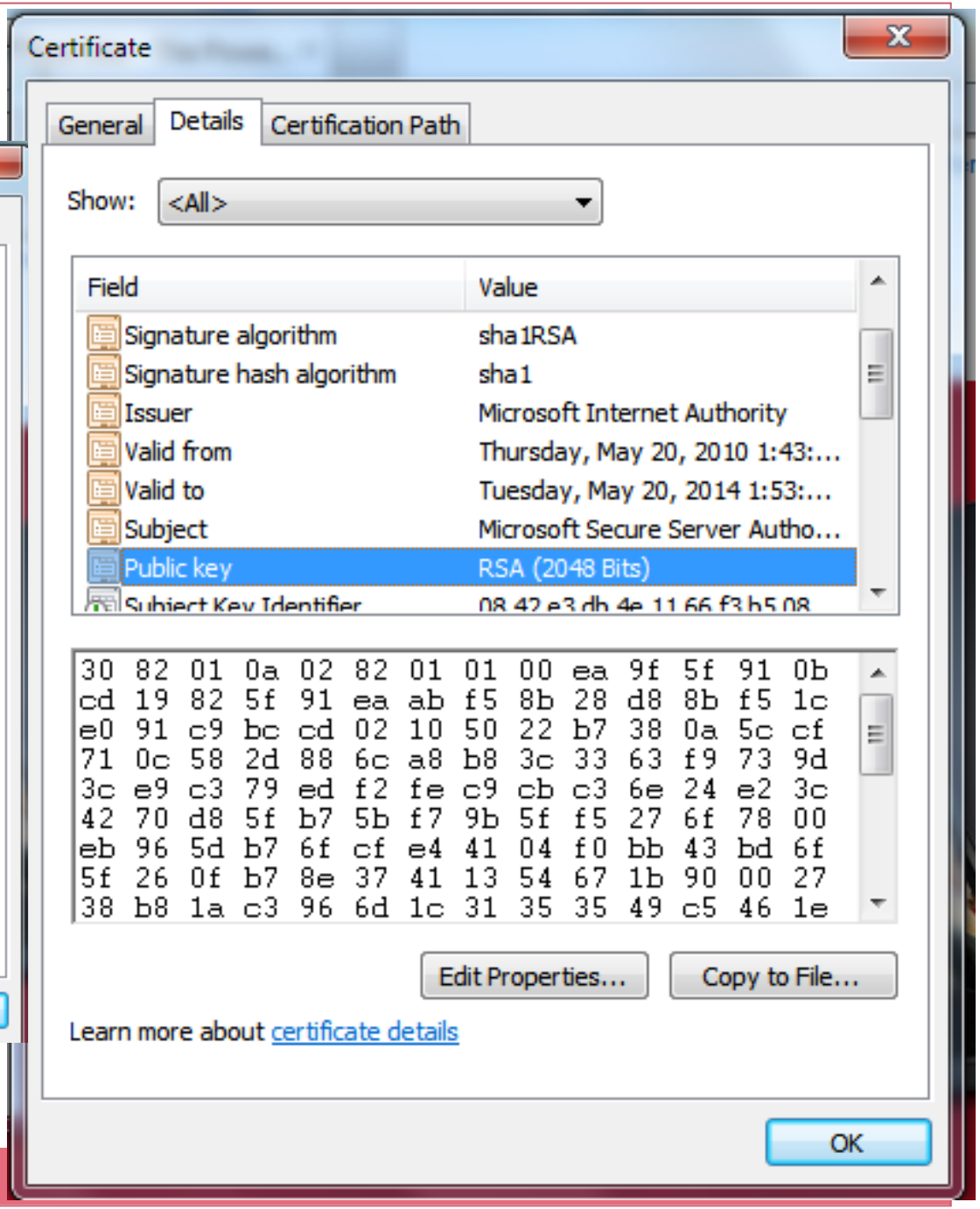
گواهی‌نامه کلید همگانی (Public-key certificates)

- هر کاربر با ارسال کلید همگانی خود، درخواست گواهی‌نامه می‌کند
  - به صورت فردی یا با یک ارتباط امن احراز اصالت شده
- مهر زمانی: مثلا یک کارت اعتباری مفقود و باطل شود




Internet Options
Certificates
Intended purpose:
<All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Issued To
Issued By
Expiratio...
Friendly Name
Microsoft Internet ...
GTE CyberTrust Globa...
4/14/2018
<None>
Microsoft Secure S...
Microsoft Internet Au...
5/20/2014
<None>
Microsoft Windows ...
Microsoft Root Authority
12/31/2002
<None>
Root Agency
Root Agency
1/1/2040
<None>
www.verisign.com/...
Class 3 Public Primary ...
10/25/2016
<None>
Import...
Export...
Remove
Advanced
Certificate intended purposes
<All>
View
Learn more about certificates
Close
OK
Cancel
Apply
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Protects e-mail messages
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• Ensures software came from software publisher
• Protects software from alteration after publication
Issued to: Microsoft Secure Server Authority
Issued by: Microsoft Internet Authority
Valid from 5/20/2010 to 5/20/2014
Issuer Statement
Learn more about certificates
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
61 03 33 36 00 05 00 00 00 30
Signature algorithm
sha1RSA
Signature hash algorithm
sha1
Issuer
Microsoft Internet Authority
Valid from
Thursday, May 20, 2010 1:43:...
Valid to
Tuesday, May 20, 2014 1:53:...
Subject
Microsoft Secure Server Autho
V3
Edit Properties...
Copy to File...
Learn more about certificate details
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Signature algorithm
sha1RSA
Signature hash algorithm
sha1
Issuer
Microsoft Internet Authority
Valid from
Thursday, May 20, 2010 1:43:...
Valid to
Tuesday, May 20, 2014 1:53:...
Subject
Microsoft Secure Server Autho...
Public key
RSA (2048 Bits)
30 82 01 0a 02 82 01 01 00 ea 9f 5f 91 0b
cd 19 82 5f 91 ea ab f5 8b 28 d8 8b f5 1c
e0 91 c9 bc cd 02 10 50 22 b7 38 0a 5c cf
71 0c 58 2d 88 6c a8 b8 3c 33 63 f9 73 9d
3c e9 c3 79 ed f2 fe c9 cb c3 6e 24 e2 3c
42 70 d8 5f b7 5b f7 9b 5f f5 27 6f 78 00
eb 96 5d b7 6f cf e4 41 04 f0 bb 43 bd 6f
5f 26 0f b7 8e 37 41 13 54 67 1b 90 00 27
38 b8 1a c3 96 6d 1c 31 35 35 49 c5 46 1e
Edit Properties...
Copy to File...
Learn more about certificate details
OK

گواهی‌نامه X.509

- استاندارد ITU-T: بخشی از X.500
- استفاده در S/MIME، IP Security و SSL/TLS
- استفاده از رمزنگاری کلیدهمگانی و امضای دیجیتال
  - گواهی‌نامه محدودیتی بر الگوریتم مورد استفاده نمی‌گذارد ولی RSA را توصیه می‌کند
  - استفاده از تابع چکیده‌ساز دلخواه برای امضای دیجیتال

$$CA\ll A\gg = CA\ \{V, SN, AI, CA, UCA, A, UA, Ap, T^A\}$$

$Y\ll X\gg$ = the certificate of user X issued by certification authority Y

$Y\ \{I\}$ = the signing of I by Y. It consists of I with an encrypted hash code appended

V = version of the certificate

SN = serial number of the certificate

AI = identifier of the algorithm used to sign the certificate

CA = name of certificate authority

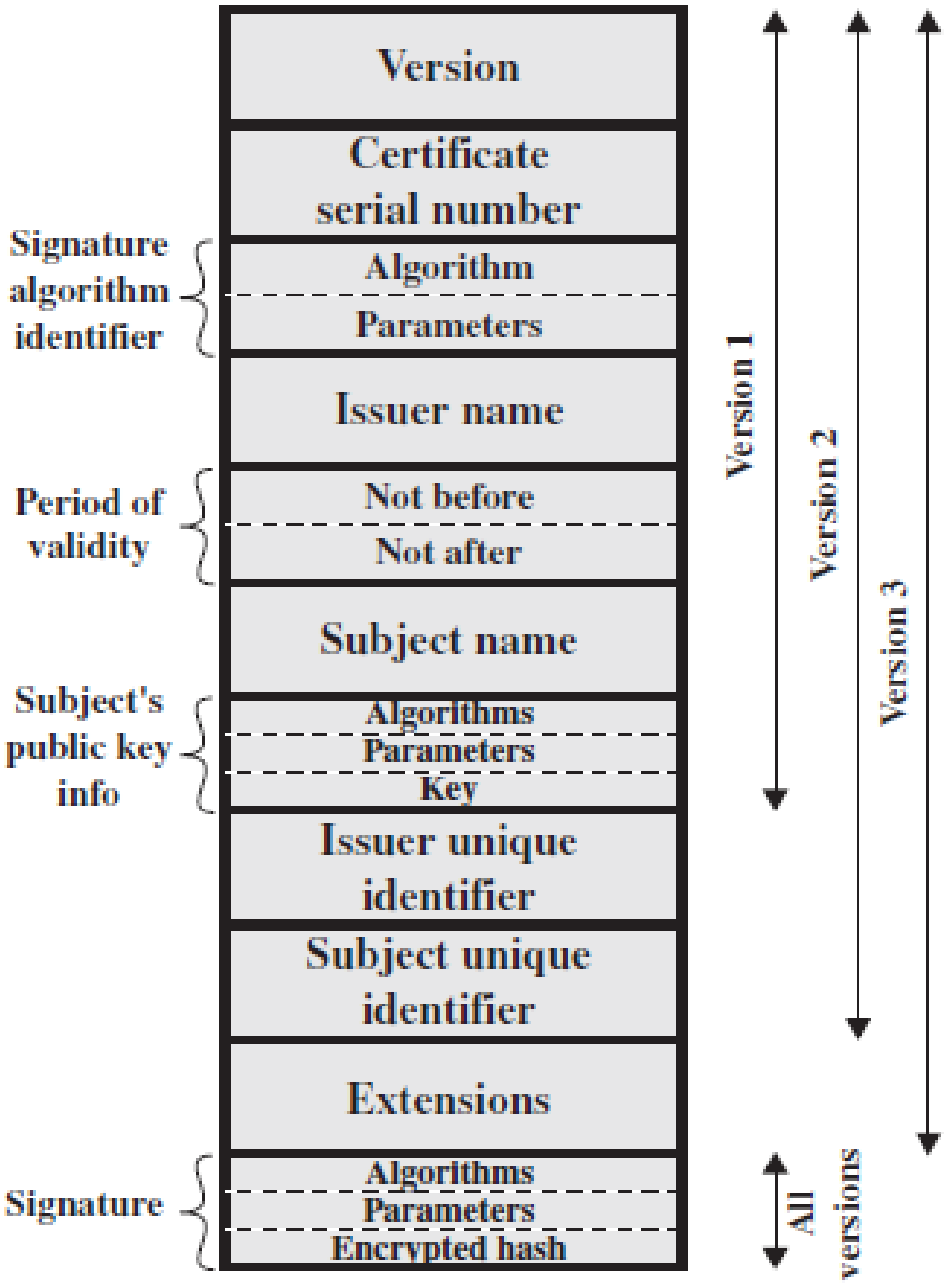
UCA = optional unique identifier of the CA

A = name of user A

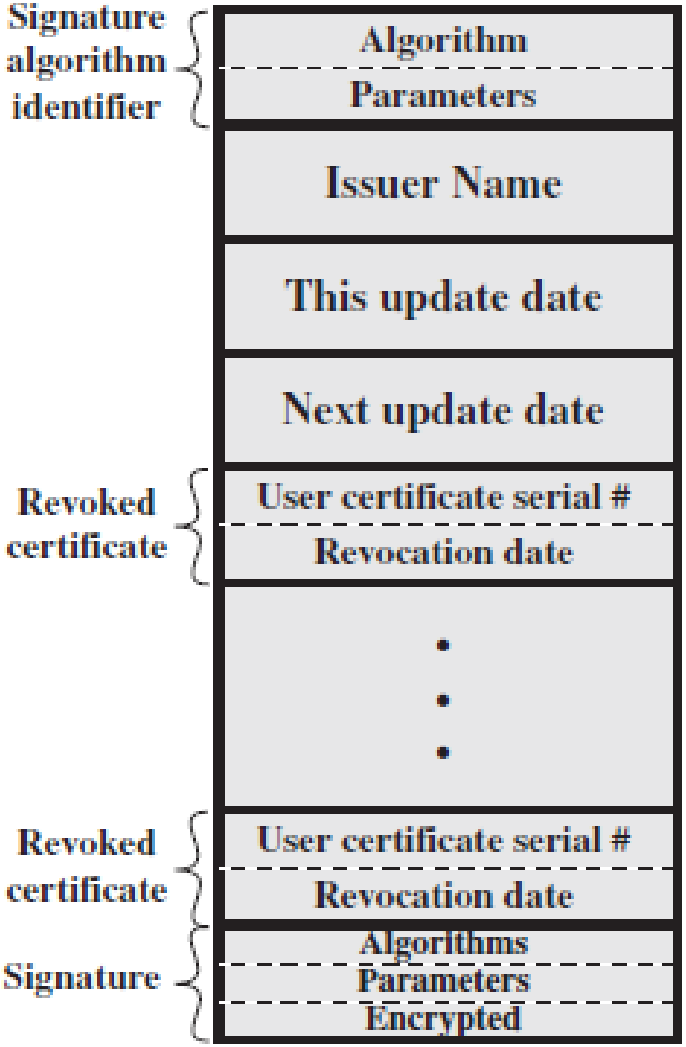
UA = optional unique identifier of the user A

Ap = public key of user A

T^A = period of validity of the certificate



(a) X.509 certificate



(b) Certificate revocation list

زیرساخت کلید همگانی
public-key infrastructure (PKI)

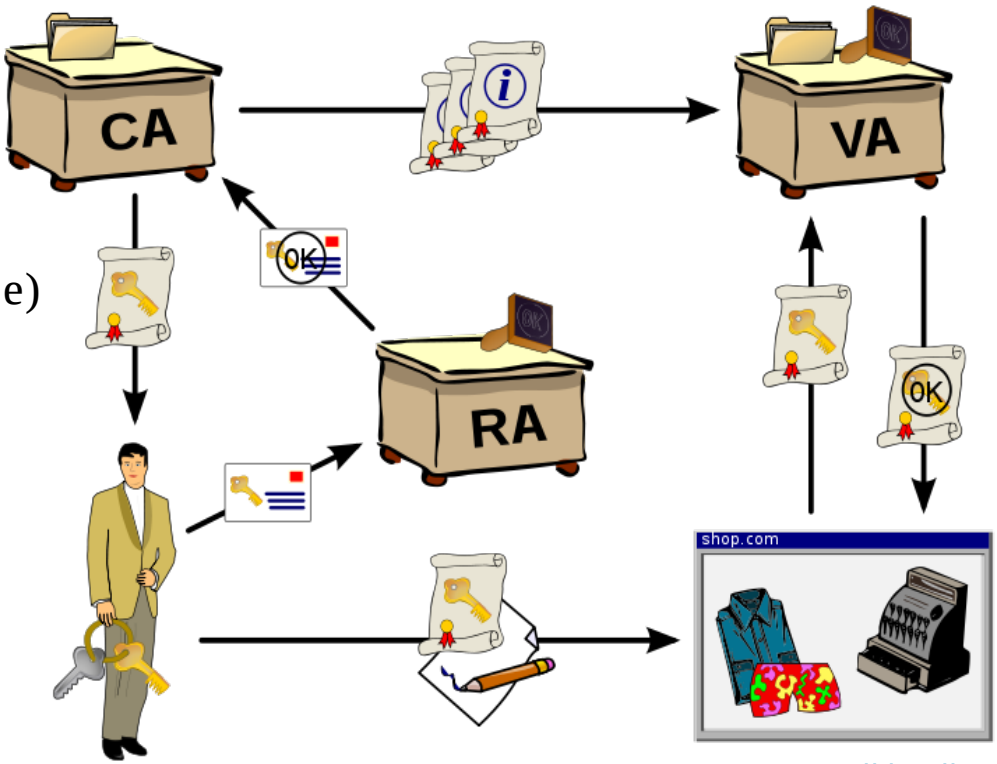
- **تعریف (RFC 2822 (Internet Security Glossary:**

- مجموعه‌ای از سخت‌افزارها، نرم‌افزارها، افراد، سیاست‌ها و رویه‌های مورد نیاز برای صدور، مدیریت، ذخیره‌سازی، توزیع و ابطال گواهی‌نامه‌های دیجیتالی بر اساس رمزنگاری نامتقارن (کلید همگانی)

- PKIX: بر اساس گواهی‌نامه X.509

Public Key Infrastructure (PKI)

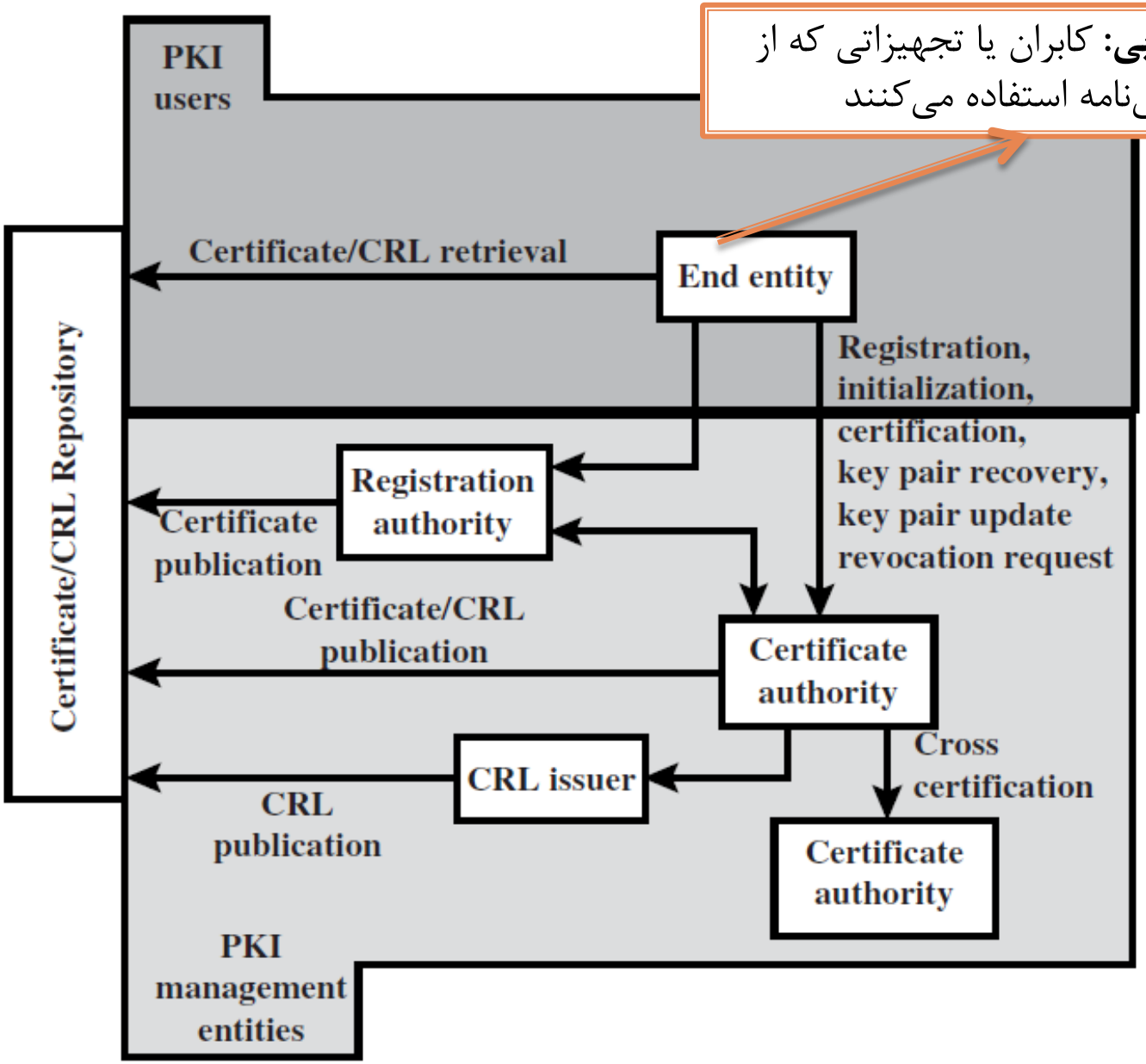
- Certificate Authority (CA)
  - Trusted Third Party
  - Public Key is known
  - CertCA is a signature on:
    - The identity
    - Its public Key
    - Other information (e.g. lifetime)
- Registration Authority (RA):
  - Verifies the identity
- Validation Authority (VA):
  - Validates the public key



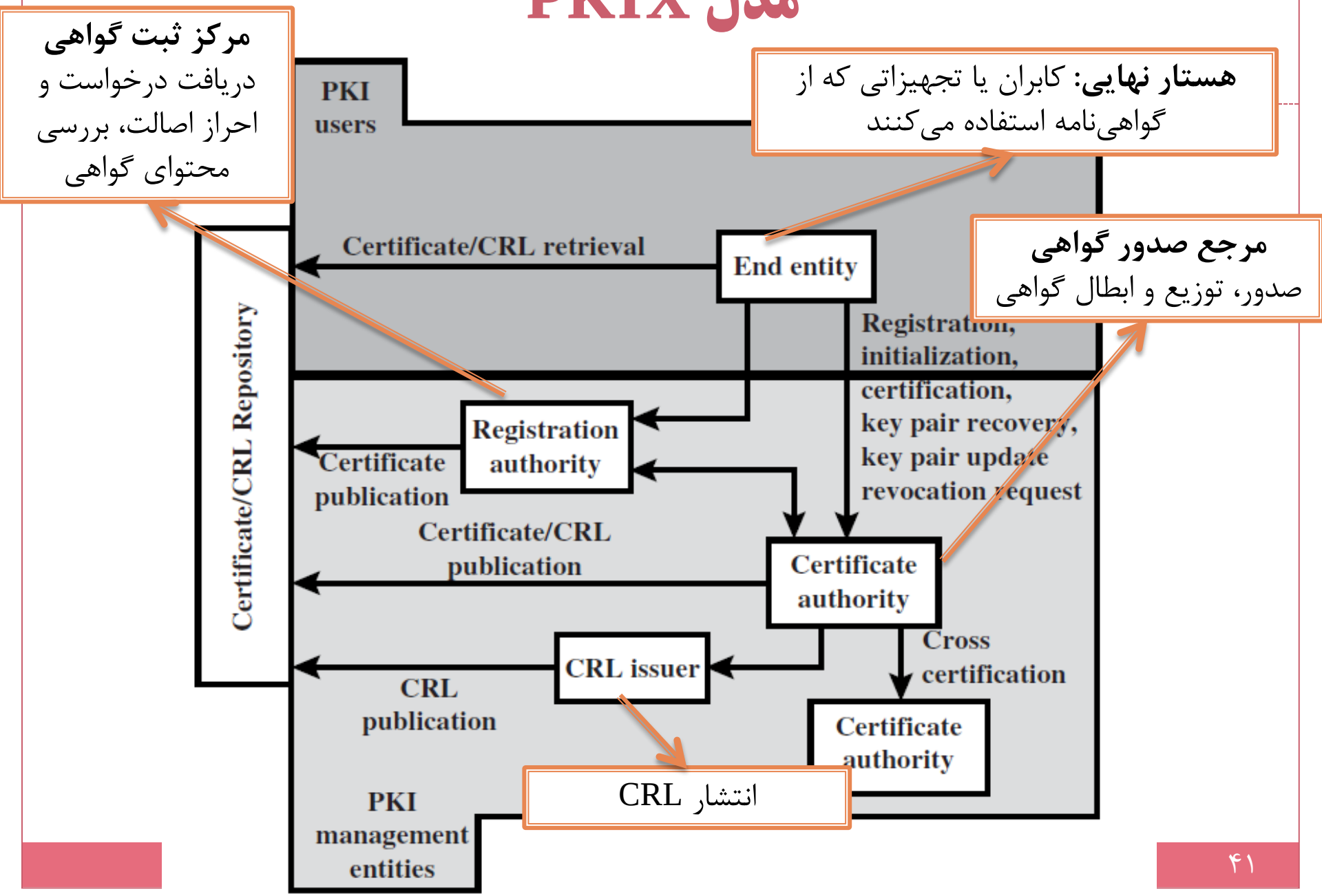
src: wikipedia

مدل PKIX

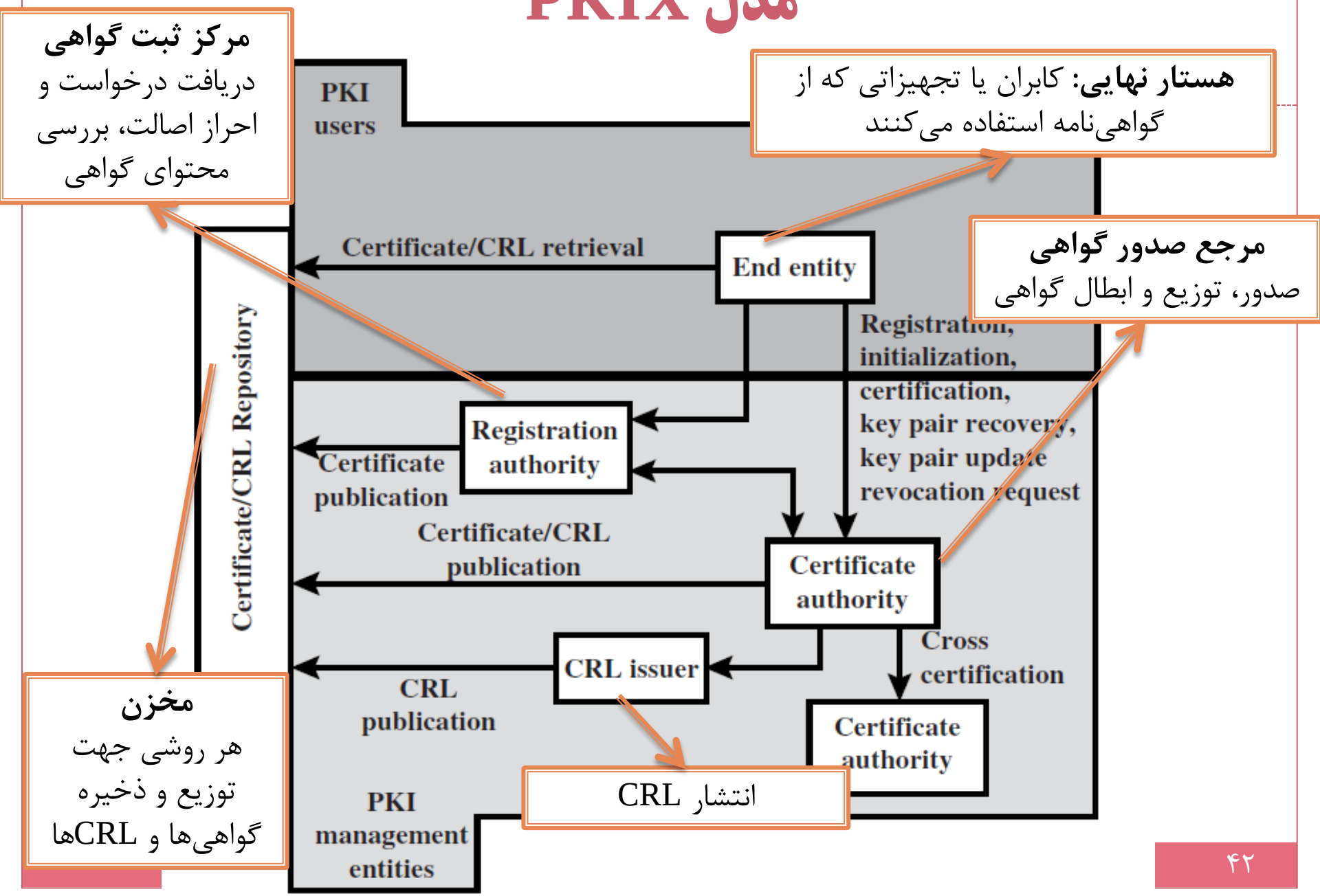
هستار نهایی: کابران یا تجهیزاتی که از گواهی‌نامه استفاده می‌کنند



مدل PKIX


مرکز ثبت گواهی
دریافت درخواست و
احراز اصالت، بررسی
محتوای گواهی
هستار نهایی: کابران یا تجهیزاتی که از
گواهی‌نامه استفاده می‌کنند
مرجع صدور گواهی
صدور، توزیع و ابطال گواهی
PKI
users
Certificate/CRL retrieval
End entity
Registration,
initialization,
certification,
key pair recovery,
key pair update
revocation request
Certificate/CRL Repository
Registration
authority
Certificate
publication
Certificate/CRL
publication
Certificate
authority
Cross
certification
CRL issuer
CRL
publication
Certificate
authority
PKI
management
entities
انتشار CRL

مدل PKIX



مرکز ثبت گواهی
دریافت درخواست و احراز اصالت، بررسی محتوای گواهی

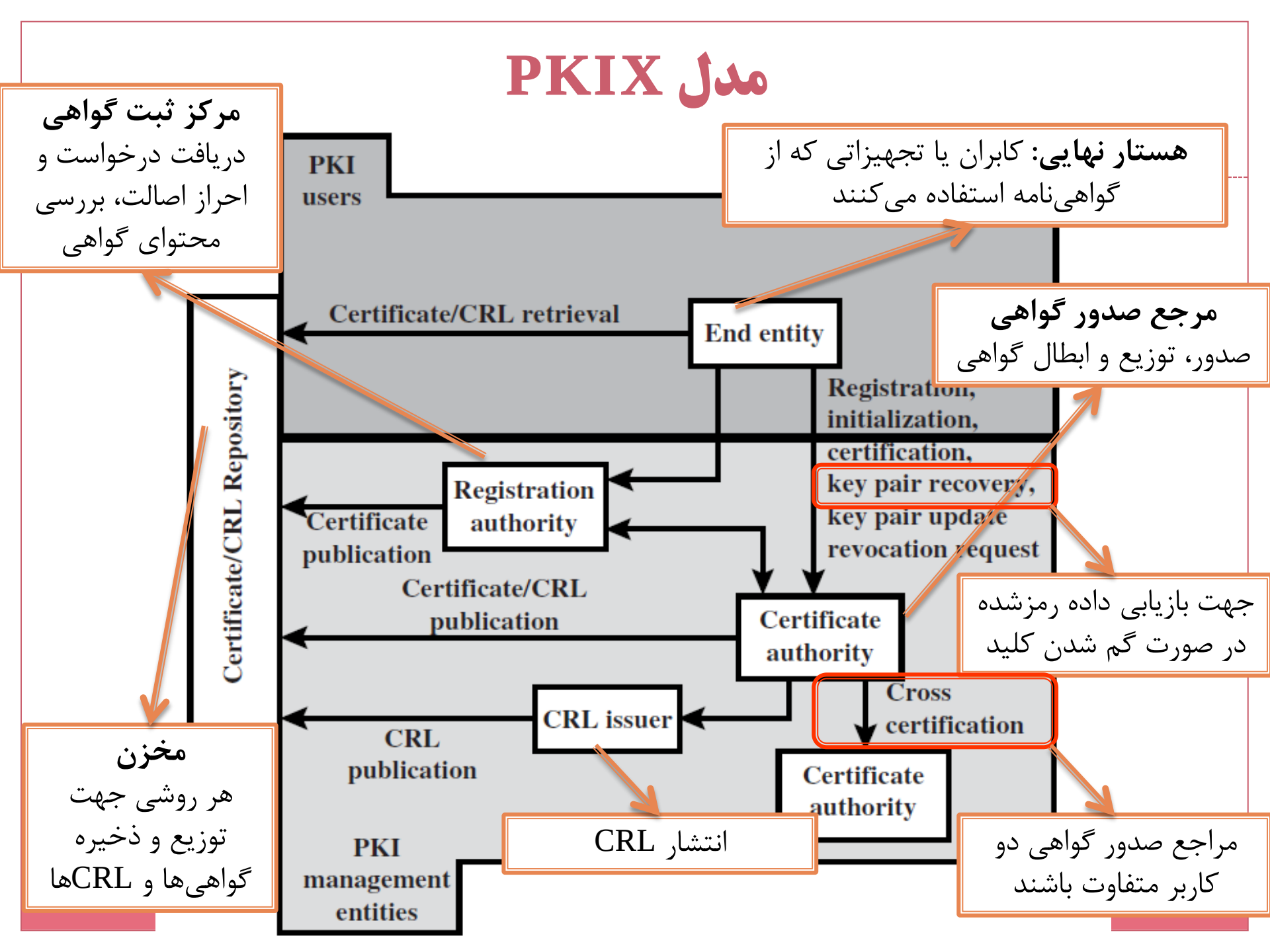
هستار نهایی: کابران یا تجهیزاتی که از گواهی‌نامه استفاده می‌کنند

مرجع صدور گواهی
صدور، توزیع و ابطال گواهی

مخزن
هر روشی جهت توزیع و ذخیره گواهی‌ها و CRLها

انتشار CRL

مدل PKIX



مرکز ثبت گواهی
دریافت درخواست و احراز اصالت، بررسی محتوای گواهی

هستار نهایی: کاربران یا تجهیزاتی که از گواهی‌نامه استفاده می‌کنند

مرجع صدور گواهی
صدور، توزیع و ابطال گواهی

جهت بازیابی داده رمزشده در صورت گم شدن کلید

مخزن
هر روشی جهت توزیع و ذخیره گواهی‌ها و CRLها

انتشار CRL

مراجع صدور گواهی دو کاربر متفاوت باشند