دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکدهٔ مهندسی کامپیوتر و فنآوری اطلاعات

مبانی امنیت اطلاعات

(ترم بهمن ۹۸)

Digital Signature

نستوه طاهری جوان

nastooh@aut.ac.ir

امضای دیجیتال

- ✓ کاربردهای امضای فیزیکی (دستنویس):
  - تصدیق اصالت (احراز هویت)
  - انکار ناپذیری
- ✓ دلایل اقبال و اعتماد به امضای فیزیکی:
  - سادگی تولید.
  - سادگی تشخیص.
    - از روی خصیصه های فیزیکی، مانند اندازه، زاویه، تناسب، فشار روی کاغذ و و و
  - مشکل بودن جعل.

nastooh@aut.ac.ir

امضای دیجیتال

- در یک کلام، دلیل به کاربردن امضای فیزیکی:
  تفاوت کپی و اصل آن

اما در دنیای دیجیتال مفاهیم مطرح شده معنا ندارند و کپی و اصل یکسانند.

nastooh@aut.ac.ir

امضای دیجیتال مبتنی بر کلید عمومی

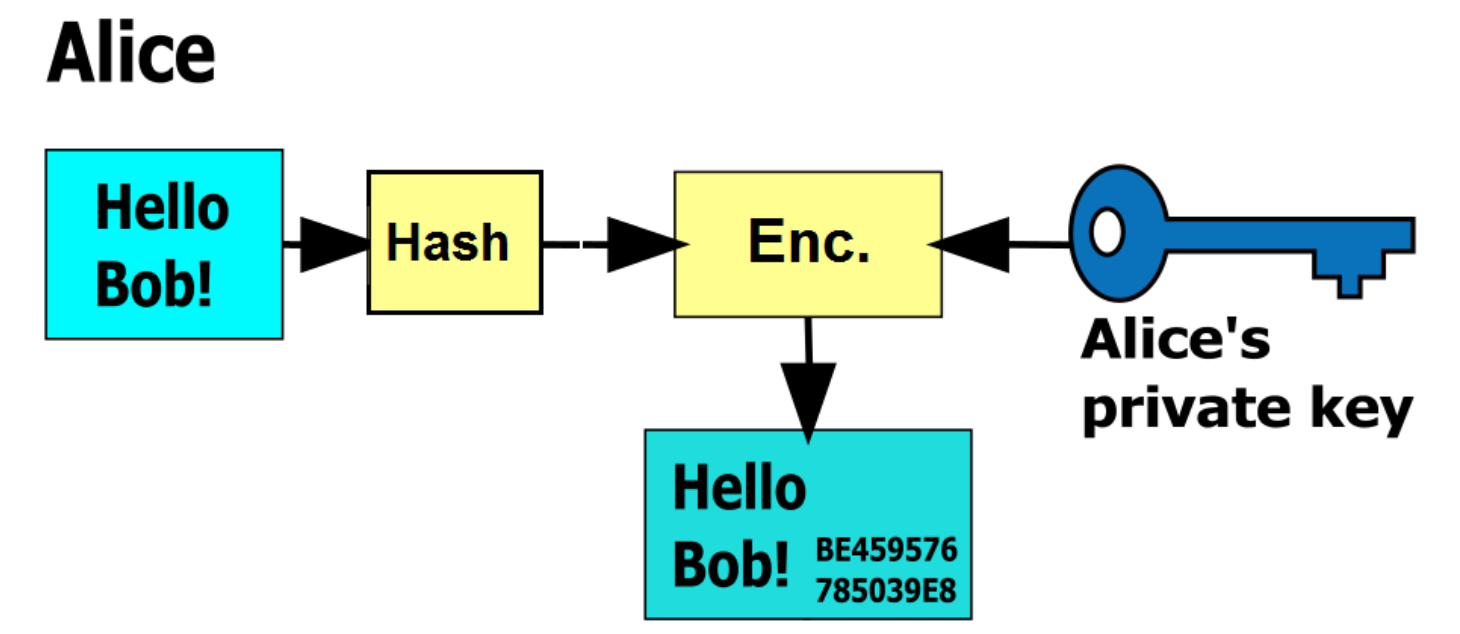
- ✓ تولید امضا:
  - گام اول: فرستند از دادهٔ اصلی، یک خلاصه تهیه میکند.
    - مثلا با یک الگوریتم درهم ساز استاندارد.
  - گام دوم: فرستنده خلاصهٔ پیام را با استفاده از کلیدخصوصی اش رمز میکند.
    - اولین بار است که با کلید خصوصی رمزگذاری می کنیم!!!
    - مثلا به کمک الگوریتم RSA.
    - خروجی این گام، عملا امضای دیجیتال سند مذکور است.

امضای تولید شده در مرحلهٔ دوم، به همراه اصل داده برای گیرنده رسال می گردد.

nastooh@aut.ac.ir

امضای دیجیتال مبتنی بر کلید عمومی

✓ تولید امضا:



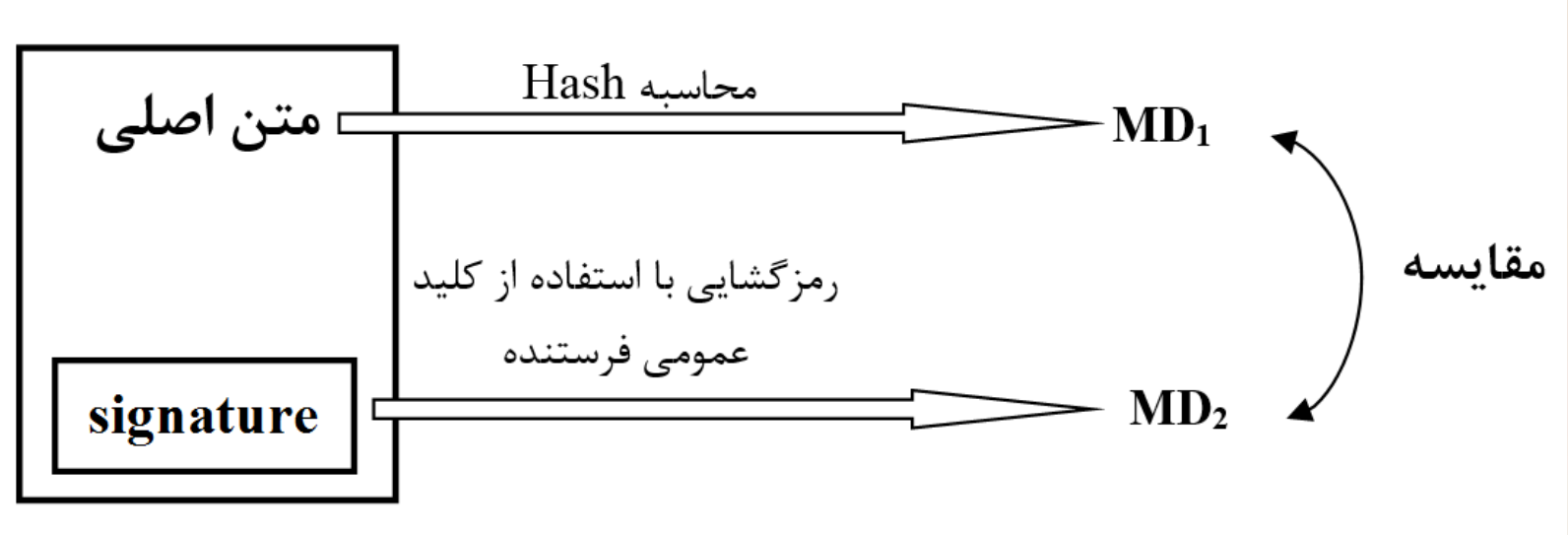
nastooh@aut.ac.ir

امضای دیجیتال مبتنی بر کلید عمومی

- ✓ بررسی صحت امضا در گیرنده:
  - گام اول: جدا کردن امضا از متن اصلی
  - گام دوم: محاسبهٔ خلاصه از روی دادهٔ دریافتی
    - توسط الگوریتم یکسان با مبدا
  - گام سوم: رمزگشایی امضای دریافتی به کمک کلید عمومی فرستنده
  - گام چهارم: مقایسهٔ نتایج گام دوم و سوم

امضای دیجیتال مبتنی بر کلید عمومی

✓ بررسی صحت امضا در گیرنده:



بررسی امکان جعل، توسط ترودی؟

nastooh@aut.ac.ir

امضای دیجیتال مبتنی بر کلید عمومی

- ✓ خصوصیات امضای دیجیتال:
  - بررسی امکان جعل، توسط ترودی
  - چگونگی ارضای انکار ناپذیری
  - چگونگی ارضای احراز هویت
  - مشکل ذاتی PKC:
    - اعتبارسنجی کلیدهای عمومی/خصوصی

MAC

- ✓ کدهای MAC (Message Authentication Code)
  - ○ هدف: احراز سلامت و هویت پیام
    - در واقع نوعی امضای دیجیتال ساده، بدون استفاده از رمزنگاری های متداول
  - ○ کاربرد: عموما بررسی سلامت و هویت بسته های شبکه
    - مثلا کاربرد HMAC در IPsec
  - ○ خصوصیات:
    - مبتنی بر یک رشتهٔ مشترک و سری
    - مبتنی بر توابع درهم ساز
    - بسیار ساده تر و سریع تر از امضای دیجیتال

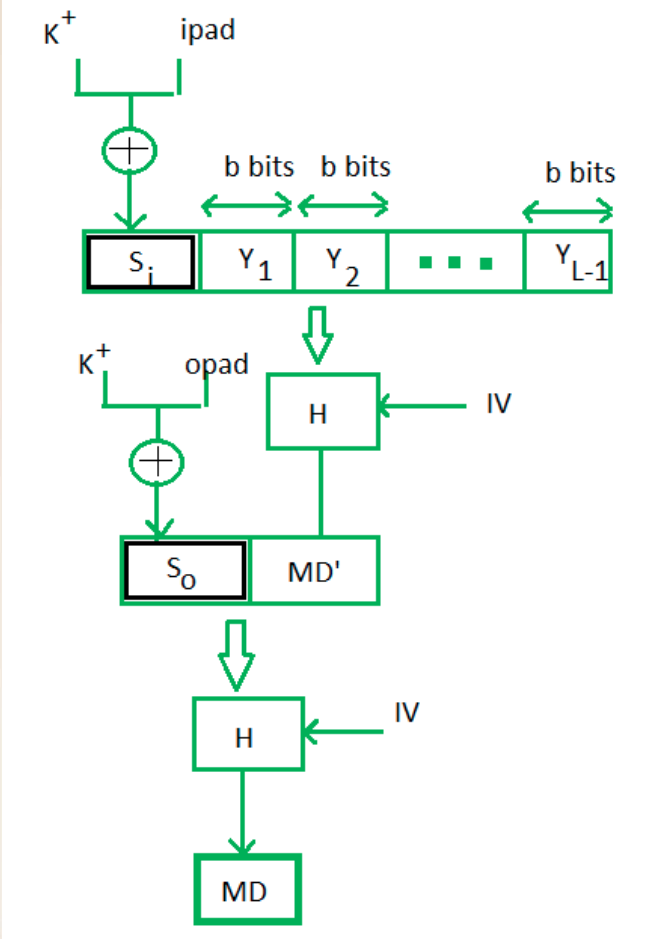
HMAC

- ✓ معرفی HMAC (Hashed MAC)
  - روال کار
    - توافق بین یک کلید مشترک و سری
    - Xor کردن کلید با یک رشتهٔ ثابت $ipad=363636\ldots_{Hex}$
      - طول رشتهٔ ثابت به اندازهٔ طول قطعه است.
    - الحاق نتیجهٔ Xor به ابتدای کل پیام
      - پیام اصلی می تواند هر طولی داشته باشد.
    - محاسبهٔ چکیدهٔ کل پیام به کمک یک تابع درهم ساز، مثلا SHA1
    - Xor کردن کلید با یک رشتهٔ ثابت $opad=5C5C5C\ldots_{Hex}$
    - الحاق نتیجهٔ Xor به ابتدای پیام (چکیدهٔ قبلی)
    - محاسبهٔ چکیدهٔ پیام به کمک همان تابع درهم ساز.

nastooh@aut.ac.ir

HMAC

✓ معرفی HMAC (Hashed MAC)



- H: تابع درهم ساز
- K^+: کلید توافق شده

nastooh@aut.ac.ir

منابع

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

nastooh@aut.ac.ir

پایان

nastooh@aut.ac.ir