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

# ۲

# رمزنگاری کلاسیک

- سرفصل‌های این بخش:
  - مدل رمز متقارن و اصطلاحات پایه
  - روش‌های جانشینی: سزار، تک‌الفبایی، Playfair، Vigenère
  - روش‌های جابجایی و ماشین‌های روتور (Enigma)
  - استگانوگرافی

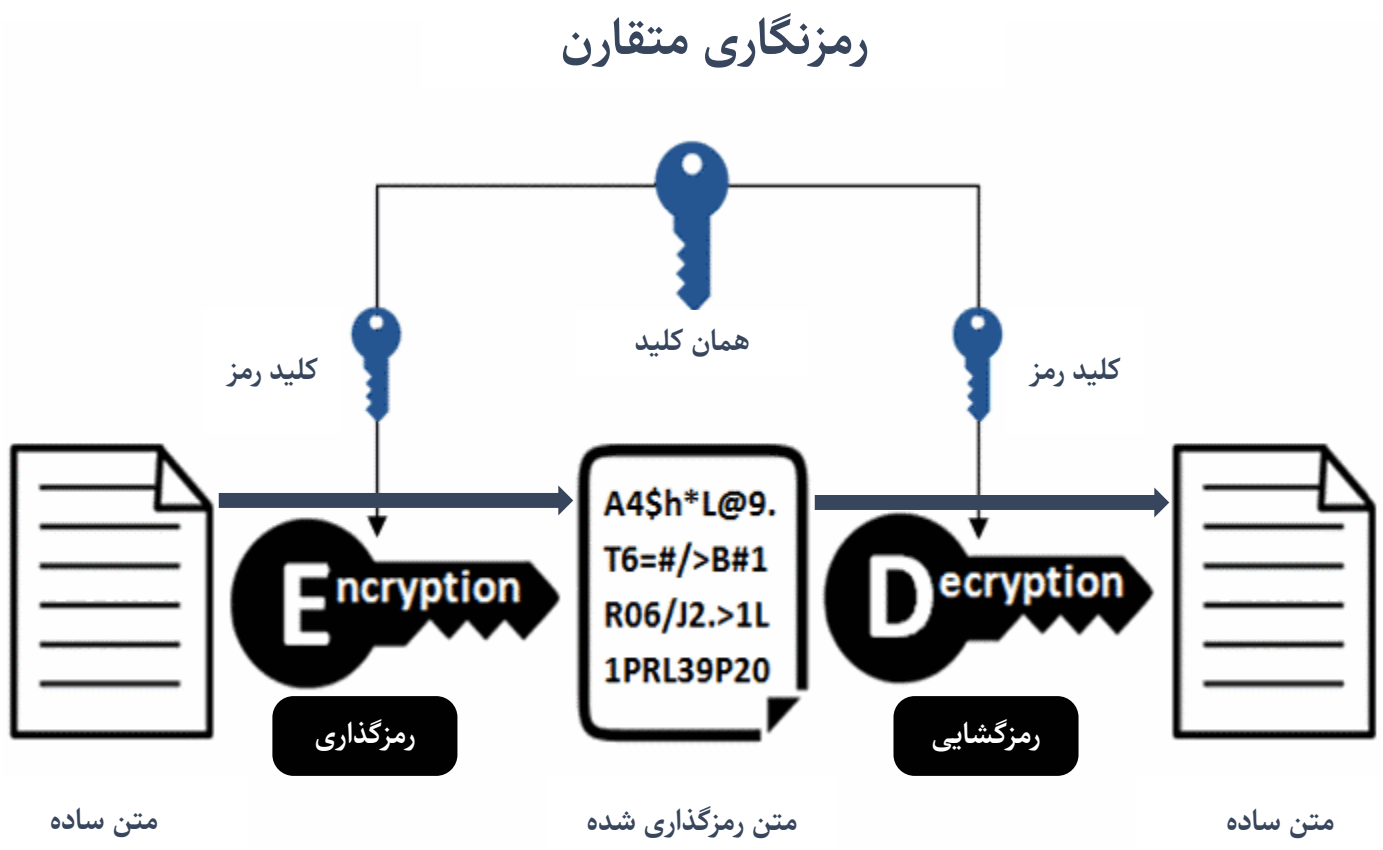
# مدل رمز متقارن

- **متن ساده و متن رمز:** متن ساده (Plaintext) پیام اصلی خوانا و متن رمز (Ciphertext) خروجی نامفهوم پس از رمزگذاری است.
- **کلید (Key):** مقداری مستقل از الگوریتم که رفتار دقیق تبدیل را کنترل می‌کند؛ امنیت سامانه باید فقط به محرمانه‌ماندن کلید وابسته باشد، نه پنهان‌ماندن الگوریتم (اصل کرکهف).
- **رمزگشایی و کلید یکسان:** چون کلید رمزگذاری و رمزگشایی یکسان است، هر دو طرف باید از قبل این کلید مشترک را به‌صورت امن دریافت کرده باشند.
- **تحلیل رمز در برابر جستجوی فراگیر:** مهاجم یا با تحلیل ریاضی الگوریتم (Cryptanalysis) یا با امتحان تمام کلیدهای ممکن (Brute-Force) تلاش می‌کند متن اصلی را بازیابی کند.

حضرت امام محمد بن علی باقر علیه السلام: خداوند این دنیا را به نیکوکار و بدکار می‌بخشد ولی ایمان را جز به برگزیدگان خلقش نمی‌دهد.

اصول کافی جلد ۳ صفحه ۳۰۵

## نمودار مدل رمزگذاری متقارن با فرستنده، الگوریتم رمزگذاری، متن رمز، الگوریتم رمزگشایی و کلید مشترک




حضرت امیرالمومنین علی بن ابیطالب صلوات الله علیه و آله:
خداوند شش طایفه را به سبب داشتن شش خصلت عذاب می‌کند:
عرب‌ها را به سبب تعصب، ملاکان را به سبب تکبر، فرمانروایان را به سبب ستم، فقیهان را به سبب حسادت، بازرگانان را به سبب خیانت و روستاییان را به سبب جهالت.
اصول کافی جلد ۸ صفحه ۱۶۲

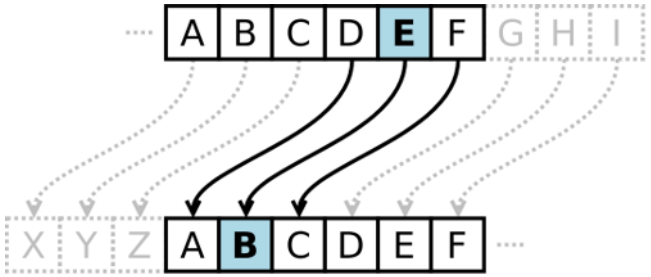
# روش‌های جانشینی

- **رمز سزار:** ژولیوس سزار برای فرمان‌های نظامی هر حرف را چند جایگاه در الفبا جابه‌جا می‌کرد؛ ساده اما با فقط ۲۵ کلید ممکن، به‌راحتی با جستجوی فراگیر شکسته می‌شود.
- **جانشینی تک‌الفبایی:** با جایگشت کامل ۲۶ حرف، فضای کلید به‌شدت افزایش می‌یابد، اما چون هر حرف همیشه با یک حرف ثابت جایگزین می‌شود، تحلیل فراوانی حروف (که نخستین‌بار توسط دانشمند عرب الکندی ابداع شد) به‌سادگی آن را می‌شکند.
- **رمز Playfair:** برای مقابله با تحلیل فراوانی تک‌حرفی ابداع شد؛ حروف را دوتایی (دای‌گراف) رمز می‌کند و بدین‌ترتیب فراوانی آماری حروف منفرد را پنهان می‌کند.
- **رمز Vigenère:** با استفاده از یک کلمه کلیدی، در هر موقعیت از یک الفبای جانشینی متفاوت استفاده می‌کند (چندالفبایی)؛ قرن‌ها 'غیرقابل‌شکست' تصور می‌شد تا این‌که کاسیسکی روشی برای یافتن طول کلید و شکستن آن ارائه داد.

حضرت امام محمد بن علی باقر علیه السلام: مبادا فرصت‌های به دست آمده را از دست بدهی که در این میدان آنکه وقت را ضایع کند زیان می‌بیند.
تحف العقول صفحه ۲۸۶

# رمزنگاری سزار






حضرت رسول الله محمد مصطفی صلی الله علیه و آله و سلم:

بر تو باد به خاموشی بسیار، چرا که آن موجب طرد شیطان است و در کار دین‌ات یاور توست.

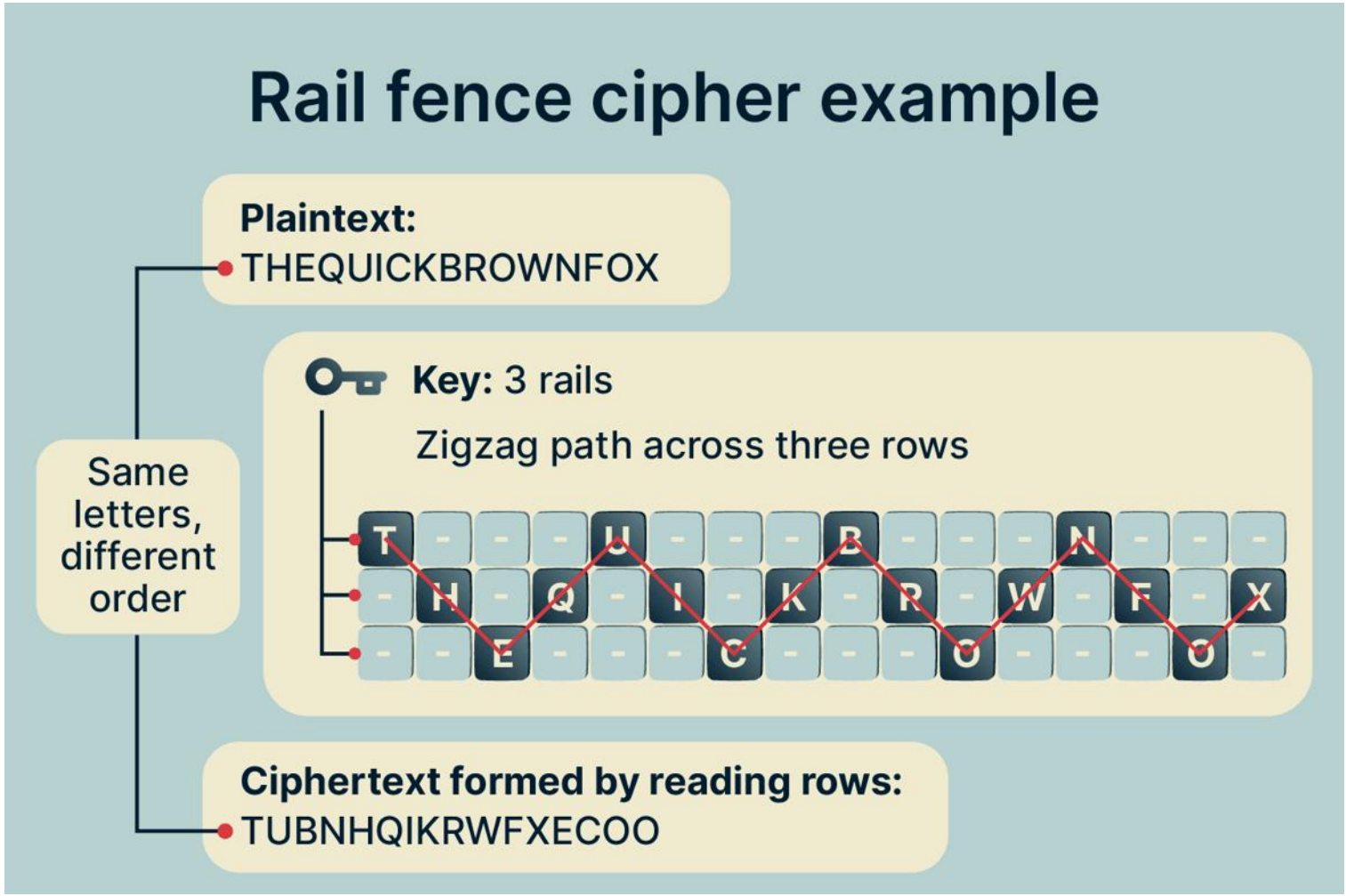
الخصال صفحه ۵۲۶

# جابجایی و ماشین‌های روتور

- **روش‌های جابجایی (Transposition):** برخلاف جانشینی، حروف متن تغییر نمی‌کنند بلکه ترتیب آن‌ها جابه‌جا می‌شود؛ نمونه ساده آن رمز نرده راه‌آهن (Rail Fence) است.
- **انگیزه ساخت ماشین روتور:** رمزهای دستی برای پردازش حجم بالای پیام‌های نظامی کند بودند؛ مهندسان اروپایی در دهه ۱۹۲۰ ماشین‌های مکانیکی‌ای طراحی کردند که با هر بار فشردن یک کلید، الفبای جانشینی را خودکار تغییر می‌دادند.
- **ماشین انیگما:** ارتش آلمان در جنگ جهانی دوم از انیگما استفاده می‌کرد که با چرخش چندین روتور، میلیون‌ها حالت رمزگذاری متفاوت ایجاد می‌کرد و تحلیل فراوانی ساده را بی‌اثر می‌کرد.
- **شکستن انیگما:** تیمی به سرپرستی آلن تورینگ در بلچلی پارک با ساخت ماشین‌های مکانیکی به‌نام Bombe، ضعف‌های ساختاری و رویه‌ای انیگما را یافتند و توانستند پیام‌های آلمان را رمزگشایی کنند.

حضرت اباعبدالله امام حسین علیه السلام: دوست تو کسی است که تو را از گناه باز دارد و دشمن تو کسی است که تو را به گناه وادارد.
کنز الفوائد صفحه ۱۲۸

# روش رمزنگاری نرده ریل




حضرت امام علی بن حسین سجاد علیه السلام: خشنودی به قضای ناخوشایند الهی، عالی‌ترین پایه‌های ایمان و یقین است.

تحف العقول صفحه ۳۱۸

# استگانوگرافی

- **تفاوت بنیادی با رمزنگاری:** رمزنگاری محتوای پیام را نامفهوم می‌کند اما وجود پیام آشکار است؛ استگانوگرافی اصلاً وجود پیام را پنهان می‌کند تا مهاجم حتی متوجه ارسال اطلاعات محرمانه نشود.
- **روش‌های کلاسیک:** پنهان کردن پیام در جوهر نامرئی، پنهان کردن تکه کاغذ داخل اثر هنری مانند مجسمه، یا جاسازی حروف اول هر خط یک متن ظاهراً بی‌ضرر.
- **استگانوگرافی دیجیتال امروزی:** پنهان کردن بیت‌های داده در کم‌اهمیت‌ترین بیت‌های پیکسل یک تصویر (LSB) یا در فایل‌های صوتی؛ تغییر آن‌قدر جزئی است که با چشم یا گوش قابل تشخیص نیست.
- **محدودیت اصلی:** استگانوگرافی به‌تنهایی ضعیف است چون با یافتن روش پنهان‌سازی، تمام پیام آشکار می‌شود؛ به همین دلیل معمولاً همراه با رمزنگاری به‌کار می‌رود تا دو لایه حفاظت ایجاد شود.

حضرت صاحب الامر امام عصر عجل الله تعالی فرجه الشریف: من مایه امنیت زمینیان هستم، همانطور که ستارگان مایه امنیت آسمانیان هستند.
بحارالانوار جلد ۵۳ صفحه ۱۸۱