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

۸

دیفی-هلمن، منحنی بیضوی و رمزنگاری پسا-کوانتومی

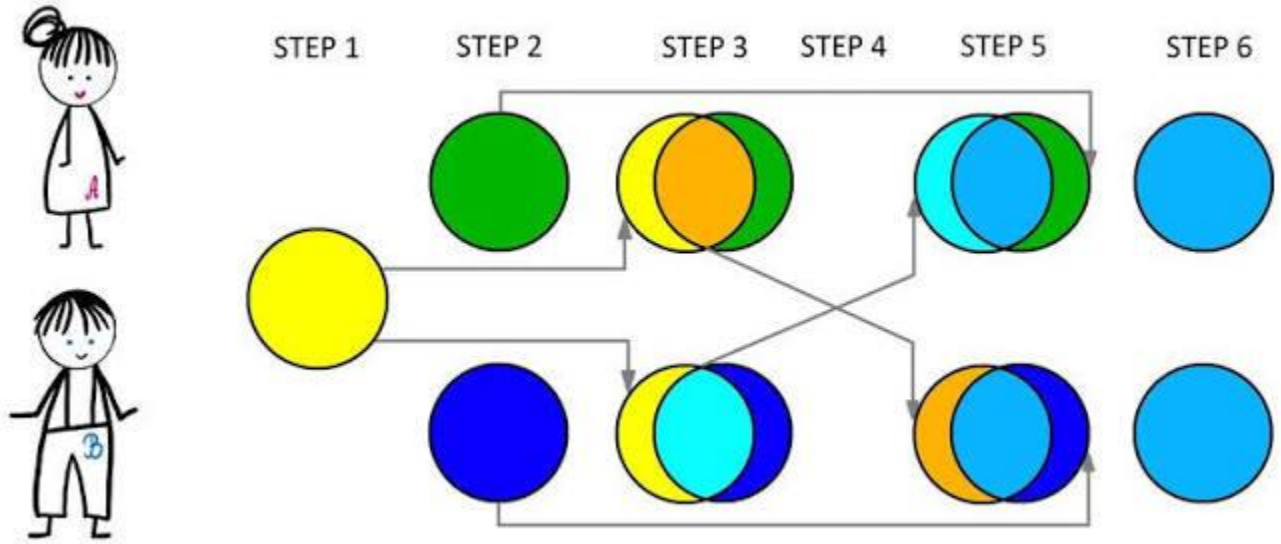
- سرفصل‌های این بخش:
  - تبادل کلید دیفی-هلمن
  - رمزنگاری منحنی بیضوی (ECC)
  - به‌روزرسانی: تهدید کوانتومی و استانداردهای NIST۲۰۲۴

تبادل کلید دیفی-هلمن

- **مسئله:** دو طرف که هیچ کلید مشترک قبلی ندارند و فقط از طریق کانالی ناامن ارتباط دارند، چگونه می‌توانند به یک کلید محرمانه مشترک برسند؟
- **تمثیل رنگ‌آمیزی:** هرکدام یک رنگ پایه مشترک (عمومی) را با یک رنگ محرمانه خودشان مخلوط کرده و نتیجه را رد و بدل می‌کنند؛ سپس هرکدام رنگ دریافتی را دوباره با رنگ محرمانه خودش مخلوط می‌کند و هر دو به یک رنگ نهایی یکسان می‌رسند، بدون این‌که رنگ‌های محرمانه اصلی هرگز فاش شده باشند.
- **پایه ریاضی:** همین ایده با توان‌رسانی پیمانه‌ای پیاده‌سازی می‌شود؛ امنیت آن به دشواری مسئله لگاریتم گسسته وابسته است.
- **نقطه ضعف بدون احراز اصالت:** این پروتکل به‌تنهایی هویت طرفین را تأیید نمی‌کند، بنابراین در برابر حمله مرد میانی آسیب‌پذیر است؛ به همین دلیل در عمل همیشه با یک مکانیزم احراز اصالت (مانند گواهی دیجیتال) همراه می‌شود.

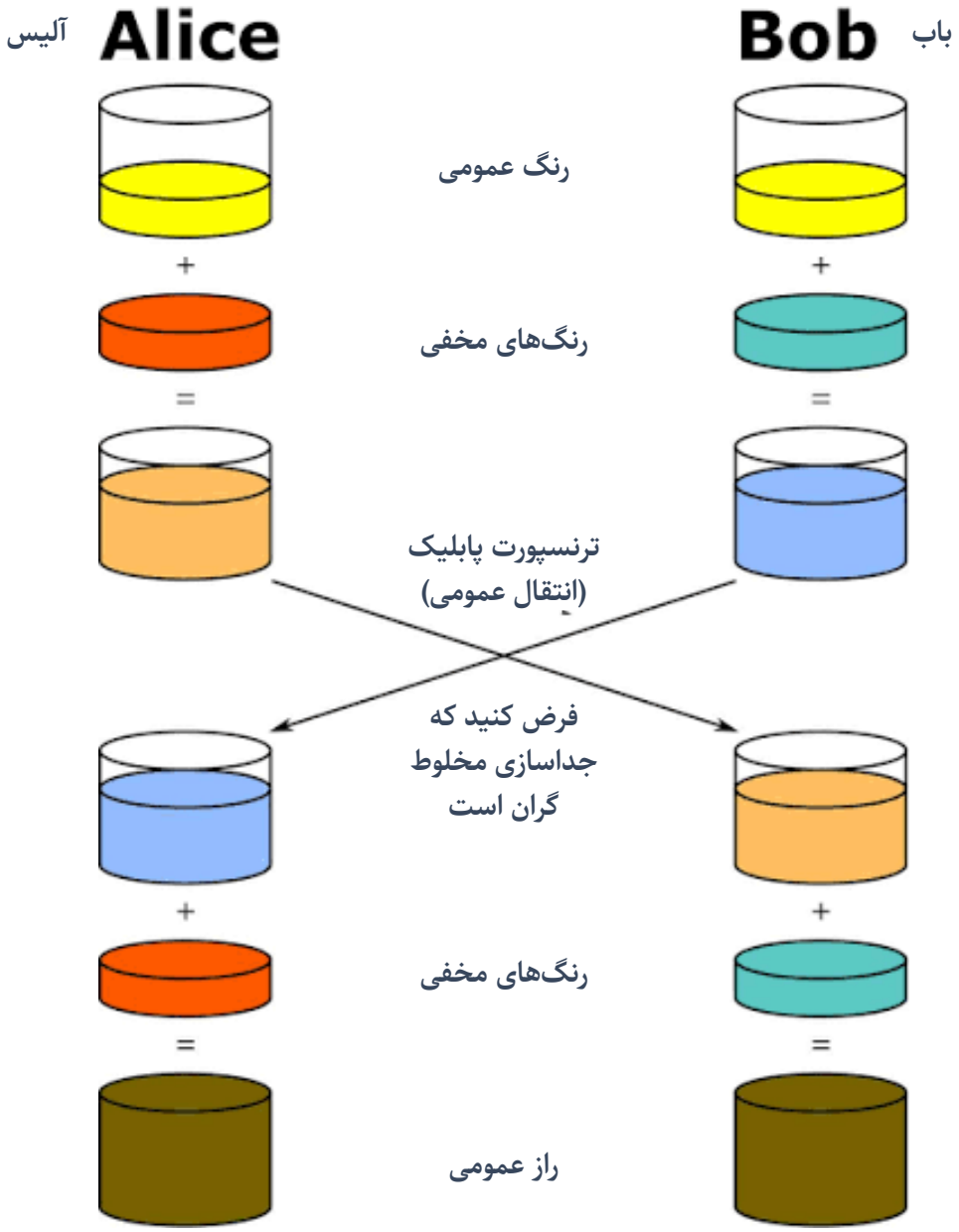
امام باقر (علیه السلام):
سخن طیّب و پاکیزه را از هر که گفت بگیرید، اگرچه او خود، بدان عمل نکند.
تحف العقول, ص ۲۹۱

نمودار تمثیل رنگ‌آمیزی دیفی-هلمن با رنگ پایه مشترک و رنگ‌های محرمانه هر طرف



امام باقر (علیه السلام):
چیزی با چیزی نیامیزد که بهتر از حلم با علم باشد.
«ماشیبَ شَیْءٌ بِشَیْء أَحْسَنَ مِنْ حِلْم بِعِلْم.»
تحف العقول, ص ۲۹۲

نمودار تمثیل رنگ‌آمیزی دیفی-هلمن با رنگ پایه مشترک و رنگ‌های محرمانه هر طرف



امام جواد علیه السلام:
همانا قائم ما مهدی علیه السلام است که بر مسلمان واجب است در زمان غیبت او منتظرش باشد و هنگام ظهورش از او اطاعت کند.
منتخب الأثر، ص ۲۲۳

پروتکل تبادل کلید دیفی-هلمن (Diffie-Hellman)

- **۱. هدف پروتکل:** ایجاد یک کلید مشترک محرمانه بین دو طرف (مثلاً آلیس و باب) از طریق یک کانال ارتباطی ناامن، بدون اینکه نیاز باشد کلید اصلی از قبل بین آن‌ها رد و بدل شده باشد.

- **۲. منطق ریاضی:** «یک‌طرفه بودن محاسبات»
  - امنیت این روش بر پایه دشواری یک مسئله ریاضی بنا شده است:
  - **محاسبات رو به جلو (آسان):** اگر پایه و توان را داشته باشیم، محاسبه باقیمانده تقسیم (Mod) بسیار سریع است.
  - **محاسبات رو به عقب (بسیار دشوار):** اگر فقط باقیمانده و پایه را داشته باشیم، پیدا کردن توان اصلی (مسئله لگاریتم گسسته) برای اعداد بزرگ، عملاً غیرممکن است.

امام رضا علیه السلام:
بی‌تردید ، خداوند عز و جل . . . انسان را به سپاس‌گزاری از خدا و پدر و مادر، فرمان داده است. پس کسی که سپاس‌گذارِ (قدرشناسِ) پدر و مادرش نباشد، از خدا سپاس‌گزاری نکرده است.
عیون أخبار الرضا علیه السلام: ج ۱، ص ۲۵۸، ح ۱۳

پروتکل تبادل کلید دیفی-هلمن (Diffie-Hellman)

۳. مراحل اجرا و نمادهای ریاضی:

- در این پروتکل، دو عدد عمومی (قابل مشاهده برای همه) انتخاب می‌شود: یک عدد پایه (g) و یک عدد پیمانه (p).

امام باقر علیه السلام :
هیچ عبادتی در روز جمعه نزد من دوست داشتنی تر از صلوات بر پیامبر و آل او نیست.
وسائل الشیعه ، ج ۷ ، ص ۳۸۸

پروتکل تبادل کلید دیفی-هلمن (Diffie-Hellman)

- **گام اول: تولید مقادیر خصوصی و عمومی**
  - هر طرف یک عدد مخفی برای خود انتخاب می‌کند و مقدار عمومی خود را محاسبه و ارسال می‌کند:
  - آلیس: یک عدد مخفی (a) انتخاب می‌کند و مقدار عمومی خود (A) را محاسبه می‌کند:

$$A = g^a \pmod p$$

(یعنی: gبه توان aتقسیم بر p، باقیمانده‌اش برابر است با A)

  - باب: یک عدد مخفی (b) انتخاب می‌کند و مقدار عمومی خود (B) را محاسبه می‌کند:

$$B = g^b \pmod p$$

(یعنی: gبه توان bتقسیم بر p، باقیمانده‌اش برابر است با B)

امام صادق علیه السلام: سه چیز از صفات خوب دنیا و آخرتند: گذشتن از کسی که به تو ستم کرده و پیوستن با آنکه از تو بریده و خویشتنداری زمانی که با تو نادانی کنند.

اصول کافی: ج۳، ص۱۶۷

پروتکل تبادل کلید دیفی-هلمن (Diffie-Hellman)

- **گام دوم: استخراج کلید مشترک**
  - هر طرف با ترکیب مقدار عمومی طرف مقابل و عدد مخفی خود، به یک نتیجه یکسان می‌رسد:
  - آلیس: کلید را با استفاده از مقدار عمومی باب محاسبه می‌کند:

$$K = B^a \pmod{p}$$

  - باب: کلید را با استفاده از مقدار عمومی آلیس محاسبه می‌کند:

$$K = A^b \pmod{p}$$

امام صادق علیه السلام:
دلها نیز، همچون مس،
زنگار می‌بندد، پس آنها را
با استغفار صیقل دهید.
عدّة الداعی، ص۲۴۹

پروتکل تبادل کلید دیفی-هلمن (Diffie-Hellman)

- **۴. نتیجه نهایی:**
  - به دلیل ویژگی‌های ریاضی توان، هر دو طرف به یک عدد کاملاً یکسان می‌رسند:

$$K = (g^b)^a \pmod p = (g^a)^b \pmod p$$

امیرالمومنین علی علیه السلام :

در هیچ یك از توشه های دنیا خیری نیست مگر در تقوا.

نهج البلاغة: خطبه ۱۱۱



پروتکل تبادل کلید دیفی-هلمن (Diffie-Hellman)

چرا شنودگر شکست می‌خورد؟

- شنودگر تمام مقادیر عمومی (g,p,A,B) را می‌بیند، اما برای رسیدن به کلید K، باید بتواند از طریق A یا B، به اعداد مخفی a یا b برسد؛ کاری که در اعداد بزرگ، از توان محاسباتی کامپیوترها خارج است.

امام صادق علیه السلام:
اگر او [امام زمان علیه السلام] را دریابم، تمام عمر به او خدمت می‌کنم.
الغیبه نعمانی، ص ۲۴۵

رمزنگاری منحنی بیضوی (ECC)

- **انگیزه پیدایش:** با رشد استفاده از تلفن‌های همراه و دستگاه‌های محدود از نظر توان پردازشی و باتری، نیاز به الگوریتمی با امنیت بالا اما کلید کوچک‌تر از RSA احساس شد.
- **پایه ریاضی متفاوت:** به‌جای تجزیه اعداد، ECC بر پایه دشواری مسئله لگاریتم گسسته روی نقاط یک منحنی بیضوی تعریف‌شده روی یک میدان متناهی بنا شده است.
- **مزیت اندازه کلید:** یک کلید ECC با طول ۲۵۶ بیت، امنیتی تقریباً معادل یک کلید RSA با طول ۳۰۷۲ بیت فراهم می‌کند؛ این یعنی محاسبات سریع‌تر و مصرف حافظه کمتر، به‌ویژه برای گوشی‌های هوشمند و دستگاه‌های اینترنت اشیا.

امیرالمومنین علی علیه السلام:
پاک‌کردن عمل [از ناخالصیها] از عمل ارزشمندتر است.
بحارالانوار: ج ۷۸، ص ۹۰

به‌روزرسانی: تهدید کوانتومی و رمزنگاری پسا-کوانتومی

- **چرا RSA و ECC تهدید می‌شوند:** الگوریتم شور نشان داده که یک کامپیوتر کوانتومی به‌اندازه کافی بزرگ می‌تواند مسئله تجزیه اعداد و لگاریتم گسسته را در زمان معقول حل کند و بنابراین کل رمزنگاری کلید عمومی امروزی را بشکند.
- **اقدام NIST:** پس از یک فرایند رقابتی هشت‌ساله، NIST در تاریخ ۱۳ اوت ۲۰۲۴ سه استاندارد رمزنگاری پسا-کوانتومی را نهایی کرد.

امام صادق علیه السلام:
در موردی که نیت و اراده آدمی قوی باشد، بدن دچار ضعف و ناتوانی نمی‌گردد.
وسائل الشیعه، ج ۱

استانداردهای پسا-کوانتومی NIST ۲۰۲۴

نام استاندارد	الگوریتم پیشین	پایه ریاضی و کاربرد
ML-KEM (FIPS 203)	CRYSTALS-Kyber	**مبتنی بر مسائل مشبکه (Lattice)؛ برای برقراری کلید مشترک –جایگزین دیفی-هلمن/RSA**
ML-DSA (FIPS 204)	CRYSTALS-Dilithium	**مبتنی بر مسائل مشبکه؛ الگوریتم عمومی امضای دیجیتال**
SLH-DSA (FIPS 205)	SPHINCS+	**مبتنی بر توابع درهم‌ساز؛ گزینه محافظه‌کارانه پشتیبان با مفروضات امنیتی متفاوت**

از امیرالمؤمنین علیه السلام نقل شده که فرمود:
کسی که منتظر امر و فرمان ما باشد، همانند کسی است که در راه خدا بخون خود غلتیده است.
منتخب الأثر/ ص ۴۹۶