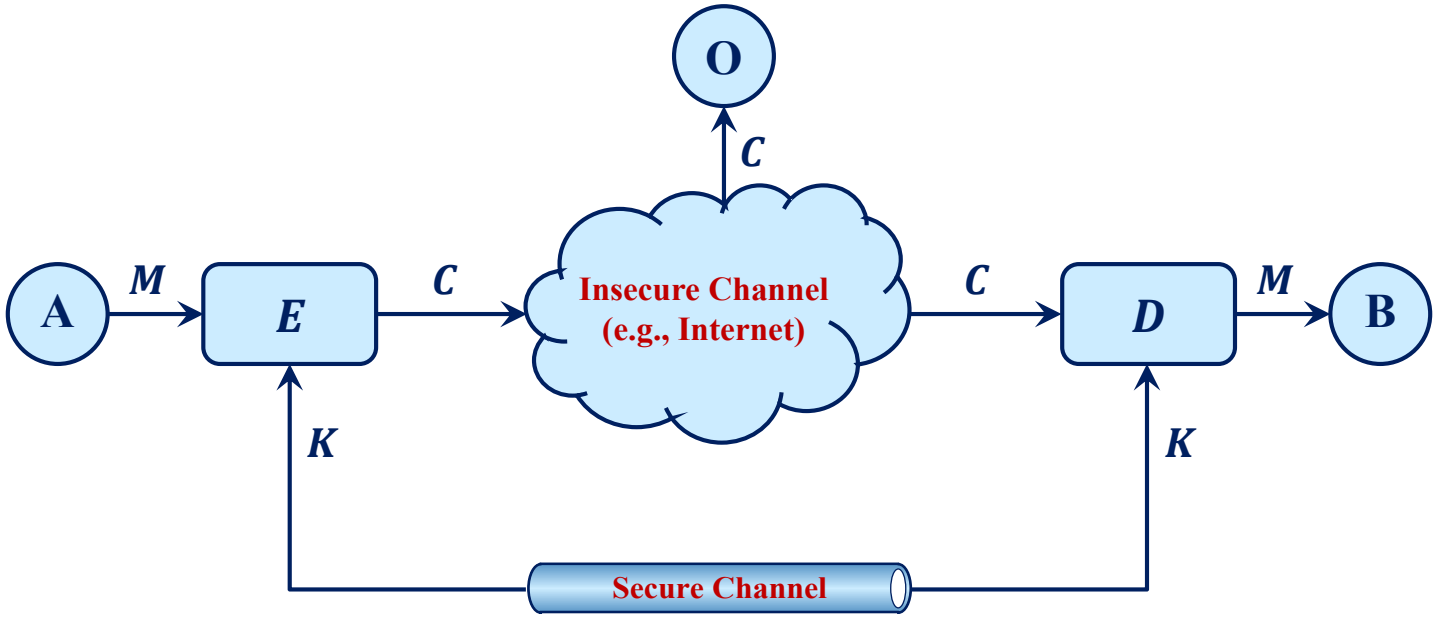
الگوریتم‌های رمز متقارن



- طرفین پروتکل
  - آلیس (A)
  - باب (B)
- شنودکننده
  - اسکار (O)
- توابع
  - رمزگذاری (E)
  - رمزگشایی (D)

الگوریتم‌های رمز متقارن

- فرض کنید در یک شبکه کامپیوتری بین هر دو میزبان یک کلید متفاوت به اشتراک گذاشته شود
  - تعداد کل میزبان‌ها
    - n
  - تعداد کل کلیدها
    - $n(n-1)/2$
  - مثال
    - ۱۰ میزبان
      - ۴۵ کلید متفاوت
    - ۱۰۰ میزبان
      - ۴۹۵۰ کلید متفاوت

الگوریتم‌های رمز کلید عمومی

- برای هر یک از طرفین پروتکل یک زوج کلید تولید می‌شود
  - کلید خصوصی (Private Key)
  - کلید عمومی (Public Key)
- فرضیات
  - هر پیام دلخواه را می‌توان با کلید عمومی رمز کرد
  - هر پیام دلخواه رمز شده با کلید عمومی را فقط با کلید خصوصی می‌توان رمزگشایی کرد
  - استنتاج کلید خصوصی از روی کلید عمومی از نظر محاسباتی غیرممکن است

الگوریتم‌های رمز کلید عمومی

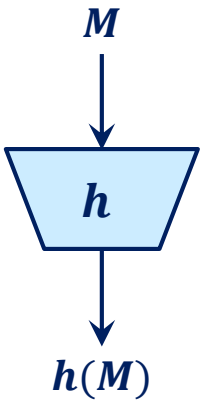
- **مثال**
  - فرض کنید کلید خصوصی باب KR_b و کلید عمومی وی KU_b باشد
  - آلیس قصد دارد پیام محرمانه M را برای باب ارسال کند
    - باب
      - ارسال کلید عمومی KU_b به آلیس
    - آلیس
      - رمزگذاری پیام M با استفاده از کلید عمومی KU_b
      - ارسال پیام رمز شده C از طریق یک کانال ناامن
    - باب
      - دریافت پیام C و رمزگشایی آن با استفاده از کلید خصوصی KR_b

توابع یک طرفه

- تابع f یک تابع یک طرفه نامیده می‌شود اگر برای هر x محاسبه $y = f(x)$ از نظر محاسباتی آسان و محاسبه $x = f^{-1}(y)$ از نظر محاسباتی غیرممکن باشد
  - f^{-1}
    - وارون تابع f
- مثال
  - مساله تجزیه اعداد به عوامل اول
  - مساله لگاریتم گسسته

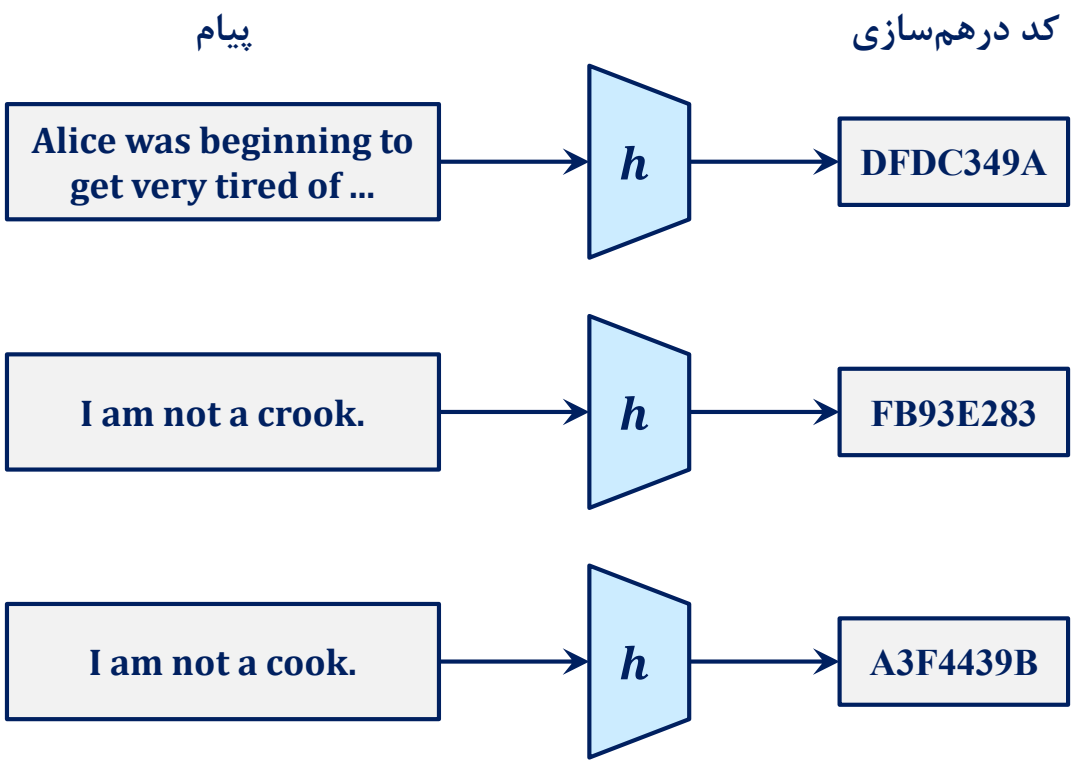
توابع درهم‌سازی

- **تابع درهم‌سازی یک طرفه**
  - **نوعی تابع یک طرفه که هر پیام با طول متغیر را به یک مقدار درهم‌سازی با طول ثابت نگاشت می‌کند**
    - **طول ورودی**
      - **متغیر**
    - **طول خروجی**
      - **ثابت**



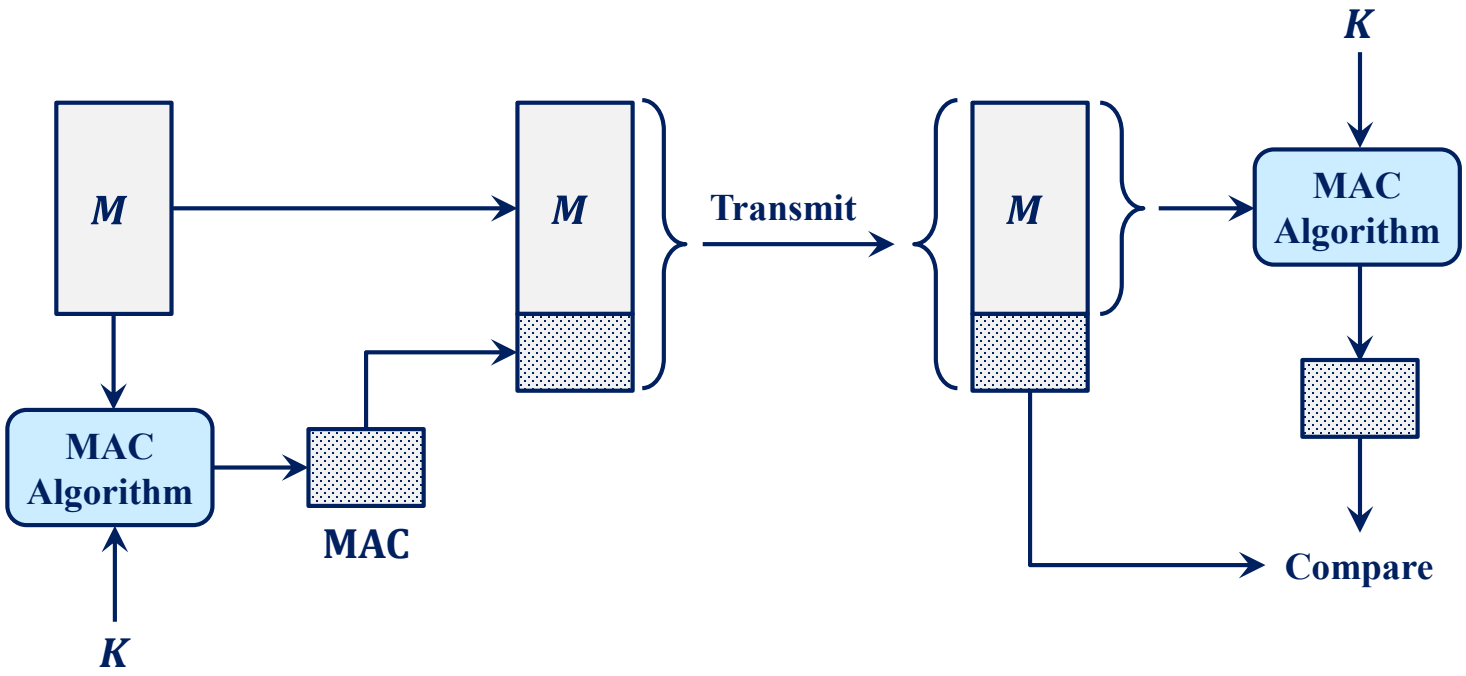
توابع درهم‌سازی

- مثال



کدهای تصدیق اصالت پیام

- کد تصدیق اصالت پیام (MAC)
  - تابعی از پیام و یک کلید سری



امضاهای دیجیتالی

- ویژگی‌های امضا
  - امضا دارای اصالت است
  - امکان جعل امضا وجود ندارد
  - امضا غیرقابل استفاده مجدد است
  - متن امضا شده غیرقابل تغییر است
  - امضا غیرقابل انکار است
- سرویس‌های امنیتی
  - تصدیق اصالت پیام
  - عدم انکار

امضاهای دیجیتالی

- امضای پیام‌ها با استفاده از الگوریتم‌های رمز کلید عمومی
  - دو مرحله
    - امضا
      - کلید خصوصی
    - درستی‌سنجی
      - کلید عمومی
  - الگوریتم‌های رمز کلید عمومی
    - RSA
    - DSA

امضاهای دیجیتالی

- مثال
  - فرض کنید کلید خصوصی آلیس KR_a و کلید عمومی وی KU_a باشد
  - آلیس قصد دارد پیام M را امضا کرده و برای باب ارسال کند
    - آلیس
      - رمزگذاری پیام M با استفاده از کلید خصوصی KR_a و ایجاد پیام امضا شده $S(KR_a,M)$
      - ارسال پیام $S(KR_a,M)$ به باب
    - باب
      - رمزگشایی پیام $S(KR_a,M)$ با استفاده از کلید عمومی KU_a
      - درستی‌سنجی امضا

امضاهای دیجیتالی

- امضای پیام‌ها با استفاده از الگوریتم‌های رمز کلید عمومی و توابع درهم‌سازی یک طرفه
  - مثال
    - آلیس قصد دارد پیام M را امضا کرده و برای باب ارسال کند
      - آلیس
        - ایجاد کد درهم‌سازی $h(M)$
        - رمزگذاری کد درهم‌سازی $h(M)$ با استفاده از کلید خصوصی KR_a
        - ارسال پیام M و کد درهم‌سازی رمز شده $S(KR_a,h(M))$ به باب
      - باب
        - رمزگشایی کد درهم‌سازی رمز شده $S(KR_a,h(M))$ با استفاده از کلید عمومی KU_a
        - درستی‌سنجی امضا