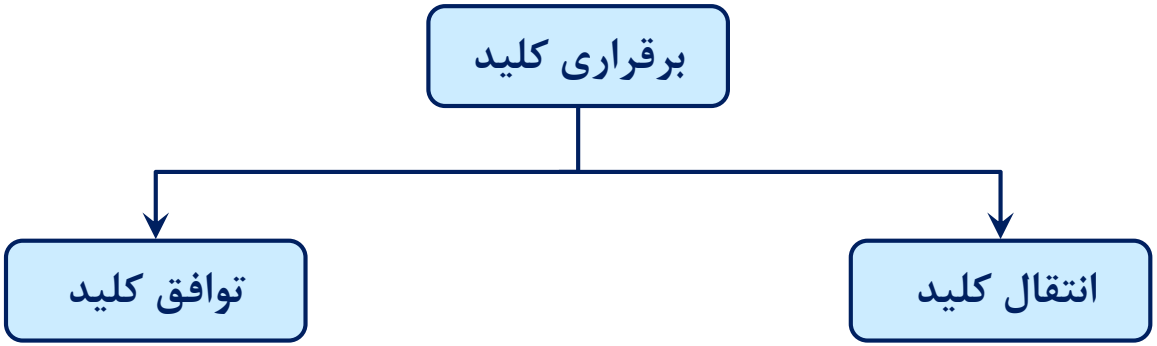
مدیریت کلید

- برقراری کلید (Key Establishment)
  - هدف
    - به اشتراک‌گذاری یک کلید سری بین دو یا چند طرف
  - دسته‌بندی پروتکل‌های برقراری کلید
    - انتقال کلید (Key Transport)
    - توافق کلید (Key Agreement)



مدیریت کلید

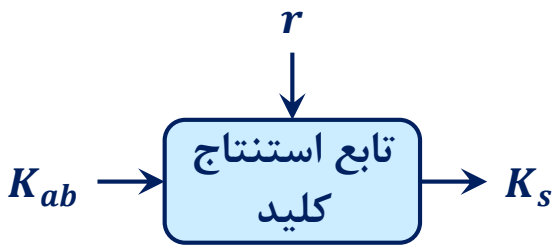
- پروتکل‌های انتقال کلید
  - یکی از طرفین پروتکل یک کلید سری تولید کرده و به طور امن بین سایر طرفین پروتکل توزیع می‌کند
- پروتکل‌های توافق کلید
  - طرفین پروتکل با همکاری هم یک کلید سری تولید می‌کنند
- انواع کلیدهای سری
- کلیدهای سری با طول عمر طولانی (Long-term Keys)
- کلیدهای نشست (Session Keys)
  - هر کلید نشست تنها برای مدت زمان محدودی معتبر است

کلیدهای نشست

- مزایای استفاده از کلیدهای نشست
  - در صورت افشای یک کلید نشست خسارت کم‌تری وارد می‌شود
  - به دلیل این که متن‌های رمز شده کم‌تری با استفاده از یک کلید نشست تولید می‌شود، بنابراین امکان انجام حمله‌های رمزنگاری کاهش می‌یابد
- ویژگی Perfect Forward Secrecy (PFS)
  - یک پروتکل برقراری کلید از ویژگی PFS برخوردار است اگر افشای کلیدهای سری با طول عمر طولانی باعث نشود که مهاجم بتواند کلیدهای نشست قبلی را به دست آورد

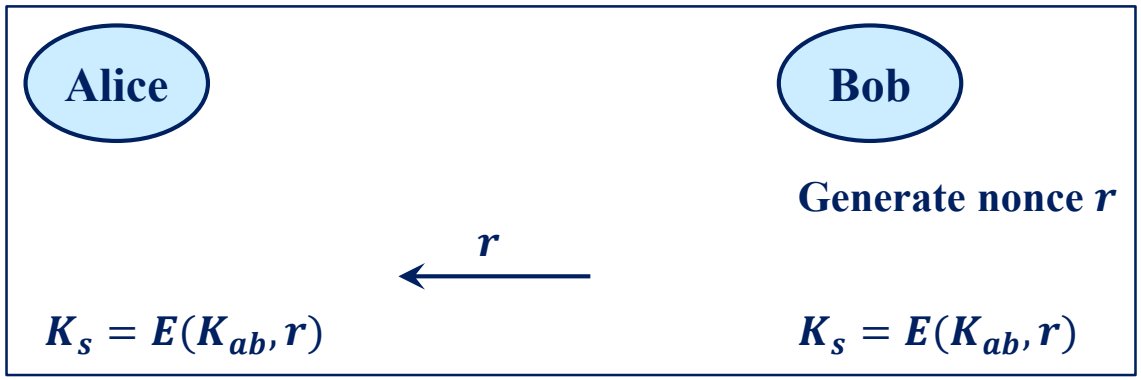
کلیدهای نشست

- استنتاج کلیدهای نشست
  - با فرض این که بین آلیس و باب کلید سری K_{ab} به اشتراک گذاشته شده باشد
    - تابع استنتاج کلید (KDF)
    - کلید نشست
      - K_s



کلیدهای نشست

- پروتکل استنتاج کلید نشست
  - نانس
    - r
  - کلید نشست
    - K_s



مدیریت کلید

- مساله توزیع n^2 کلید
  - با فرض این که در یک شبکه n کاربر وجود داشته باشد و هر کاربر تصمیم بگیرد ارتباطات امن جداگانه‌ای را با سایر کاربران برقرار کند
    - هر کاربر باید $n-1$ کلید سری ذخیره کند
    - $n(n-1)/2$ کلید سری متفاوت در شبکه وجود خواهد داشت
    - هر کاربر جدید برای توزیع کلیدهای سری مشترک باید با هر یک از کاربران دیگر یک کانال امن برقرار کند
  - مثال
    - در یک شبکه با 750 کاربر
      - تعداد کل کلیدهای سری
      - $(750 \times 749)/2 = 280875$

برقراری کلید با الگوریتم‌های رمز متقارن

- مرکز توزیع کلید (KDC)
  - یک سرویس‌دهنده مورد اعتماد که با هر کاربر یک کلید سری به اشتراک می‌گذارد
    - کلید رمزگذاری کلید (KEK)
    - یک کلید سری با طول عمر طولانی که برای ارسال امن کلیدهای نشست به کاربران مورد استفاده قرار می‌گیرد
- مزایای پروتکل‌های انتقال کلید مبتنی بر مرکز توزیع کلید
  - هر کاربر تنها باید یک کلید سری یعنی کلید رمزگذاری کلید خود را ذخیره کند
  - هر کاربر جدید برای توزیع کلید رمزگذاری کلید خود تنها باید یک کانال امن با مرکز توزیع کلید برقرار کند

برقراری کلید با الگوریتم‌های رمز کلید عمومی

- پروتکل مبادله کلید دیفی–هلمن با گواهی‌نامه‌ها
  - با فرض این که Z_p^* یک گروه دوری و g مولد گروه باشد