به نام خداوند بخشنده مهربان

مبانی امنیت شبکه

Fundamentals of Network Security



یاشار ابری

دانشکده مهندسی، دانشگاه تهران

Yasharabri.ut.ac.ir@gmail.com

yasharabri@ut.ac.ir

۱۰ کد احراز اصالت پیام و امضای دیجیتال

- سرفصل‌های این بخش:
  - چرا Hash به‌تنهایی کافی نیست: MAC و HMAC
  - رمزنگاری احراز اصالت‌شده (AEAD)
  - امضای دیجیتال و استاندارد DSS

چرا Hash به‌تنهایی کافی نیست؟

- **مشکل:** اگر مهاجم بتواند هم پیام و هم هش Hash آن را دستکاری کند (چون هر دو بدون کلید محرمانه محاسبه می‌شوند)، گیرنده متوجه تغییر نمی‌شود.
- **راه‌حل: MAC:** کد احراز اصالت پیام با ترکیب یک کلید محرمانه مشترک با محتوای پیام تولید می‌شود؛ فقط کسی که کلید را دارد می‌تواند MAC معتبر بسازد یا تأیید کند، بنابراین هم جامعیت و هم اصالت فرستنده تضمین می‌شود.
- **HMAC:** رایج‌ترین روش ساخت MAC از یک تابع Hash موجود است؛ HMAC با ترکیب هوشمندانه کلید در دو مرحله جداگانه Hash، در برابر حملات شناخته‌شده روی توابع Hash زیرین نیز مقاوم است.

امیرالمومنین علی علیه السلام:
هوای نفس، دشمن خرد است.
شرح غرر: ج۱، ص۶۸

رمزنگاری احراز اصالت‌شده (AEAD)

- **خلأ رمزگذاری ساده:** یک الگوریتم رمزگذاری معمولی فقط محرمانگی می‌دهد؛ مهاجم می‌تواند بدون دانستن کلید، بیت‌های متن رمز را دستکاری کند و نتیجه رمزگشایی نامعتبر اما نامشخص تولید شود.
- **راه‌حل: رمزگذاری + احراز اصالت هم‌زمان:** حالت‌هایی مانند GCM و CCM هم‌زمان با رمزگذاری، یک برچسب احراز اصالت (Tag) نیز تولید می‌کنند تا هرگونه دستکاری در متن رمز، در زمان رمزگشایی بلافاصله شناسایی شود.
- **جایگاه امروزی:** AES-GCM و ChaCha۲۰-Poly۱۳۰۵ امروزه استاندارد پیش‌فرض در TLS ۱.۳ هستند، دقیقاً به این دلیل که هر دو نیاز محرمانگی و جامعیت را در یک مرحله و با کارایی بالا تأمین می‌کنند.

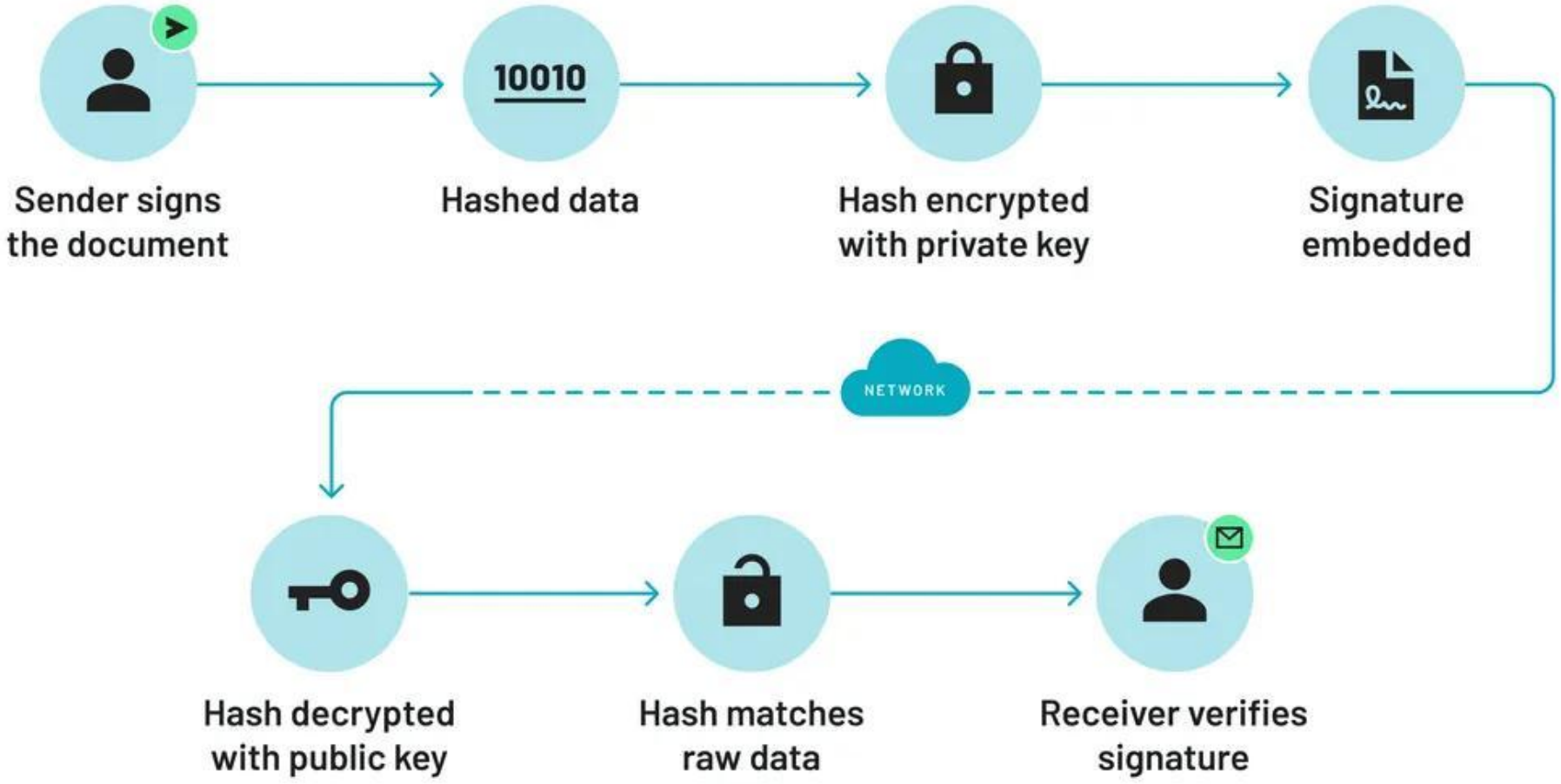
امام حسن مجتبی علیه السلام:
بزرگواری، احسان کردن داوطلبانه است و دَهِش پیش از خواهش.
بحار الأنوار: ج۴۴، ص۸۹، ح۲

امضای دیجیتال

- **شبیه‌سازی امضای دستی:** امضای دیجیتال باید ویژگی‌های امضای دستی را داشته باشد: فقط صاحب کلید بتواند آن را تولید کند، هرکسی بتواند صحت آن را بررسی کند و امکان انکار امضا از سوی امضاکننده وجود نداشته باشد.
- **مکانیزم کار:** ابتدا از پیام یک هش Hash گرفته می‌شود و سپس همان هش کوچک با کلید خصوصی امضاکننده رمز می‌شود؛ گیرنده با کلید عمومی امضاکننده، امضا را باز کرده و با هش‌ای که خودش از پیام محاسبه می‌کند مقایسه می‌کند.
- **استانداردها:** استاندارد امضای دیجیتال (DSS) الگوریتم‌های DSA و ECDSA (نسخه مبتنی بر منحنی بیضوی) را تعریف می‌کند؛ ECDSA به دلیل کلید کوچک‌تر امروزه در گواهی‌های وب و ارزهای دیجیتال بسیار رایج است.

امیرالمومنین علی علیه السلام فرمود:
منتظر فرج باشید، و از روح خدا مأیوس نشوید، که محبوب‌ترین اعمال در پیشگاه خدا انتظار فرج است.
بحارالأنوار، ج۵۱، ص ۱۲۳
.

نحوه کارکرد امضای دیجیتال



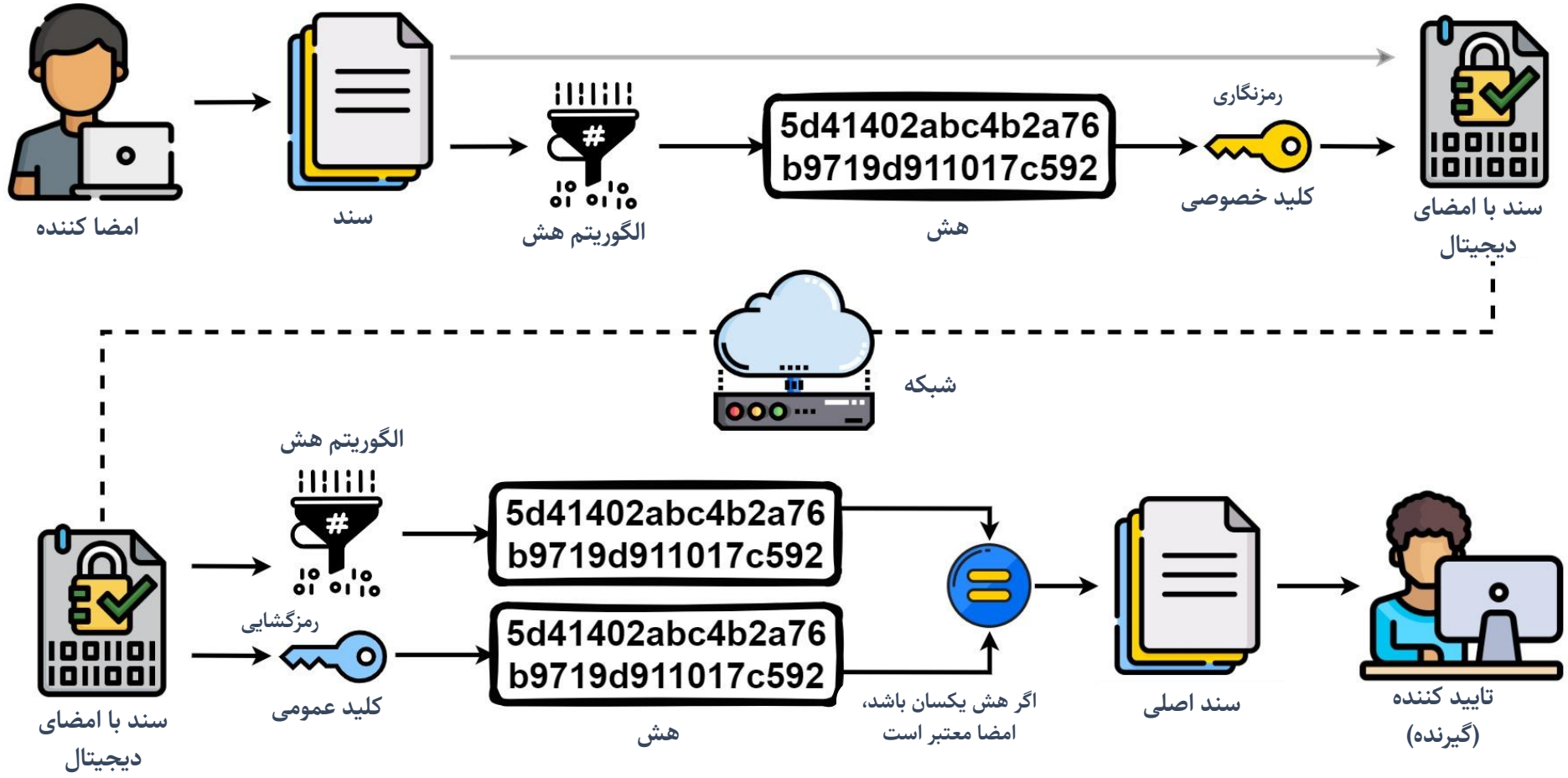
مردی از امیرالمومنین علی علیه السلام سئوال کرد:

محبوب‌ترین اعمال پیش خدا کدام است؟

امیرالمومنین علیه‌السلام فرمود: انتظار فرج.

بحارالأنوار، ج۵۲، ص ۱۲۲

جریان امضای دیجیتال از پیام تا هش Hash، رمزگذاری با کلید خصوصی و تأیید با کلید عمومی



امیرالمومنین علی علیه السلام :

عملت را دوستِ خود، و آرزویت را دشمن خود قرار ده.

شرح غرر: ج ۲، ص ۱۸۲