یا ذالامن والامان

مدیریت کلید

توسط: حمید رضا شهریاری

دانشگاه صنعتی امیرکبیر

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

http://www.aut.ac.ir/shahriari

اهداف

- آشنایی با مفاهیم :
  - تبادل / مدیریت کلید
  - کلید جلسه و کلید اصلی
  - شخص ثالث مورد اعتماد ***TTP***
- آشنایی با برخی پروتکلهای ساده توزیع کلید

فهرست

- مفاهیم اساسی مدیریت کلید
- کلید جلسه و کلید اصلی: توصیف
- مدیریت کلید مخفی
- مدیریت کلید عمومی
- اشتراک کلید جلسه
- لغت نامه
- پیوست

یا ذالامن والامان

برای دیدن معادل انگلیسی ترجمه ها به اسلاید
لغت نامه مراجعه نمایید.

کلید واژه ها:

فهرست

مدیریت کلید چیست؟

- مدیریت کلید عبارتست از مجموعه ایی از شگردها و رویه ها برای دایر نمودن و نگهداری «ارتباط کلیدی» بین طرفین مجاز.

- ارتباط کلیدی وضعیتی است که در آن طرفین برقرار کننده ارتباط داده معینی را به اشتراک می‌گذارند که مورد نیاز الگوریتم‌های رمز می‌باشد.
  - کلیدهای عمومی یا خصوصی،
  - مقداردهی های اولیه،
  - سایر پارامترهای غیر مخفی...

مدیریت کلید شامل چه رویه‌هایی است؟

1. مقدار دهی اولیه سیستمهای کاربران
2. تولید، توزیع و نصب داده های ارتباط کلیدی
3. کنترل نحوه استفاده از این کلیدها
4. به روزآوری، ابطال و نابود کردن داده های ارتباط کلیدی
5. نگهداری، نسخه برداری و بازیابی داده های ارتباط کلیدی

اهمیت مدیریت کلید

- اکثر حملات به رمزنگاری یک سیستم امنیتی در لایه مدیریت کلید می‌باشد تا الگوریتم‌هایی که از کلیدها (داده های مشترک) بهره می‌برند.
  - در حقیقت برخی این مساله را دشوارترین بخش یک سیستم امن می‌دانند.

تهدیدهای مدیریت کلید

- به خطر افتادن محرمانگی کلیدهای مخفی
- به خطر افتادن صحت (درستی) کلید های عمومی و یا مخفی
- استفاده غیر مجاز از کلیدهای عمومی و یا مخفی

فهرست

کلید جلسه و کلید اصلی: توصیف

- کلید اصلی عبارتست از یک کلید رمز کننده سایر کلیدها. به این معنا که از این کلید برای توزیع کلید سری موقتی به نام کلید جلسه استفاده مینماییم.
  - این کلید بین طرفین ارتباط و یک مرکز توزیع کلید(KDC) به اشتراک گذاشته می شود.
  - دستیابی به این کلید با مراجعه فیزیکی به KDC یا روش امن دیگری امکان پذیر است
- از کلید جلسه برای رمزنگاری(متقارن) و احراز هویت استفاده میکنیم.

سلسله مراتب کلیدها

نحوه محافظت	حجم اطلاعات	نوع
محافظت با رمزنگاری (با استفاده از کلید جلسه)		داده
محافظت با رمزنگاری (با استفاده از کلید اصلی)		کلید جلسه
محافظت فیزیکی		کلید اصلی

کلید جلسه و کلید اصلی: مقایسه

- کلید اصلی:
  - طول عمر نسبتاً زیاد،
  - میزان استفاده محدود(فقط رمز نگاری کلیدهای جلسه)،
  - خسارت گسترده درصورت افشاء
- کلید جلسه:
  - طول عمر نسبتاً کوتاه،
  - استفاده نامحدود در طول جلسه،
  - خسارت محدود و فقط در سطح داده های جلسه یک جلسه خاص

اهمیت طول عمر کلید جلسه

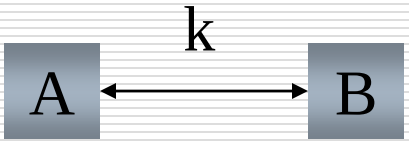
- طول عمر کوتاه:
  - امنیت بالا
    - حجم داده برای تحلیل رمز ناچیز است
    - میزان استفاده کم است
    - حتی پس از افشای کلید، زمان زیادی برای سوء استفاده موجود نیست.
  - کارایی کم
    - همیشه باید کلید را به روز کنیم
- طول عمر زیاد:
  - کارایی بالا، امنیت کم

یک مصالحه میان *امنیت* و *کارایی* بر سر تعیین طول عمر کلید جلسه برقرار است.

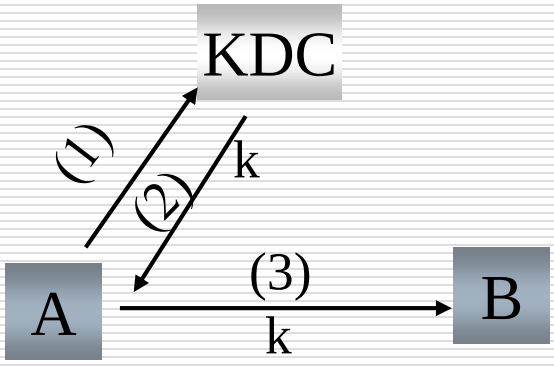
فهرست

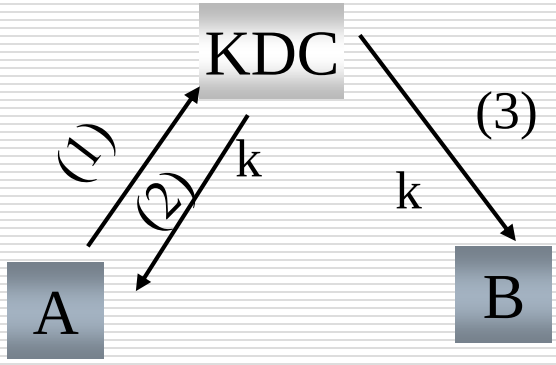
مدیریت کلید مبتنی بر کلید مخفی

- نقطه به نقطه



- مرکز توزیع کلید





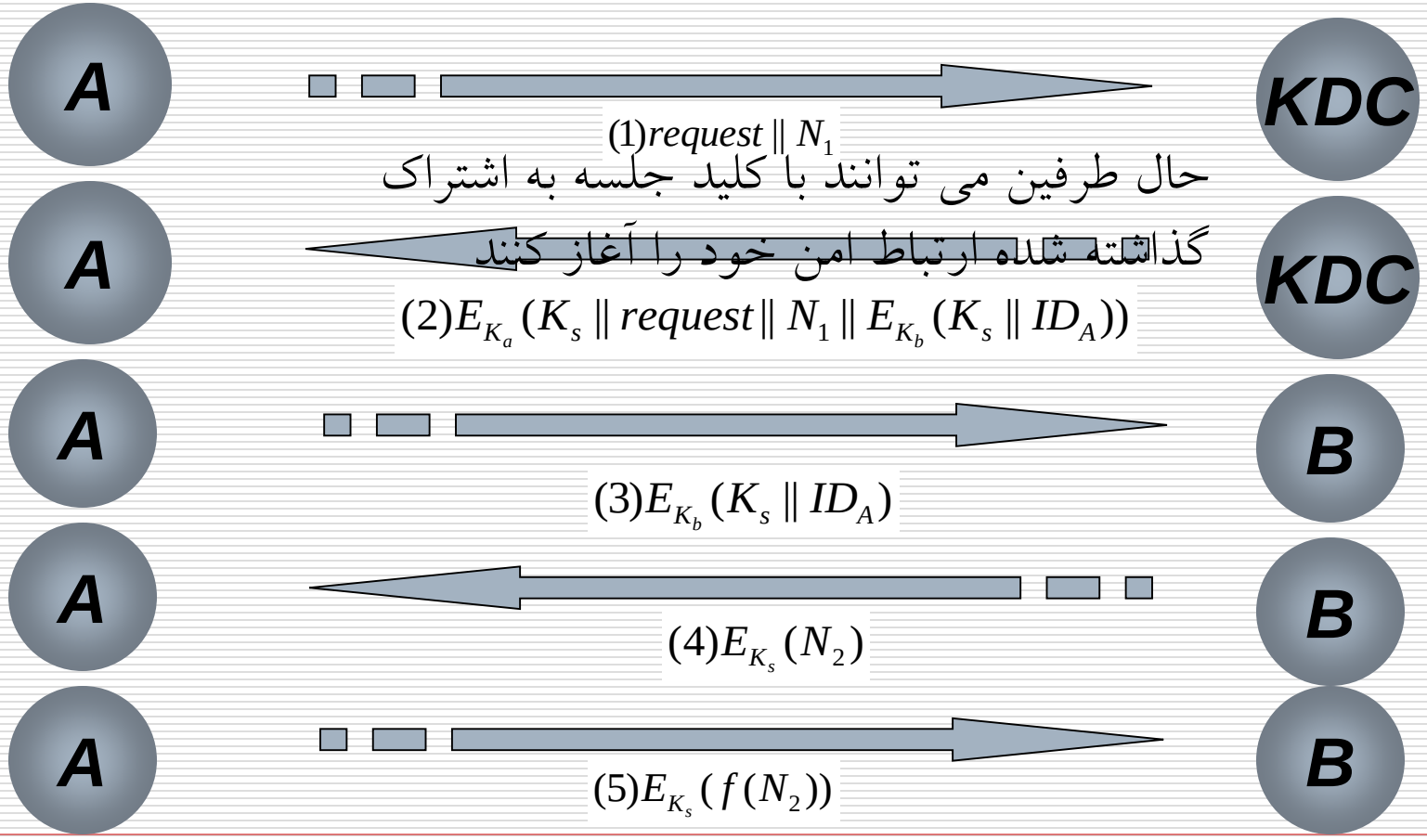
روش نقطه به نقطه

- نیاز به توافق بر روی کلید پیش از برقراری ارتباط بین هر دو نفر
- مقیاس پذیری: مشکل اصلی
  - برای ارتباط n نفر باهم به n(n-1)/2 کلید احتیاج داریم.
- علاوه بر این هیچ مرجعی برای رسیدگی به مشکل وجود ندارد

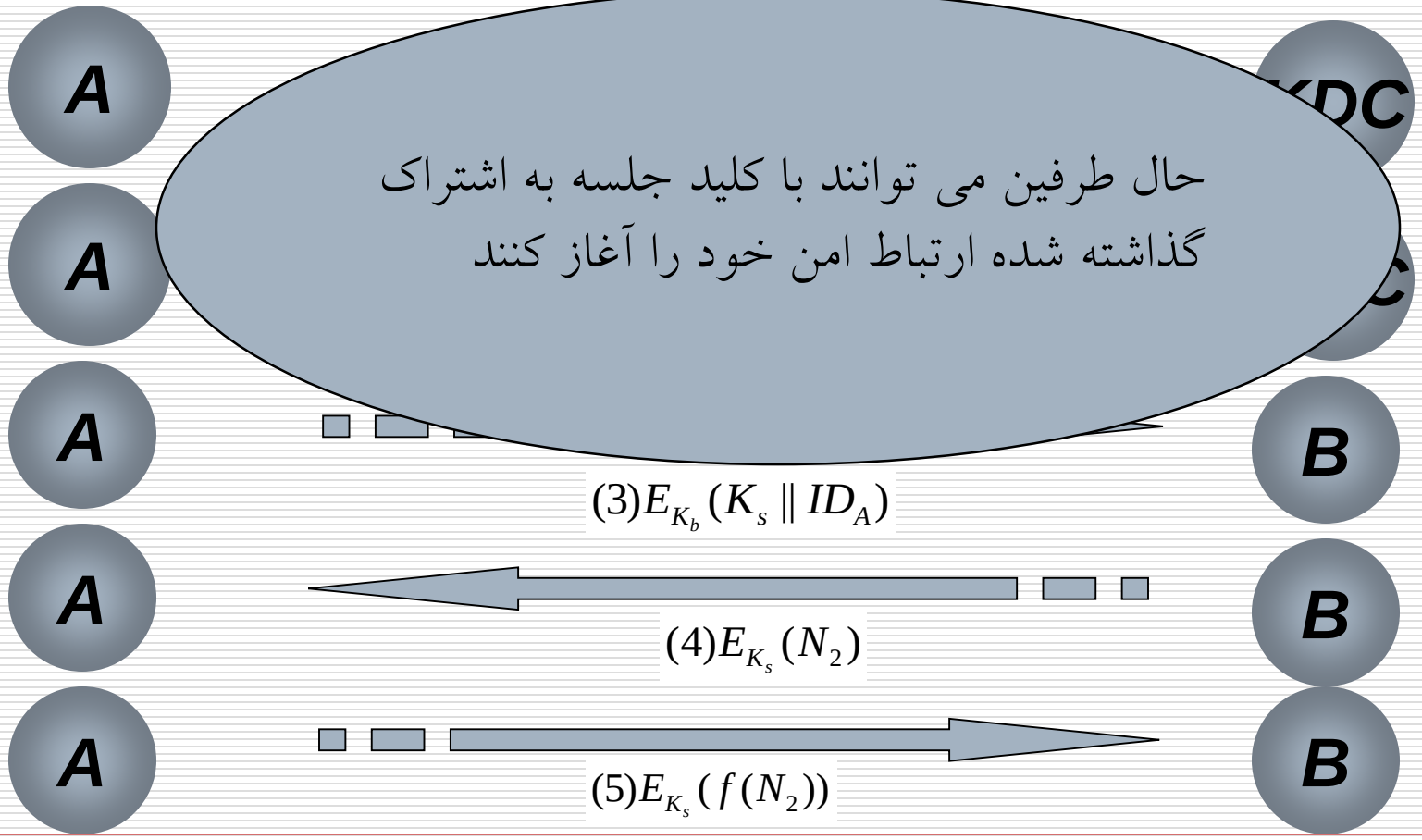
روش متمرکز توزیع کلید

- هر کاربر یک کلید اصلی با کارگزار توزیع کلید **KDC** به اشتراک گذاشته است.
  - KDC یک شخص ثالث مورد اعتماد است. (پیوست)
  - این کلیدها با یک روش امن (مثلاً مراجعه فیزیکی) توزیع شده‌اند.
- ایده:
  - هربار که کاربری قصد ارتباط با دیگران را داشته باشد از **KDC** یک کلید جلسه درخواست می‌کند.

گامهای توزیع کلید
گامهای احراز هویت



گامهای توزیع کلید
گامهای احراز هویت



روش متمرکز توزیع کلید

- نکات مثبت:
  - تعداد کلید کمتر
- نکات منفی:
  - کارگزار توزیع کلید گلوگاه امنیتی سیستم است
  - ترافیک بالا در کارگزار توزیع کلید گلوگاه کارایی سیستم است
  - نیاز به یک کارگزار بر خط داریم
    - دخالت کارگزار در برقراری هر ارتباط ضروری است.

فهرست

مزایای رمزنگاری کلید عمومی

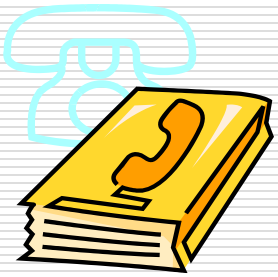
- پس از توافق روی کلیدهای عمومی، نیازی به محرمانه ماندن آنها نیست.
- نیازی به کارگزار برخط نیست.

شگردهای توزیع کلید عمومی

- Public Announcement
- اعلان عمومی
- Public available Directory
- فهرست راهنمای عمومی
- Public-key authority
- مرجع معتبر کلید عمومی
- Public-key certificates
- گواهی های کلید عمومی

اولین روش : اعلان عمومی

- فرستادن کلید عمومی خود برای شخص یا گروه گیرنده
  - مثال : الحاق کلید PGP به پیغام ایمیل یا ارسال آن به یک گروه خبری
- ضعف عمده : جعل کلید
  - ارسال یک کلید عمومی به نام شخص دیگر.
  - تا کشف شدن جعل می‌توان از آن سوء استفاده کرد

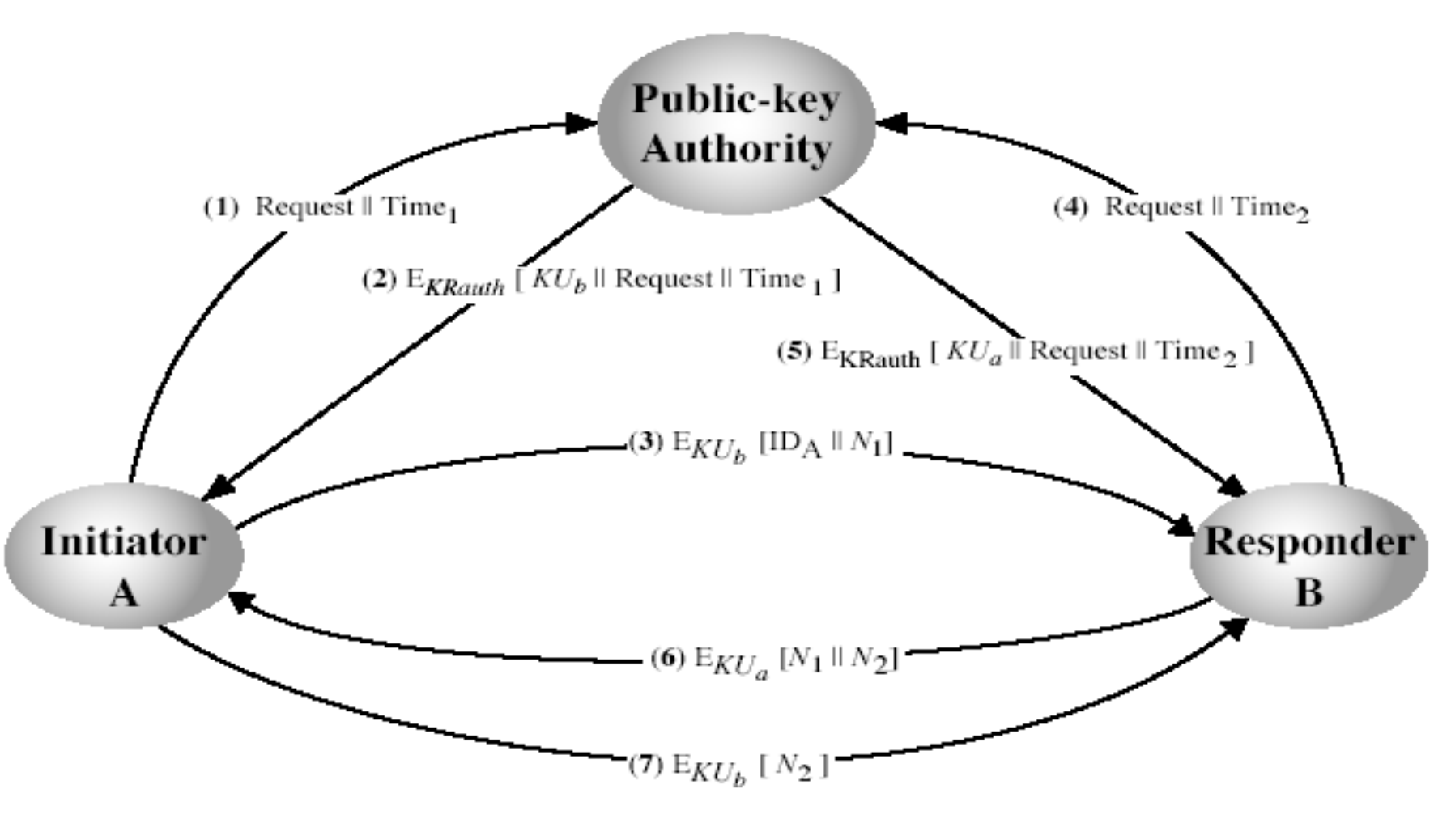


فهرست راهنمای عمومی

- یک مرجع مورد اعتماد مسؤول نگهداری یک فهرست عمومی از کلیدهای عمومی می‌باشد.
  - ثبت نام در فهرست عمومی با احراز هویت متقاضی انجام میپذیرد.
  - امکان ثبت نام و جایگزینی کلید در هر زمان وجود دارد.
    - این کار توسط صاحب اصلی کلید انجام می شود(پس از انجام احراز هویت)
  - مرجع فهرست را به صورت دوره ای منتشر می‌کند.(مانند دفترچه تلفن)
  - امکان دسترسی به فهرست وجود دارد.
- مشکل: امکان دست بردن در رکوردها یا لو رفتن کلید خصوصی مرجع مورد اعتماد

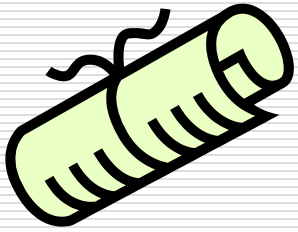
مرجع معتبر کلید عمومی

- اعمال کنترل بیشتر در توزیع کلید از طریق فهرست
  - نیاز به دانستن کلید عمومی فهرست
  - برای برقراری ارتباط، گیرنده و فرستنده از مرجع مربوطه کلید عمومی یکدیگر را در خواست می‌کنند.
  - گیرنده و فرستنده سپس به احراز هویت یکدیگر می‌پردازند.
- مرجع، گلوگاه سیستم است.
- هنوز خطر دستکاری در فهرست وجود دارد.


Public-key Authority
(1) Request || Time1
(2) EKRauth [KUb || Request || Time 1]
(4) Request || Time2
(5) EKRauth [KUa || Request || Time 2]
(3) EKUb [IDA || N1]
Initiator A
Responder B
(6) EKUa [N1 || N2]
(7) EKUb [N2]

گواهی‌های کلید عمومی

- تبادل کلید بدون تماس با مرجع
- گواهی شامل هویت فرد و کلید عمومی اوست.
  - سایر اطلاعات :
    - زمان اعتبار
    - مجوز نوع استفاده
- داده‌های فوق با کلید خصوصی CA رمز شده است.
- اعتبار کلید عمومی را می توان با دانستن کلید عمومی CA بررسی کرد.

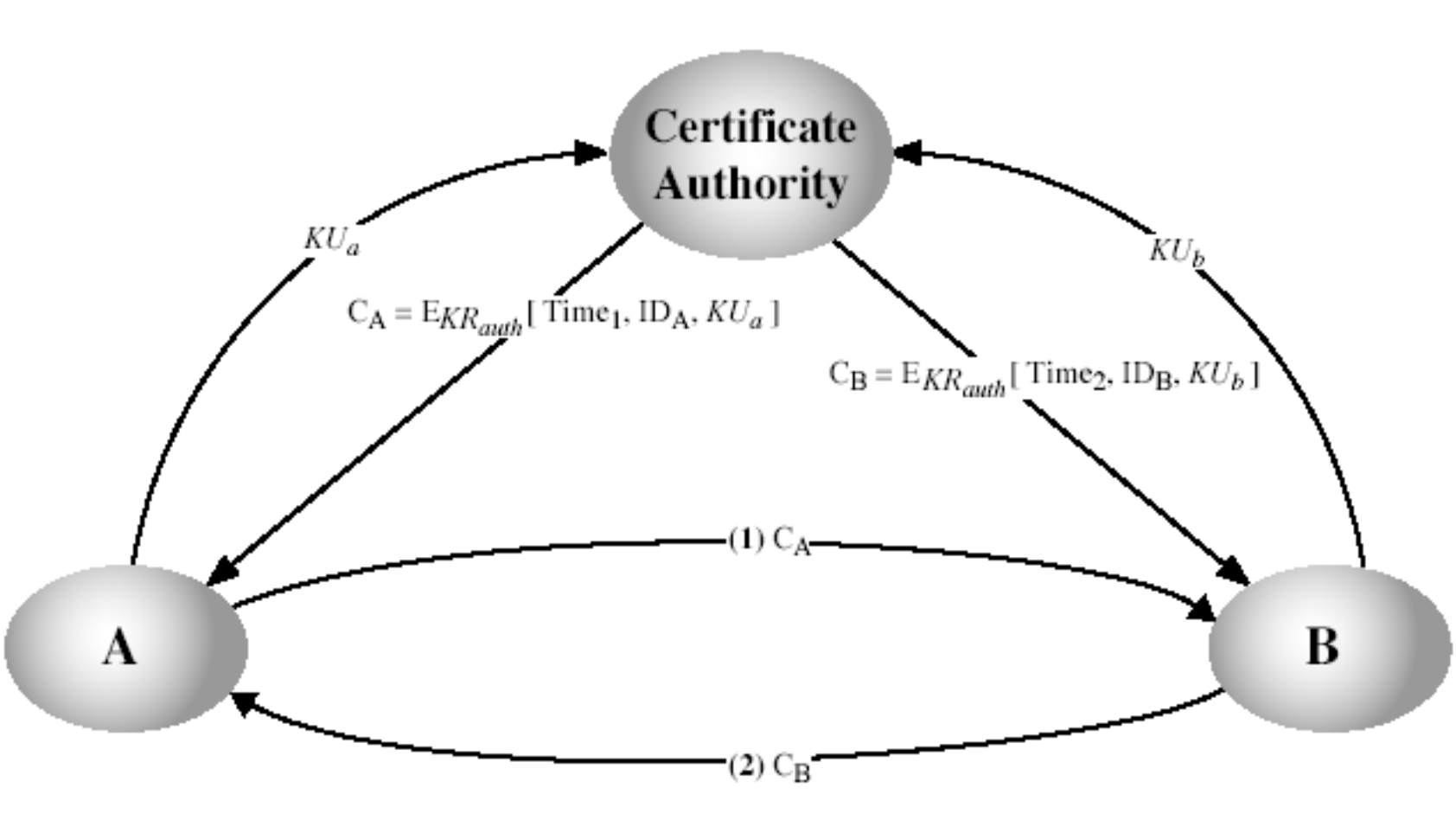


مثالی از گواهی کلید عمومی

Serial Number:	48
Certificate for:	Bob Burton
Company:	Fox Consulting
Issued By:	Awfully Big Certificate Co.
Email Address:	bsmith@pleasantville.ca.us
Activation:	Jan. 10, 2000
Expiration:	Jan. 10, 2002
Public Key:	24219743597430832a2187b 6219a75430d843e432f21e09 bc080da43509843

ABC's Digital Signature

0a213fe67de49ac8e9602046fa7de22
39316ab233dec70095762121aef4fg6
6854392ab02c4


Certificate Authority
KU_a
KU_b
$C_A = E_{KR_{auth}}[\text{Time}_1, \text{ID}_A, KU_a]$
$C_B = E_{KR_{auth}}[\text{Time}_2, \text{ID}_B, KU_b]$
(1) C_A
A
B
(2) C_B

مرجع معتبر کلید عمومی یا گواهی های کلید عمومی؟

- مرجع معتبر
  - مرجع حکم شخص ثالث مورد اعتماد بر خط دارد.
    - در هر ارتباط باید ابتدا با مرجع تماس گرفت.
  - گیرنده و فرستنده می‌توانند با ذخیره کلیدها تماس خود با مرجع را کاهش دهند.
    - اگر کلید یک کاربر تغییر کند یا حذف شود، چه کنیم؟
- گواهی
  - CA حکم شخص ثالث مورد اعتماد خارج از خط دارد.
    - نیاز به فهرستهای ابطال گواهی دارد.

فهرست

کلید جلسه + کلید عمومی

- از آنجا که الگوریتم‌های کلید عمومی بسیار کندتر از الگوریتم‌های مرسوم (کلید مخفی) می‌باشند، از این کلیدها جهت توزیع کلید جلسه (و نه رمزگذاری) بهره می‌بریم.

اشتراک کلید جلسه

- بنا نهادن *دو جانبه* کلید جلسه
  - طرفین به طور مستقل در انتخاب کلید تاثیر گذار می‌باشند.
    - مثال : روش Diffie-Hellman
- توزیع یک *جانبه* کلید جلسه
  - یکی از دو طرف کلید را معین کرده و به دیگری ارسال می‌نماید.
    - مثال : روش ارائه شده توسط Merkle

الگوریتم Diffie Hellman

- الگوریتم به اشتراک گذاری کلید
- امنیت برمفروضات DH (پیوست)
- بر روی مقادیر q و α توافق می‌کنند.
- q یک عدد اول و α یک مولد برای این عدد می‌باشد.

Diffie - Hellman الگوریتم

طرفین روی مقدار q و α با هم توافق می‌کنند.

Alice	Bob
عدد تصادفی X_A را انتخاب می‌کند	عدد تصادفی X_B را انتخاب می‌کند
$Y_A = \alpha^{X_A} \bmod q$	
	$Y_B = \alpha^{X_B} \bmod q$
$K_{AB} = (Y_B)^{X_A} \bmod q$	$K_{AB} = (X_A)^{Y_B} \bmod q$

کلید مشترک برابر است با $\alpha^{(X_A \times X_B)} \bmod q$

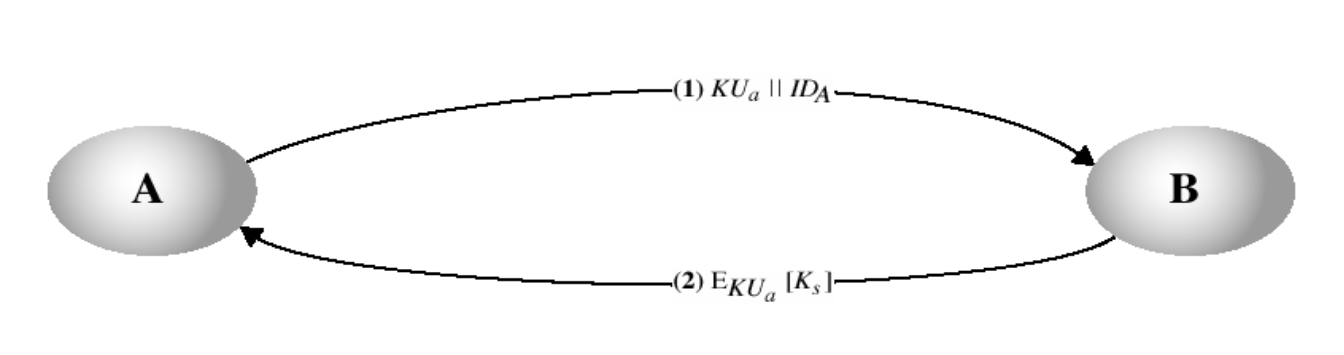
Diffie-Hellman

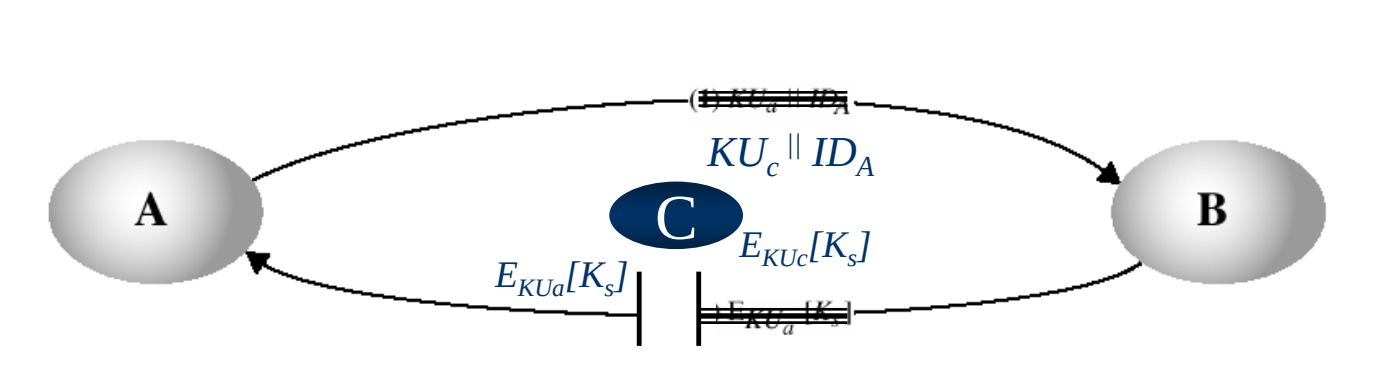
- مثال
  - توافق روی $q=353$ و $\alpha=3$
  - تولید کلیدهای مخفی
    - انتخاب $x_A=97$ توسط A و $x_B=233$ توسط B
  - محاسبه کلید عمومی
    - $y_A=3^{97} \bmod 353 = 40$
    - $y_B=3^{233} \bmod 353 = 248$
  - محاسبه کلید جلسه توافقی
    - $K_{AB}= y_B^{x_A} \bmod 353 = 248^{97} = 160$
    - $K_{AB}= y_A^{x_B} \bmod 353 = 40^{233} = 160$

روش Merkleجهت توزیع یک‌جانبه کلید

- یک روش ساده (ارائه شده توسط *Merkle* در سال *۱۹۷۹*)
  - زوج کلید عمومی و خصوصی توسط *A* استفاده می‌شود.
  - کلید عمومی و هویت *A* برای *B* فرستاده می‌شود.
  - تولید کلید جلسه *k* توسط *B*، رمزکردن آن با کلید عمومی *A* و بازگرداندن کلید رمزشده برای *A*
  - بدست آوردن کلید جلسه توسط *A*
  - تنها در مقابل حمله غیرفعال مقاومت می‌کند.

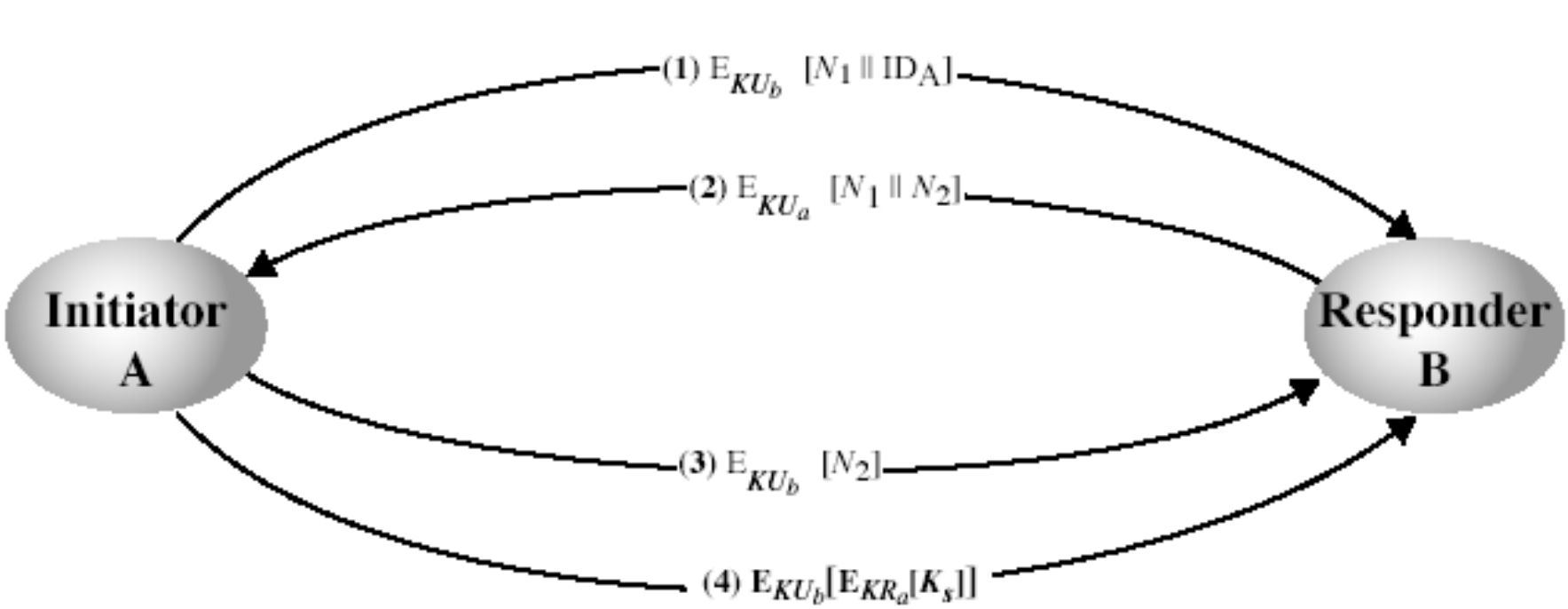
حمله Man In The Middle توسط C به پروتکل





یک پروتکل قوی‌تر

- سه گام آغازین برای احراز هویت و جلوگیری از حمله تکرار می‌باشد.
- اگر سه مرحله اول انجام نشود، شخص ثالث با دانستن کلید جلسه قبلی به راحتی می تواند جلسه جدیدی را با B آغاز کند.
- گام نهایی، محرمانگی و احراز هویت، هر دو را برآورده می‌کند.



روش ترکیبی

- کلید عمومی+رمزنگاری متقارن

- ۳ سطح را شامل می شود:
  - توافق KDC با هر یک از کاربران روی یک کلید اصلی(master key)
    - استفاده از کلید عمومی برای توزیع کلیدهای اصلی
  - استفاده از کلید اصلی(رمزنگاری متقارن) برای توزیع کلیدهای جلسه
  - استفاده از کلید جلسه برای انتقال محرمانه داده ها

کارآیی روش ترکیبی

- توزیع مداوم کلید با رمزنگاری کلید عمومی کارآیی سیستم را کاهش می‌دهد. با کمک روش ترکیبی به طور موردی از رمزنگاری کلید عمومی برای به روز درآوردن کلید اصلی بهره می‌جوییم.

لغت نامه

Unauthorized	غیر مجاز
Directory	فهرست
Session Key	کلید جلسه
Bottleneck	گلوگاه
Certificate	گواهی
Centralized	متمرکز
Confidentiality	محرمانگی
Authority	مرجع
KDC	مرکز توزیع کلید
Trade Off	مصالحه
Initialization	مقداردهی اولیه
Back Up	پشتیبان گیری
Master Key	کلید اصلی

Key Management	مدیریت کلید
Revocation	ابطال
Keying Relationship	ارتباط کلیدی
Announcement	اعلان
Restoration	بازیابی
On line	برخط
Forge	جعل
Off Line	برون‌خط
In line	برخط
Tampering	دستکاری
Procedure	رویه
TTP :Trusted Third Party	شخص ثالث مورد اعتماد

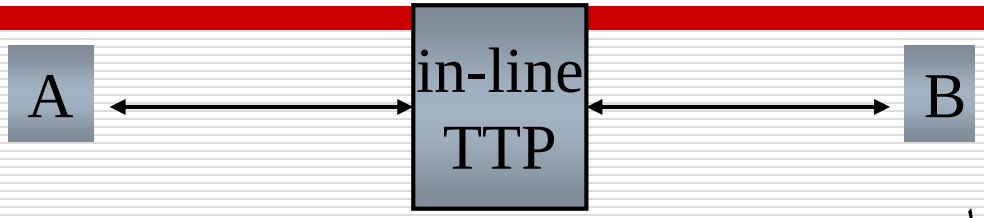
یا ذالامن والامان

پیوست
شخص ثالث

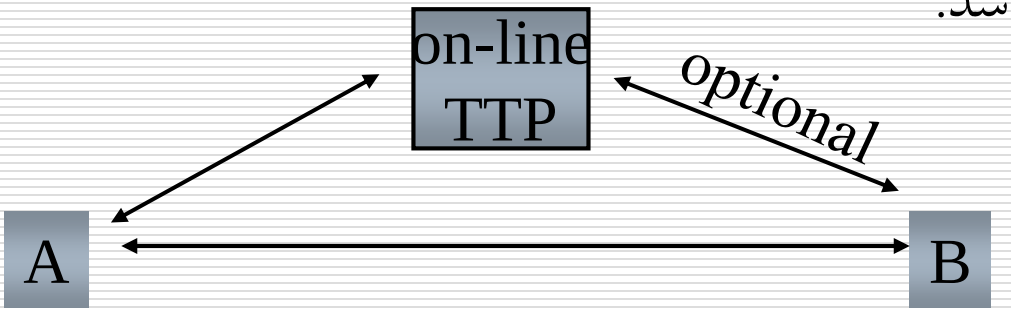
شخص ثالث مورد اعتماد TTP

- بسیاری از پروتکلها برای اجرای صحیح به یک شخص ثالث مورد اعتماد نیاز دارند.
  - این شخص در بسیاری از مواقع تبدیل به گلوگاه میشود☹
    - منجر به مشکلاتی در زمینه مقیاس پذیری میشود
  - باید به این شخص اعتماد کنیم☹
  - به این شخص وابسته میشویم☹
  - ...

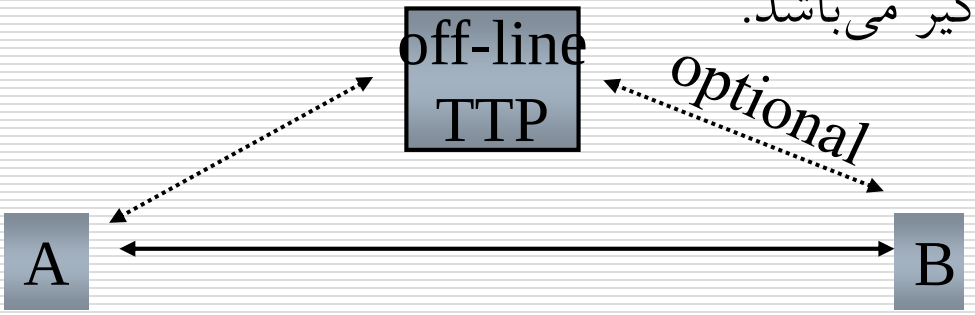
انواع شخص ثالث مورد اعتماد



در خط: ***TTP*** همواره درگیر می‌باشد.



برخط: ***TTP***در بخشی از ارتباط درگیر می‌باشد.



خارج از خط: ***TTP*** تنها در موارد خاص دخالت می‌کند.

یا ذالامن والامان

Diffie Hellman مفروضات

لگاریتم گسسته

q یک عدد اول و α یک مولد برای این عدد میباشد.

- یعنی هر عدد بین ۱ تا q را میتوان به صورت توانی از α نشان داد.
- اگر $a = \alpha^b \bmod q$ باشد آنگاه عملیات یافتن b از روی a را محاسبه لگاریتم گسسته گویند.
- فرض: محاسبه لگاریتم گسسته از لحاظ محاسباتی ناممکن است.

فرض CDH

- فرض کنید مقادیر $\alpha^a \bmod q$ و $\alpha^b \bmod q$ داده شده اند.
- فرض CDH یا دیفی هلمن محاسباتی:
  - محاسبه $\alpha^{ab} \bmod q$ از روی مقادیر بالا از لحاظ محاسباتی ناممکن است.
  - این فرض اساس امنیت تبادل کلید دیفی هلمن است.

Discrete Logarithm Timeline