دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)
دانشکدهٔ مهندسی کامپیوتر و فنآوری اطلاعات

مبانی امنیت اطلاعات

(ترم بهمن ۹۸)

احراز هویت

نستوه طاهری جوان

nastooh@aut.ac.ir

احراز هویت

- ✓ سه روش کلی برای احراز هویت
  - احراز هویت بر اساس اطلاعاتی که کاربر در اختیار دارد
    - مانند کلمات عبور
  - احراز هویت بر اساس چیزهایی که کاربر در تملک خود دارد
    - مانند کلید
    - اسمارت کارت
  - احراز هویت بر اساس ویژگی های منحصر به فرد کاربر
    - مانند مکانی که از آنجا ارتباط برقرار کرده (بیشتر در شبکه کاربرد دارد)
    - اثر انگشت
    - اسکن چشم

nastooh@aut.ac.ir

احراز هویت

- ✓ استفاده از کلمهٔ عبور
  - حالت User Generated PSWs
    - مزیت: به خاطر سپردن راحت توسط کاربر
    - عیب: حدس زدن راحت توسط نفوذگر
  - حالت System Generated PSWs
    - مزایا و معایب، عکس حالت فوق
  - حالت Associative PSWs
    - پرسیدن سوالهایی از کاربر...
      - تیم مورد علاقه
      - اولین معلم

احراز هویت

- ✓ احراز هویت مبتنی بر چالش-پاسخ
  - طرف اول یک عدد تصادفی بزرگ انتخاب کرده و برای طرف دوم ارسال می کند.
  - طرف دوم یک تبدیل خاص بر روی این عدد اعمال کرده و برای طرف اول بازمیگرداند
  - طرف اول با بررسی پاسخ دریافتی، پِی به هویت طرف دوم می برد.
  - در صورت نیاز، عکس این روال نیز انجام می شود.

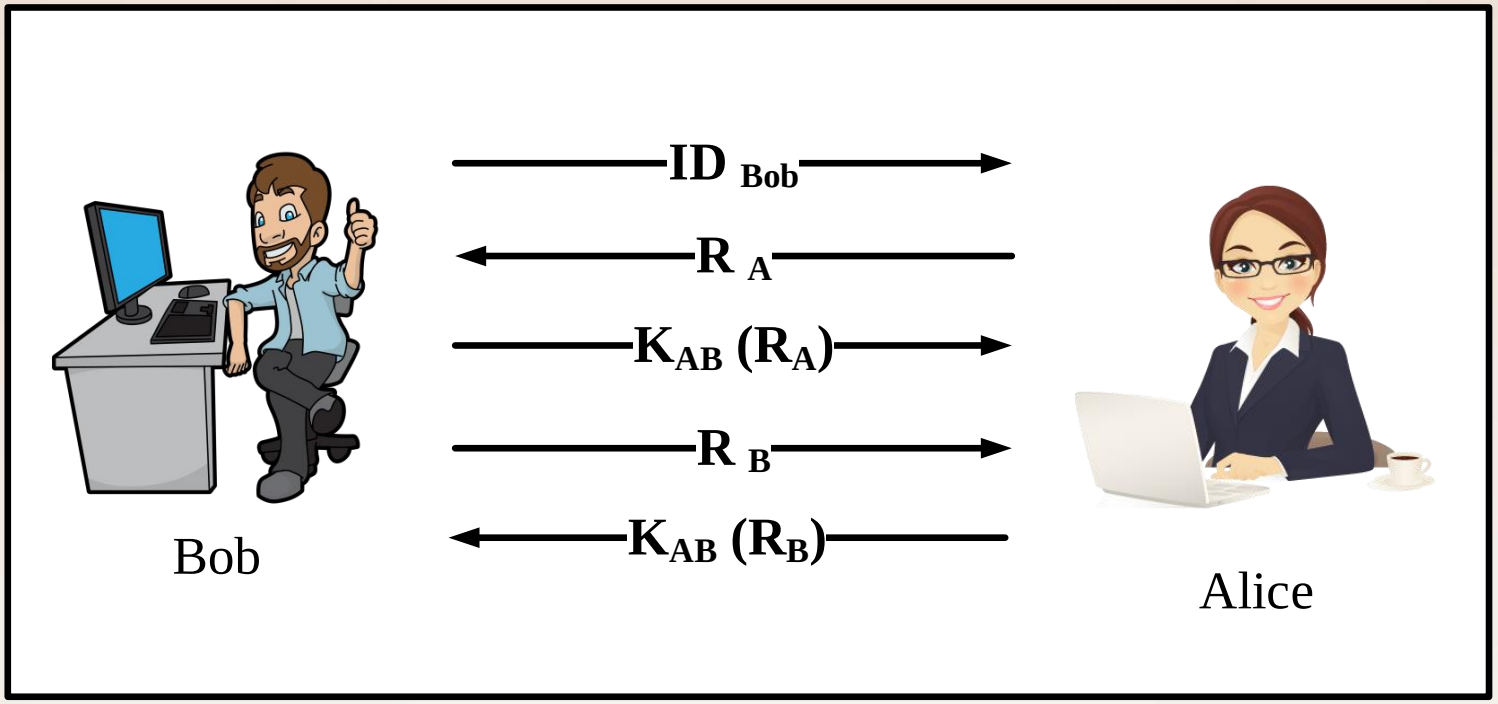
احراز هویت

- احراز هویت بر اساس کلید مشترک و سری

- هر دو طرف بر روی یک کلید مشترک و سری توافق کرده اند.
- مبتنی بر چالش-پاسخ هر دو طرف، طرف مقابل را بررسی می کنند.

احراز هویت

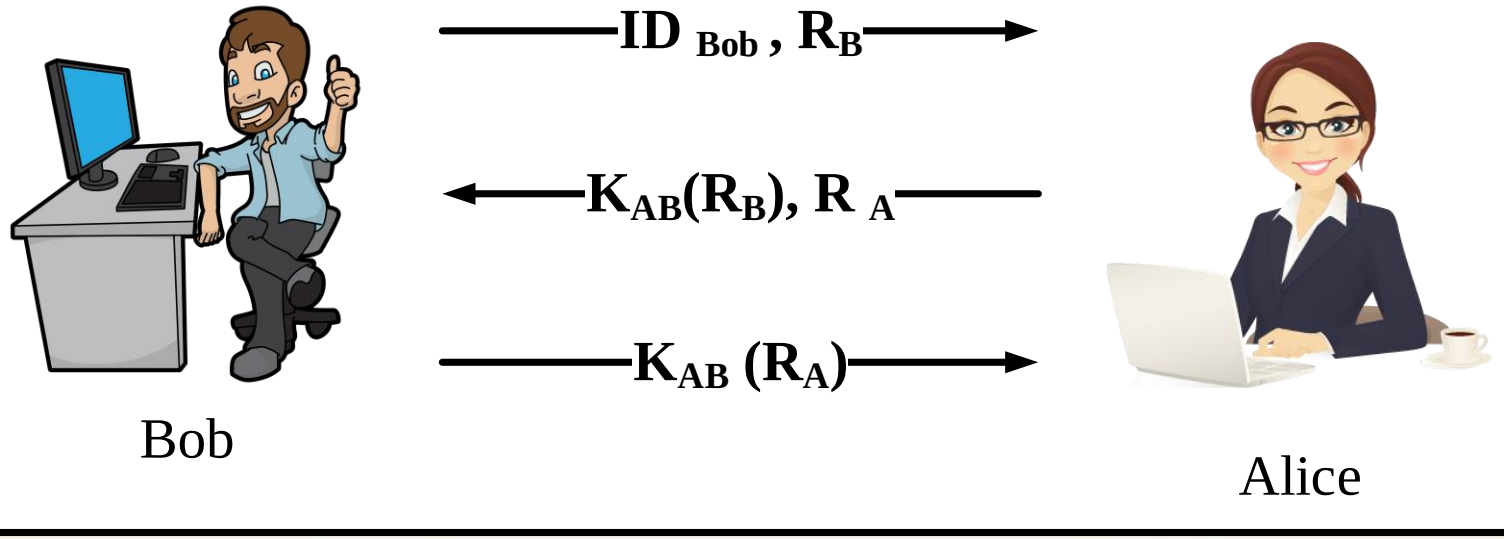
- احراز هویت بر اساس کلید مشترک و سری



- ایراد ضمنی: طولانی بودن تعداد مراحل
- آیا می توان مراحل را کاهش داد؟

احراز هویت

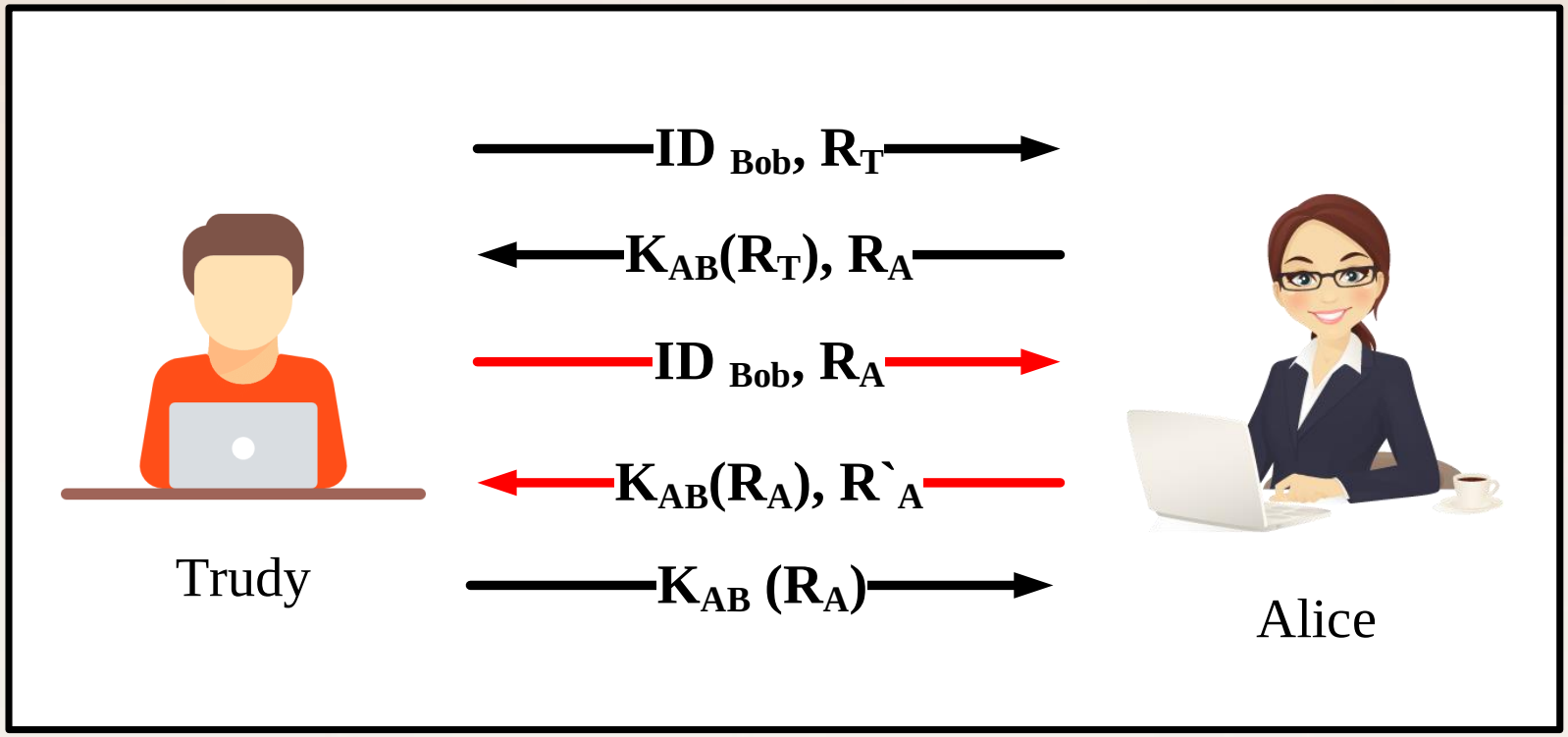
- احراز هویت بر اساس کلید مشترک و سری
  - کوتاه شدهٔ روال قبلی، با ادغام پیام ها



nastooh@aut.ac.ir

احراز هویت

- احراز هویت بر اساس کلید مشترک و سری
  - حملهٔ Reflection Attach برعلیه روال پیشین



ترودی پاسخ مربوط به چالش آلیس را بر روی یک نشست دیگر از خود وی می پرسد!

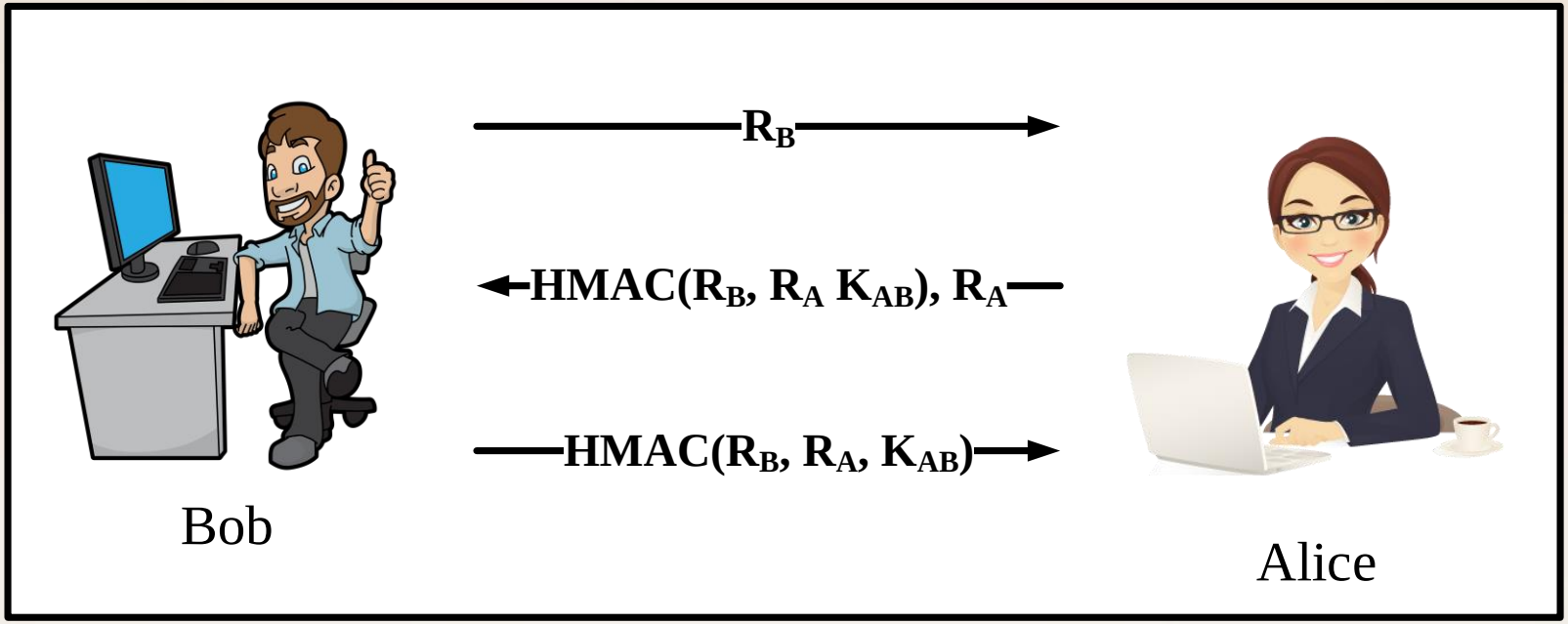
nastooh@aut.ac.ir

احراز هویت

- احراز هویت بر اساس کلید مشترک و سری
  - چند نکته
    - در کاربردهایی که یکی از طرفین چندین نشست دارد، نباید بتوان از اطلاعات (مثلا اعدد) یک نشست در نشستی دیگر استفاده کرد.
    - اگر طرفین اعداد خود را از مجموعه های متفاوتی انتخاب می کردند، این اتفاق رخ نمیداد.
      - « **مثلا همیشه طرف اول ارتباط از اعداد زوج، و طرف دوم از اعداد فرد استفاده کنید**

احراز هویت

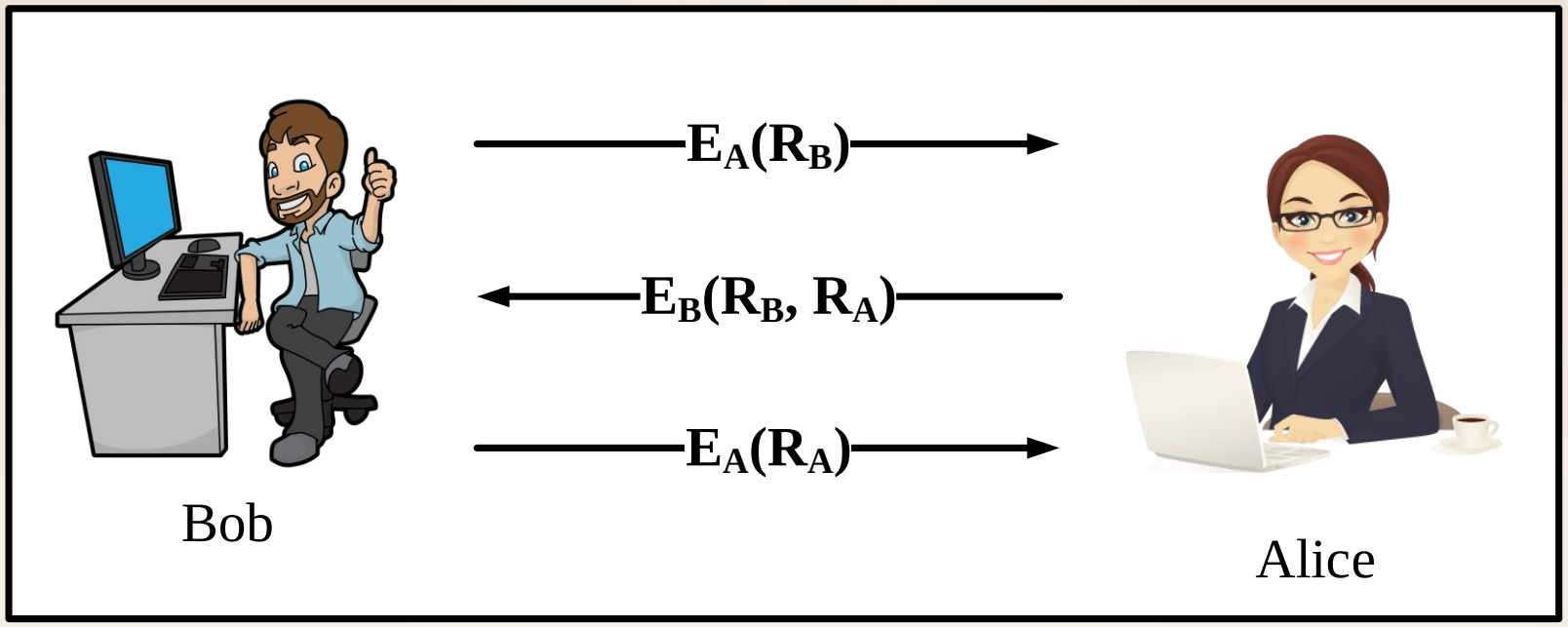
- احراز هویت با استفاده از HMAC
  - یاداوری: در HMAC، طرفین یک کلید مشترک و سری دارند.



- مزیت این روش سرعت پیاده سازی آن است.

احراز هویت

- احراز هویت بر اساس PKC
  - فرض: می توان کلید عمومی افراد را با روشی مطمئن به دست آورد.

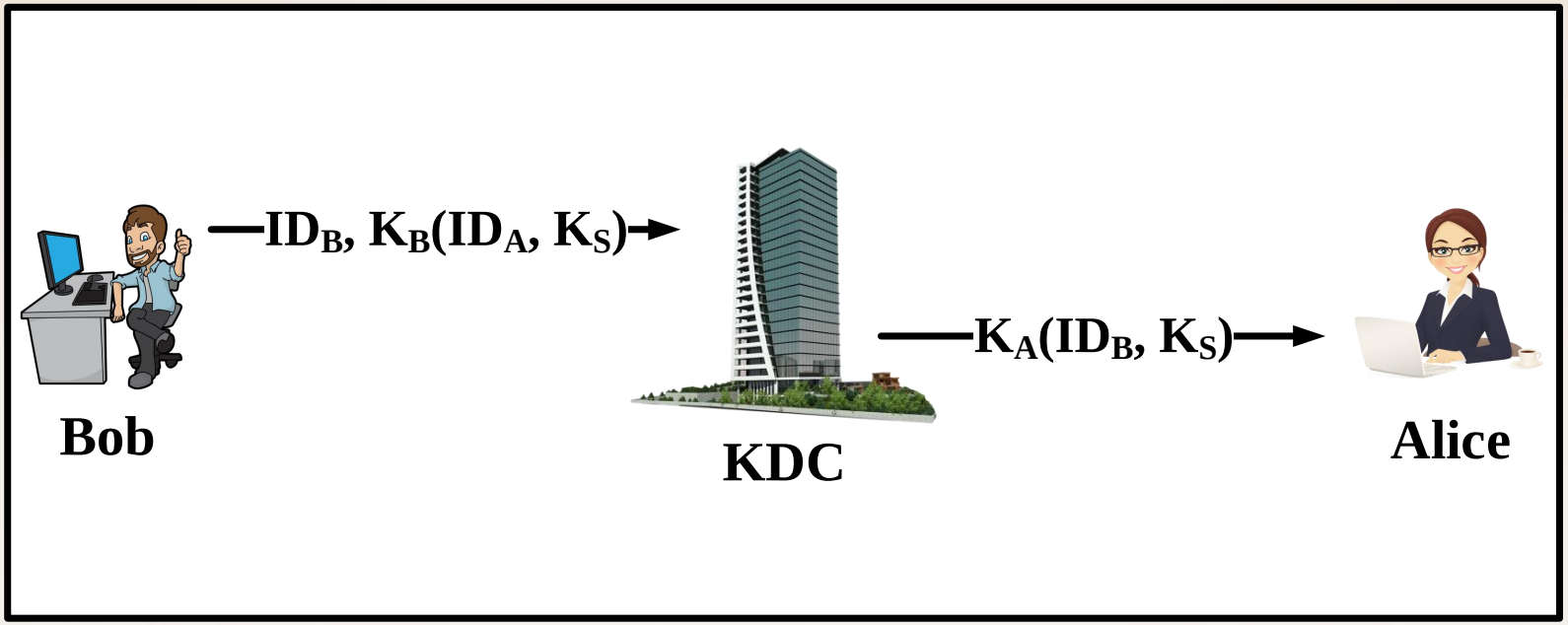


می توان کلید نشست را برای کارها و مراحل بعدی را در همین فاز سِت کرد.

احراز هویت

- احراز هویت بر اساس مرکز توزیع کلید
  - در پیاده سازی KDC(Key Distribution Center)، فرض بر این است که افراد حضوراً به این مراکز مراجعه کرده و کلید خود را شخصاً دریافت (یا ثبت) می کنند!

ساده ترین حالت برای استفاده از KDC

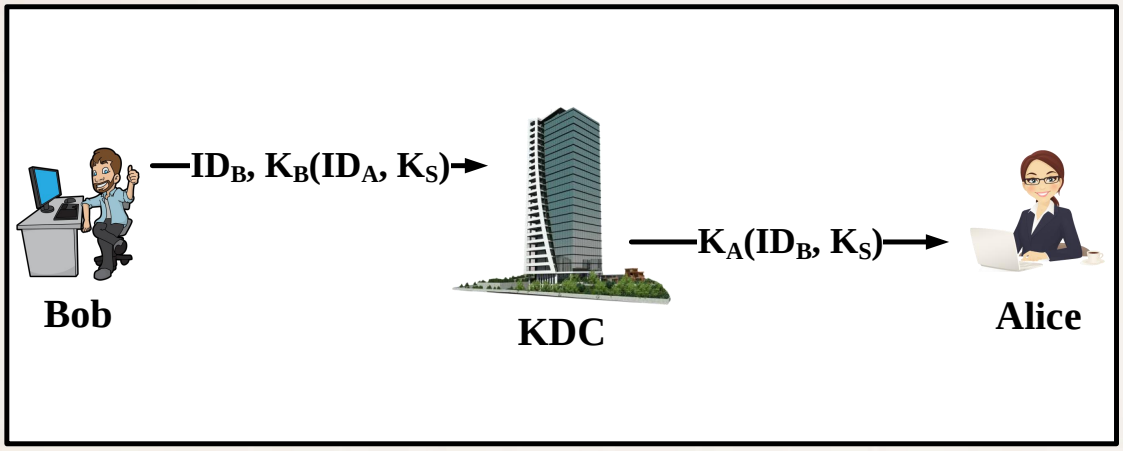


- کلید نشست برای کاربردها و مراحل بعدی استفاده می شود

احراز هویت

- احراز هویت بر اساس مرکز توزیع کلید
  - بر علیهٔ مکانیزم سادهٔ پیشین، حملهٔ Replay Attack را می توان انجام داد.
  - فرض کنید ترودی، پیام دوم را شنود و ذخیره کند.
  - نمی تواند آن را باز و استخراج کند، اما میتواند فردا آنرا دوباره برای آلیس ارسال کند و یک نشست جدید را آغاز کند.

- به پروتکل قبل دقیق تر نگاه کنید:



nastooh@aut.ac.ir

احراز هویت

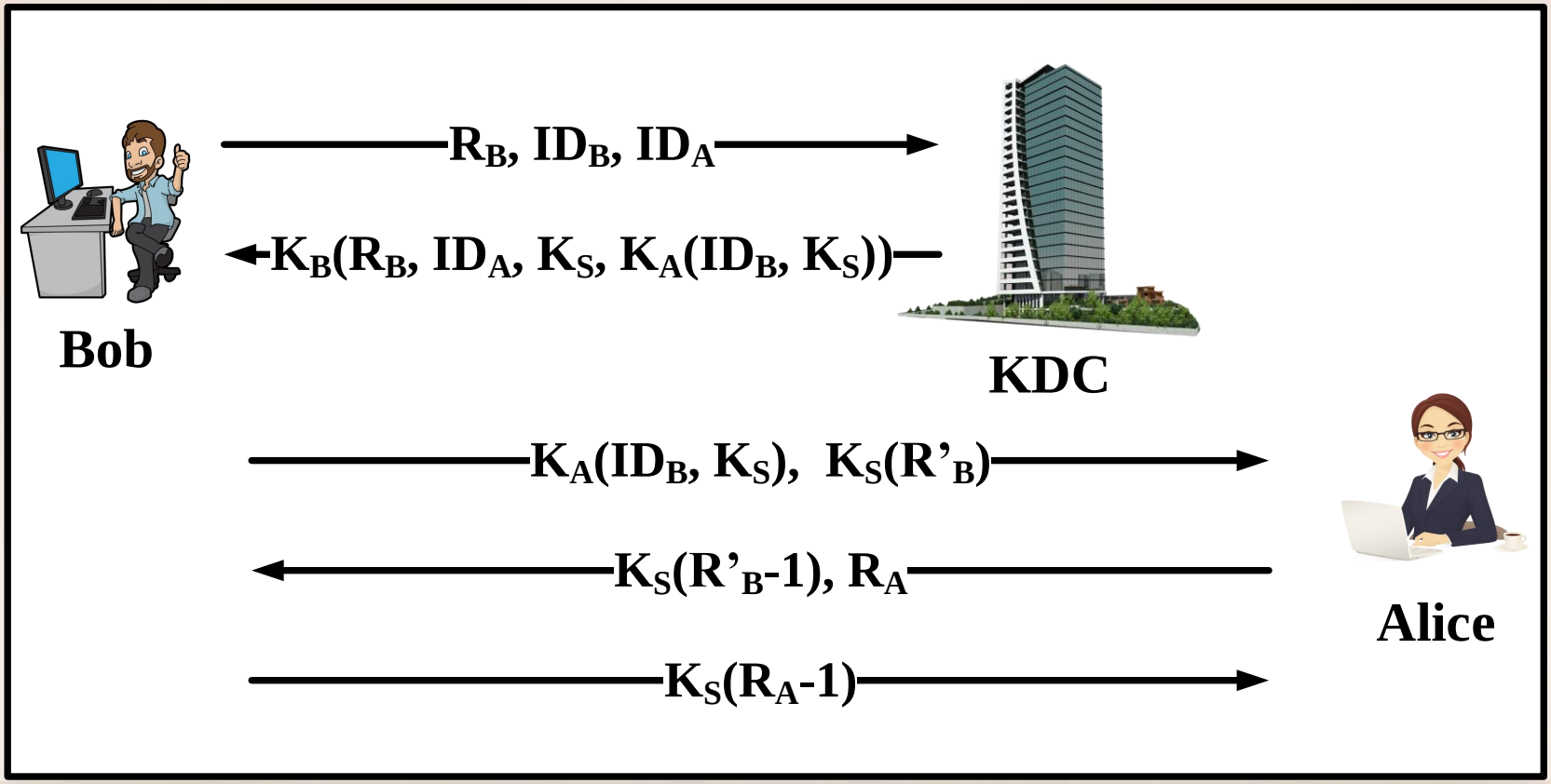
- احراز هویت بر اساس مرکز توزیع کلید
  - یک پروتکل عملیاتی شده مبتنی بر KDC: **نیدهام-شرودر**
  - سال ۱۹۷۸

- **استفادهٔ خیلی مختصر و مفید از KDC**

nastooh@aut.ac.ir

احراز هویت

- احراز هویت بر اساس مرکز توزیع کلید
  - یک پروتکل عملیاتی شده مبتنی بر KDC: **نیدهام-شرودر**



nastooh@aut.ac.ir

احراز هویت

- احراز هویت بر اساس مرکز توزیع کلید
  - یک پروتکل عملیاتی شده مبتنی بر KDC: **نیدهام-شرودر**

1. **باب یک رشتهٔ تصادفی برای KDC ارسال می کند.**
2. **KDC چند قلم را با کلید باب رمز کرده و برایش پس می فرستد، شامل:**
   - **رشته ی تصادفی اول (باب مطمئن می شود که پاسخ تقاضای کنونی را گرفته)**
   - **یک کلید نشست. (به پیشنهاد KDC)**
   - **آی دی آلیس+کلید نشست رمز شده با کلید آلیس که به آن تیکت گوییم. (واضح است باب محتوای آن را نمی توان استخراج کند)**
3. **باب از پیام دریافتی از KDC کلید نشست و تیکت را استخراج می کند.**

نقش KDC تمام می شود.

nastooh@aut.ac.ir

احراز هویت

- احراز هویت بر اساس مرکز توزیع کلید
  - یک پروتکل عملیاتی شده مبتنی بر KDC: **نیدهام-شرودر**

4. **باب یک رشته تصادفی جدید و شناسه خود را با کلید نشست رمز کرده و به همراه تیکت(باز نشده) برای آلیس ارسال می کند.**
5. **آلیس به کمک کلید خودش، تیکت را رمزگشایی کرده و کلید نشست را استخراج کرده و شناسه باب را میبیند. (آلیس هویت باب را درک کرد)**
6. **آلیس با کمک کلید نشست (بازیابی شده از داخل تیکت)، رشته تصادفی باب رو استخراج می کند.**
7. **آلیس یک واحد از رشته تصادفی باب کسر کرده و با کلید نشست رمز کرده و برای باب ارسال می کند به همراه یک رشته تصادفی جدید.**
   - **کسر یک واحد برای جلوگیری از حملهٔ تکرار است.**
8. **باب نیز پس از رمزگشایی رشته تصادفی آلیس، یک واحد از آن کسر کرده و با کلید نشست رمز کرده و برای آلیس ارسال می کند.**
   - **تا آلیس متوجه به روز بودن این نشست جاری شود.**

nastooh@aut.ac.ir

احراز هویت

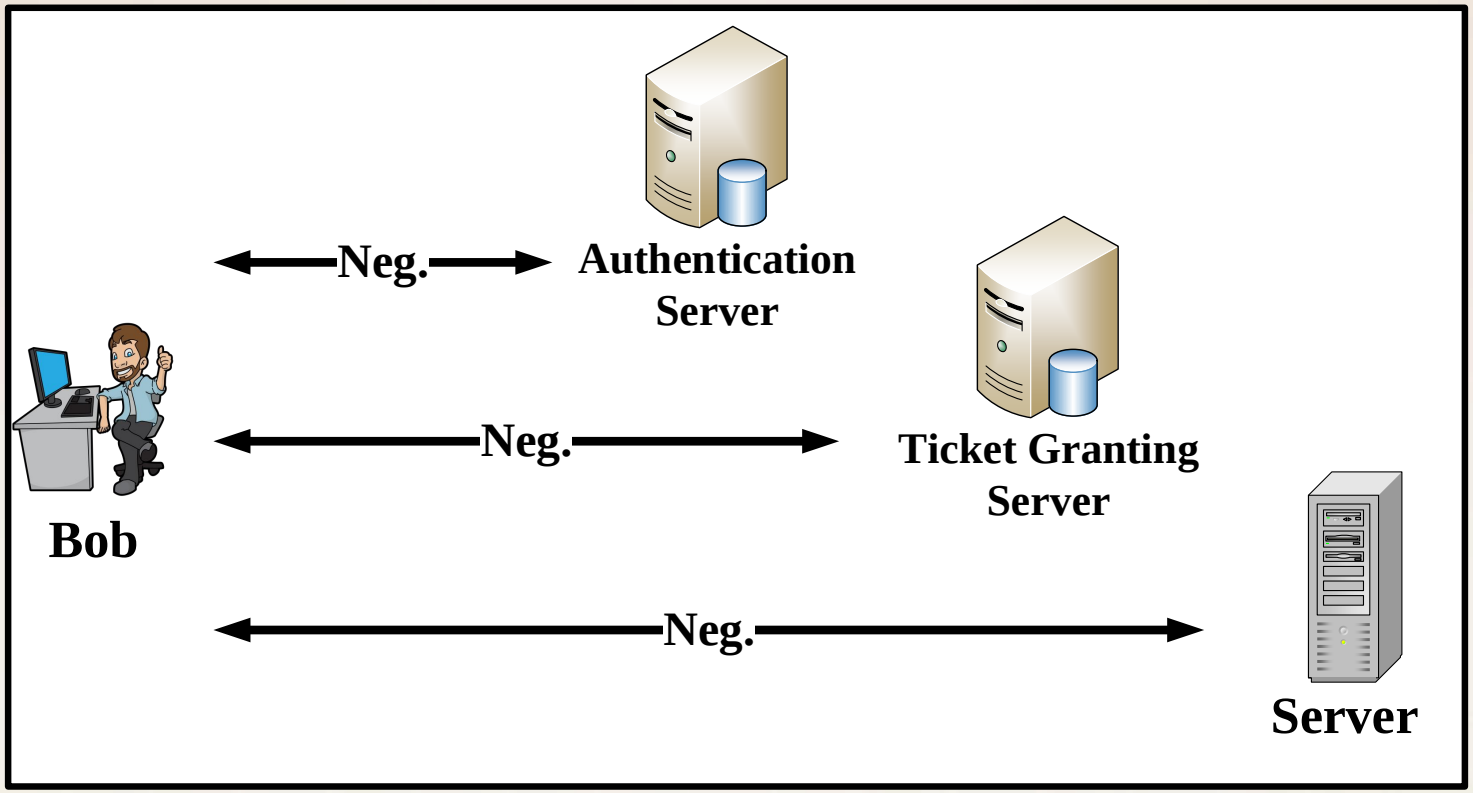
- پروتکل Kerberos
  - مبتنی بر پروتکل نیدهام-شرودر
  - معرفی شده در دانشگاه MIT اواسط دهل هشتاد میلادی
  - استفادهٔ موثری در ویندوزهای سرور و لینوکس
  - نسخهٔ ۵ آن در سال ۲۰۰۵ توسط IETF معرفی شد.
  - در اساطیر یونانی، کربروس یک اژدها (سگ)ی سه سر است که از دروازه های جهنم نگهبانی می کند تا کسی به آن وارد نشود!!! ☺

nastooh@aut.ac.ir

احراز هویت

- پروتکل Kerberos

شمای کلی سرورهای سه گانهٔ کربروس



nastooh@aut.ac.ir

احراز هویت

- پروتکل Kerberos به بیان بسیار ساده

گام اول: احراز هویت با AS

سرور AS همانند یک KDC عمل کرده و کاربر را احراز هویت کرده
و یک کلید نشست و یک تیکت برای سرورِ TGS برای کاربر صادر می کند.

گام دوم: دریافت مجوز از TGS

کاربر با کمک تیکتی که از AS گرفته است از طریق TGS برای هر یک از سرورهای شبکه که نیاز دارد یک کلید نشست خاص آن سرور دریافت می کند.

گام سوم:

سرویس دهندهٔ نهایی، با کمک کلید نشست خاص، کاربر را شناسایی کرده و نشست نهایی برقرار می شود.

جزئیات پروتکل کربروس را با دقت بررسی کنید.

nastooh@aut.ac.ir

منابع

[1] William Stallings, “Cryptography and Network Security,” 7th ed.

nastooh@aut.ac.ir

پایان

nastooh@aut.ac.ir