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

# ۷ نظریه اعداد پیشرفته و رمزنگاری کلید عمومی

- سرفصل‌های این بخش:
  - اعداد اول و قضایای فرما و اویلر
  - چرا رمزنگاری کلید عمومی اختراع شد
  - الگوریتم RSA گام به گام

# اعداد اول و پایه‌های ریاضی RSA

- **نقش اعداد اول:** امنیت RSA بر این حقیقت استوار است که ضرب دو عدد اول بزرگ بسیار ساده، اما تجزیه حاصل‌ضرب آن‌ها به دو عدد اول اصلی از نظر محاسباتی بسیار دشوار است.
- **قضیه اویلر:** این قضیه رابطه‌ای بین توان‌رسانی پیمانه‌ای و تابع اویلر $\phi(n)$ [میخوانیم فی اِن] برقرار می‌کند که مستقیماً در اثبات صحت عملکرد رمزگذاری و رمزگشایی RSA استفاده می‌شود.
- **آزمون اول‌بودن:** چون تست قطعی اول‌بودن اعداد بسیار بزرگ کند است، الگوریتم‌های احتمالاتی مانند میلر-رابین با چند بار تکرار، با احتمال عملاً یقینی مشخص می‌کنند یک عدد بزرگ اول است یا نه.

حضرت ابا عبدالله الحسین، سید الشهداء علیه‌السلام: «برای هر غم و دردی درمان و دارویی است و جبران و درمان گناه، طلب مغفرت و آمرزش از درگاه خداوند است.» منتخب میزان الحکمه، صفحه ۱۷۰

# انقلاب رمزنگاری کلید عمومی

- **مشکل بنیادی رمز متقارن:** در رمزنگاری متقارن، هر جفت از کاربران به یک کلید محرمانه جداگانه نیاز دارند؛ برای n کاربر به $\frac{n(n-1)}{2}$ کلید نیاز است که توزیع امن آن‌ها در شبکه‌های بزرگ عملاً دشوار می‌شود.
- **ایده دیفی، هلمن و مرکل (۱۹۷۶):** این پژوهشگران پیشنهاد دادند از یک جفت کلید ریاضی مرتبط استفاده شود: یک کلید عمومی که همه می‌توانند بدانند و یک کلید خصوصی که فقط صاحب آن می‌داند؛ آنچه با یکی رمز شود فقط با دیگری باز می‌شود.
- **دو کاربرد مجزا:**
  - اگر با کلید عمومی گیرنده رمز کنیم، فقط خودش (با کلید خصوصی) می‌تواند بخواند ⟵ محرمانگی
  - اگر با کلید خصوصی خودمان رمز کنیم، همه می‌توانند با کلید عمومی ما تأیید کنند که پیام از ما آمده ⟵ احراز اصالت و امضای دیجیتال.

امام باقر (علیه السلام):
چه بسا حریصی بر امری از امور دنیا دست یافته و چون بدان رسیده باعث نافرجامی و بدبختی او گردیده است، و چه بسا کسی که برای امری از امور آخرت کراهت داشته و بدان رسیده، ولی به وسیله آن سعادتمند گردیده است.
تحف العقول, ص ۲۸۷

# الگوریتم RSA

- **ساخت کلید:** دو عدد اول بزرگ p و q انتخاب و $n = p \times q$ و $\phi(n) = (p-1)(q-1)$ محاسبه می‌شود؛ سپس عددی مانند e که با ϕ (n) اول نسبت به هم باشد به‌عنوان کلید عمومی و d که معکوس ضربی e پیمانه ϕ (n) است به‌عنوان کلید خصوصی انتخاب می‌شود.

- **رمزگذاری و رمزگشایی:** رمزگذاری با توان‌رسانی متن ساده به توان e پیمانه n و رمزگشایی با توان‌رسانی متن رمز به توان d پیمانه n انجام می‌شود.

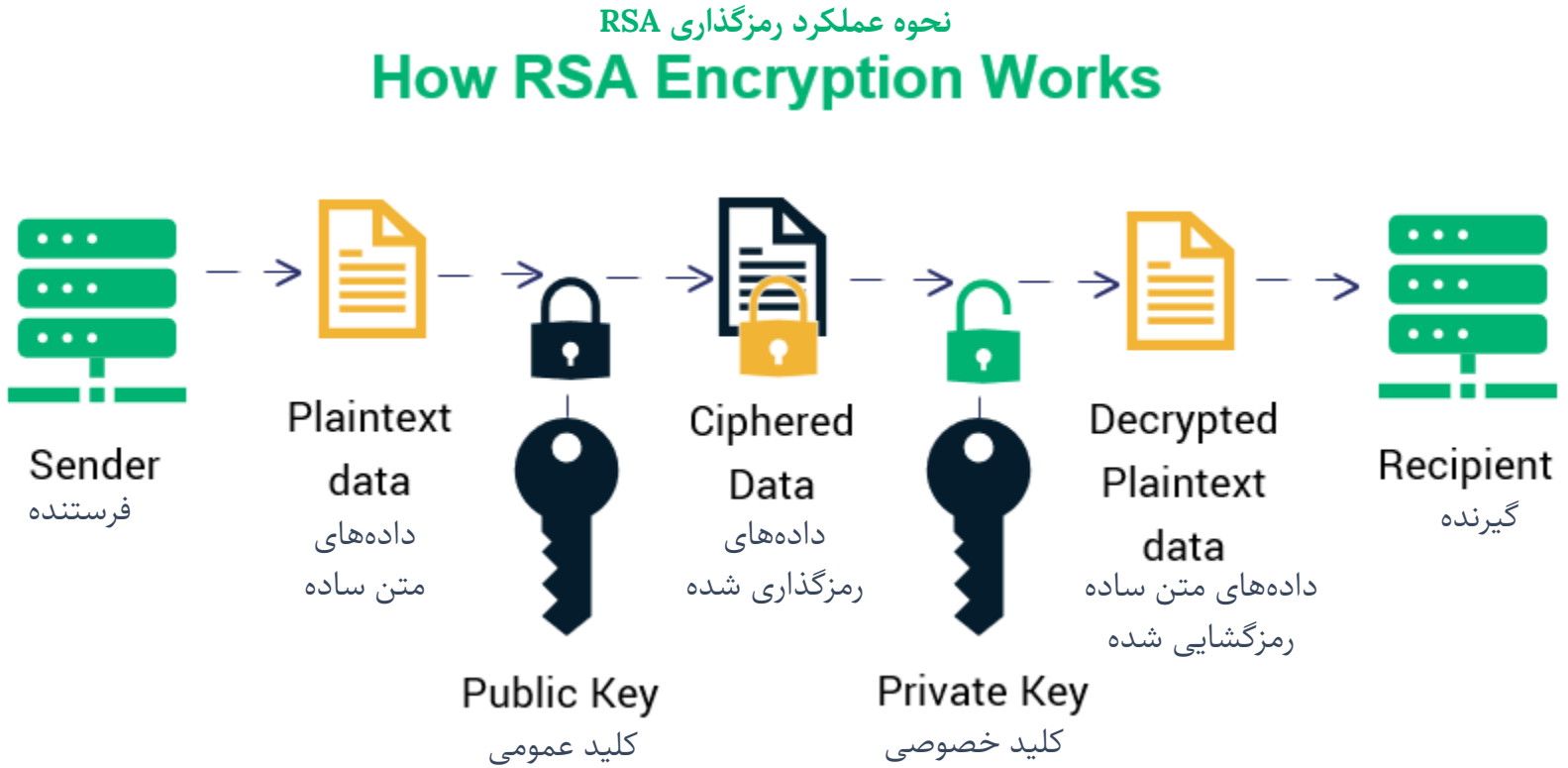
$$\text{Encryption: } C = M^e \pmod{n}$$

$$\text{Decryption: } M = C^d \pmod{n}$$

- **منبع امنیت:** برای رمزگشایی بدون داشتن d، مهاجم عملاً باید n را به p و q تجزیه کند که برای اعداد چندصد رقمی با کامپیوترهای کلاسیک عملاً غیرممکن است.

امام باقر (علیه السلام):
فضیلتی چون جهاد نیست، و جهادی چون مبارزه با هوای نفس نیست
تحف العقول, ص ۲۸۶

# نمودار ساده RSA با کلید عمومی و خصوصی




امام باقر (علیه السلام):
تو را به پنج چیز سفارش می کنم۱. اگر مورد ستم واقع شدی ستم مکن،۲. اگر به تو خیانت کردند، خیانت مکن،۳. اگر تکذیبت کردند، خشمگین مشو،۴. اگر مدحت کنند، شاد مشو،۵. و اگر نکوهشت کنند بیتابی مکن.
تحف العقول, ص ۲۸۴

حضرت علی علیه السلام:

# آنچه برای خود نمی‌پسندی، برای دیگران هم نپسند.

وَ اکرَه لَهُ ما تَکرَهُ لِنَفسِک

نامه ۳۱ نهج البلاغه

(نامه امیرالمومنین علی علیه السلام به امام حسن علیه السلام)




دانشگاه تهران
دانشکده مهندسی کامپیوتر

## با تشکر از حسن توجه شما