sooraac.ir

یا ذاالامن والامان

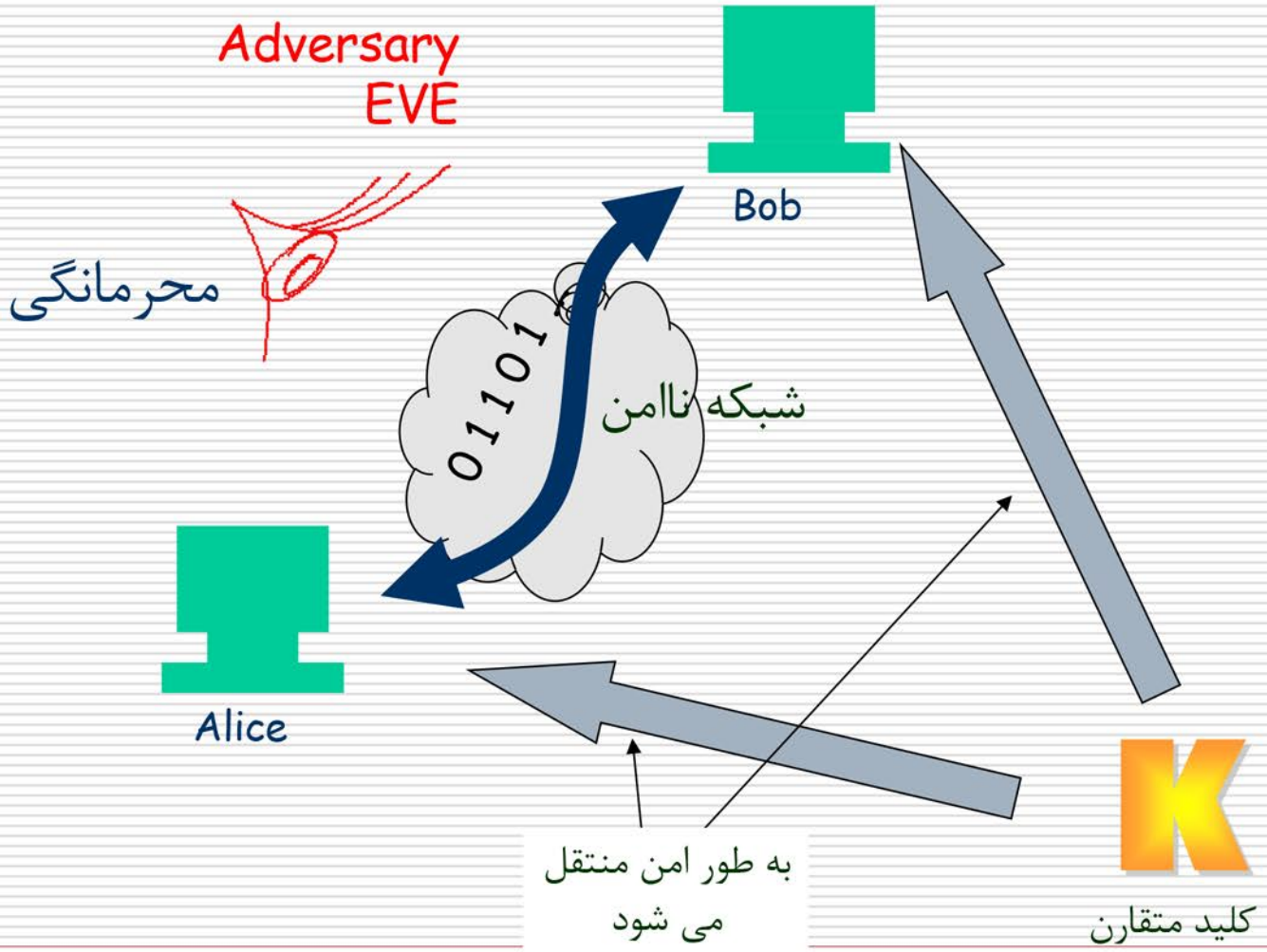
امنیت داده و شبکه

رمزنگاری متقارن (مدرن)

شرکت و آموزشگاه فنی و حرفه‌ای سورا

www.sooraac.ir

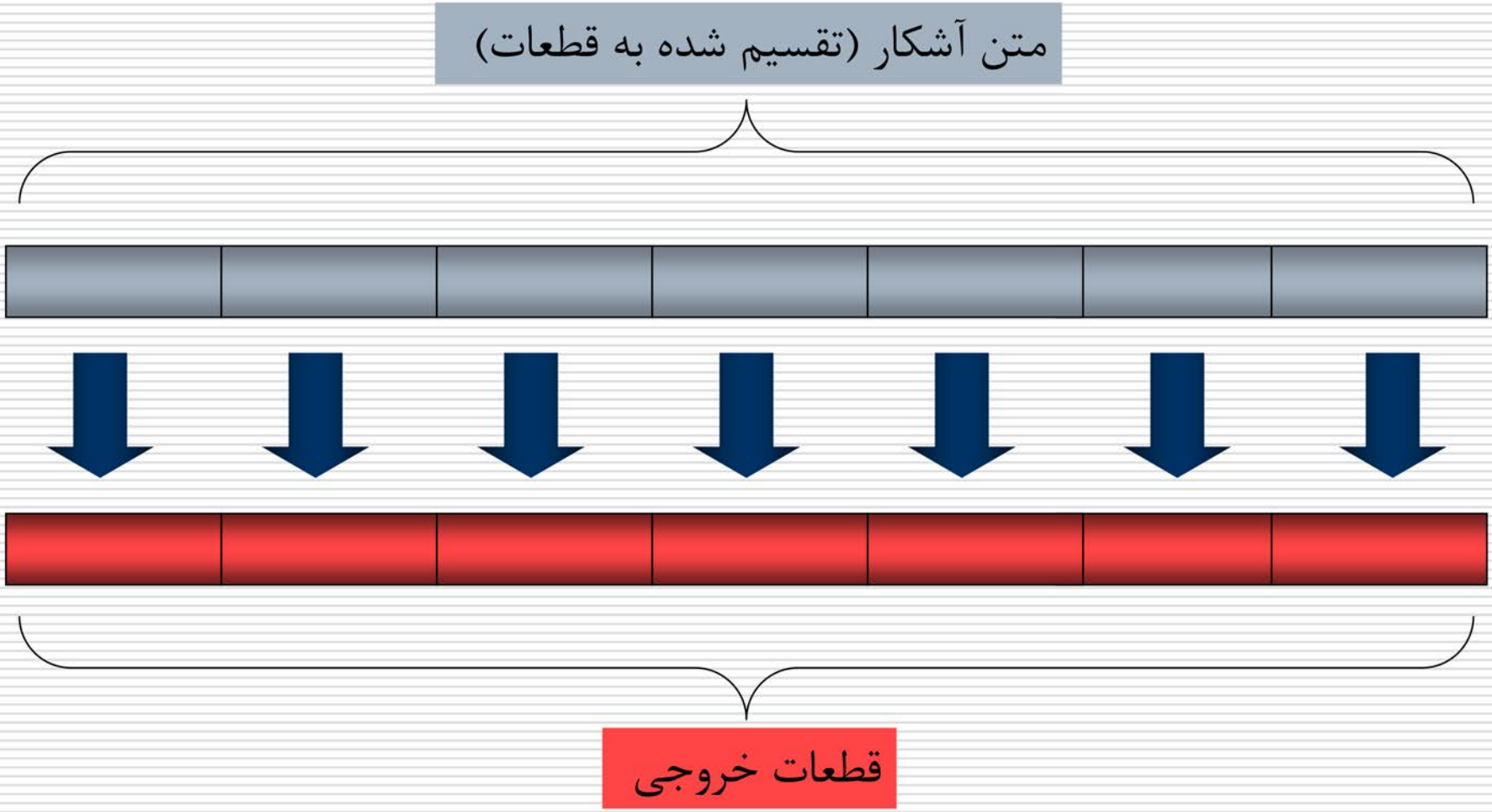
رمزنگاری متقارن



الگوریتم‌های رمز متقارن

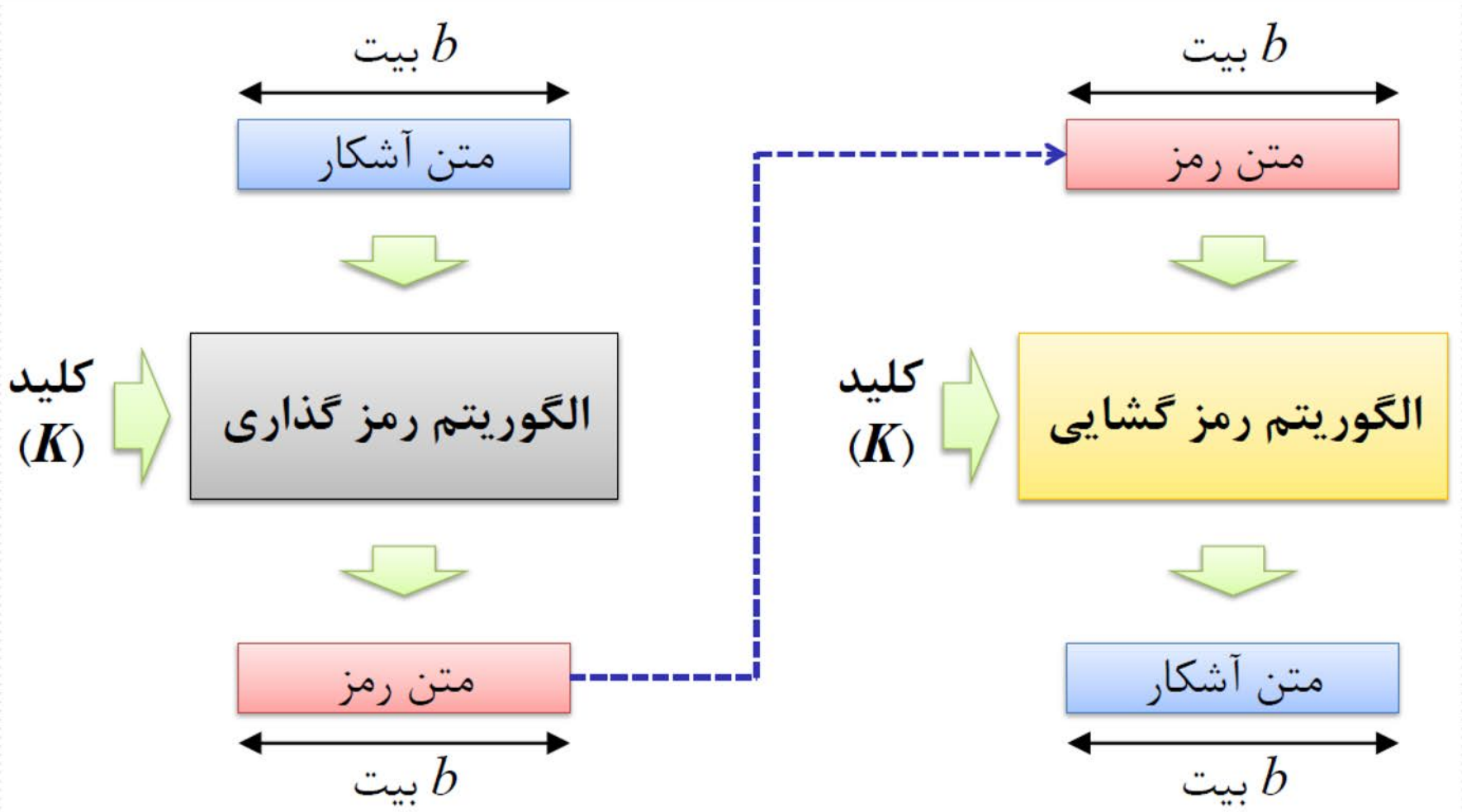
- رمزهای متقارن را می‌توان با دو روش عمده تولید کرد:
  - **رمزهای قطعه‌ای (Block Cipher)**
    - پردازش پیغام ها بصورت قطعه به قطعه
    - اندازه متعارف مود استفاده برای قطعات ۶۴، ۱۲۸یا ۲۵۶ بیتی است.
  - **رمزهای جریانی (Stream Cipher)**
    - پردازش پیغام‌ها بصورت پیوسته

رمزهای قطعه‌ای

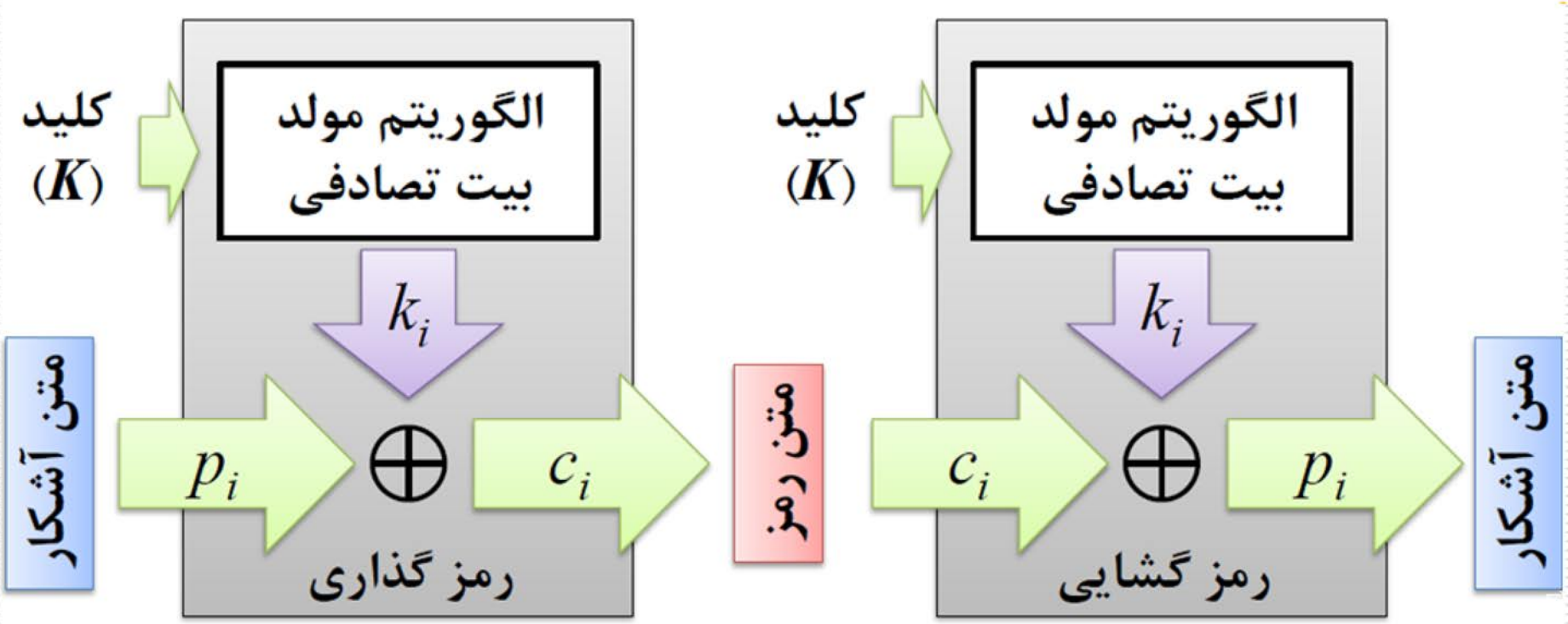


sooraac.ir

رمزهای قطعه‌ای



رمزهای جریانی



رمزگذاری کلاسیک–رمزگذاری مدرن

- در روش‌های رمزگذاری مدرن، علاوه بر اَعمال جانشینی و جایگشت از توابع ساده مانند XOR استفاده می‌شود.
- مجموعه اعمال فوق طی مراحل متوالی روی متن اولیه اعمال می‌شوند.
- تکنیک بکارگرفته شده در Rotor Machineها الهام بخش روشهای رمزگذاری مدرن بوده است.

sooraac.ir

شانون و رمز جانشینی و جایگشت

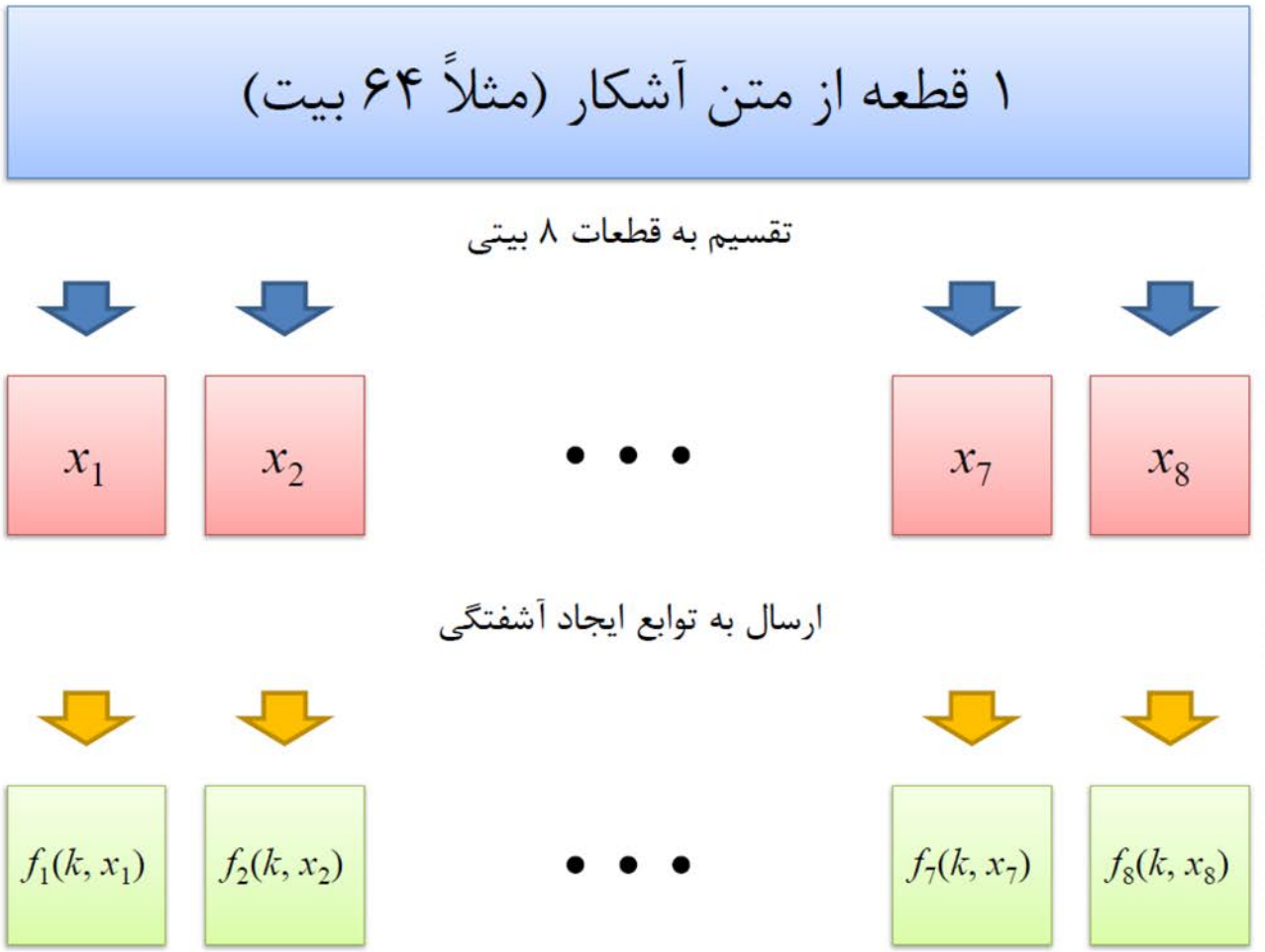
- شانون ایده استفاده از شبکه اَعمال جانشینی و جایگشت را در سال ۱۹۴۹ مطرح کرد.
- پایه رمزهای مدرن بر اساس این دو عمل است:
  - جانشینی (S-box)
  - جایگشت (P-box)
- این دو عمل، گمراه‌کنندگی (Confusion) و پراکندگی (Diffusion) پیام موردنظر و کلید را موجب می‌شوند.

Claude E. Shannon
(1916 – 2001)

گمراه‌کنندگی و پراکندگی

- الگوریتم‌های رمز باید خصوصیات آماری پیام اصلی (متن آشکار) را به طور کامل مخفی کنند.
- رمز One-Time Pad این عمل را انجام می‌دهد.
- شانون پیشنهاد کرد که از ترکیب جانشینی و جایگشت برای ارضای دو خصوصیت زیر استفاده کند:
- **گمراه‌کنندگی (Confusion)**: رابطه بین متن رمزشده و کلید تا حد امکان پیچیده باشد.
- **پراکندگی (Diffusion)**: ساختار آماری متن آشکار بر روی حجم وسیعی از متن‌های رمزشده ممکن پراکنده شود.

گمراه‌کنندگی (Confusion)

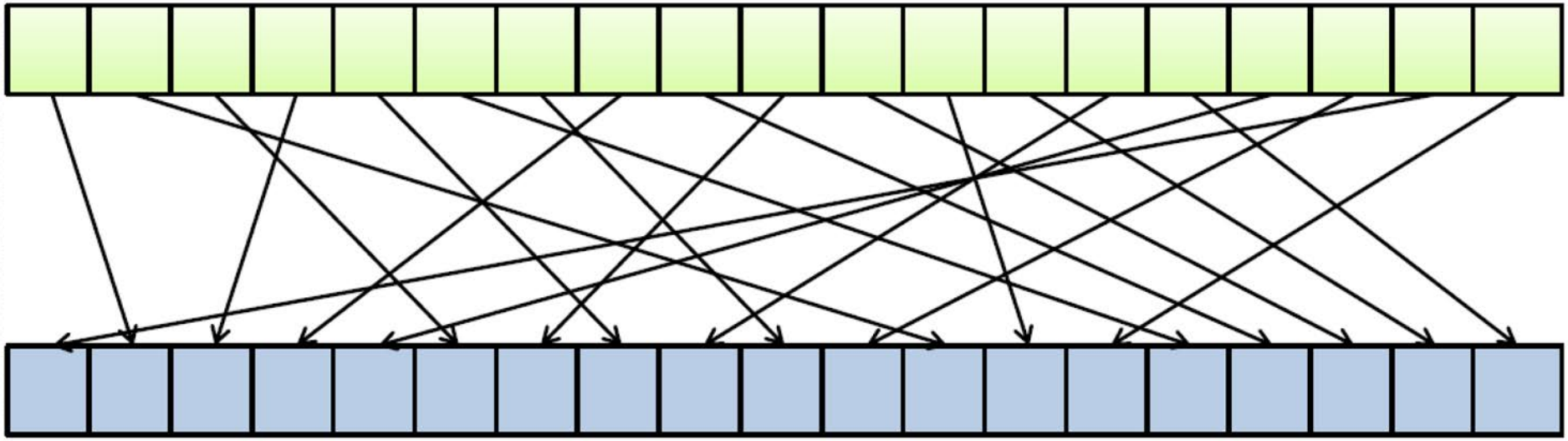


توابع گمراه‌کنندگی (آشفتگی)

- ورودی هر یک از توابع گمراه‌کنندگی، کلید و بخشی از متن آشکار است.
- طراحی توابع آشفتگی با ورودی کوچکتر ساده‌تر است؛ اما تحلیل آن توسط مهاجم نیز آسانتر خواهد بود.
  - نیا به مصالحه
  - امروزه ورودی ۸ بیتی مناسب به نظر می‌رسد.

پراکندگی (Diffusion)

- خروجی، جایگشت بیت‌های ورودی است.
- چگونگی جایگشت می‌تواند وابسته به کلید باشد.
- اثر موضعی توابع آشفتگی پخش می‌شود.



دور (Round)

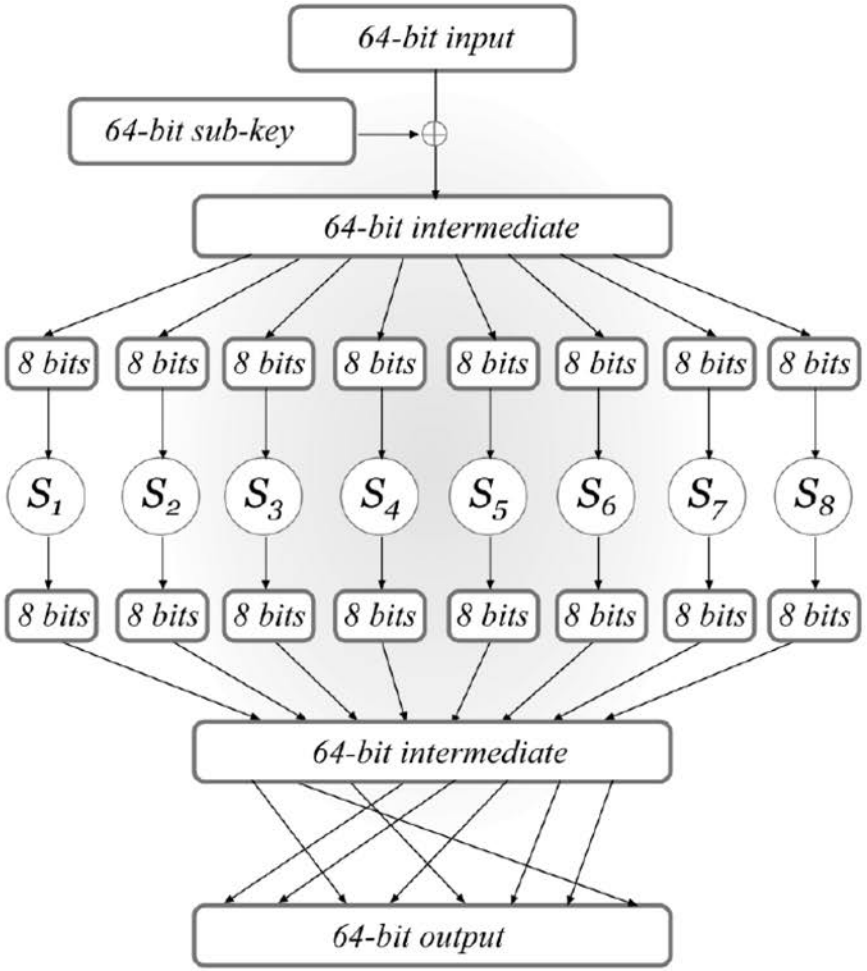
- **دور:** یک مرحله اِعمال آشفتگی + یک مرحله پراکندگی
- یک الگوریتم رمز از چندین دور تشکیل می‌شود.
  - توابع آشفتگی و پراکندگی هر دور می‌تواند متفاوت باشد.
- با افزایش تعداد دور، رمز پیچیده تر شده ولی کارایی آن کمتر می‌شود.
- یکی از وظایف طراح رمز آن است که تعداد دور بهینه را پیدا کند.

شبکه جانشینی-جایگشتی (SPN)

- Substitution-Permutation Network
  - نوع خاصی از الگوی آشفتگی-پخش
  - توابع دور آن، شکل مشخصی دارند.
    - غیر وابسته به کلید، آشکار برای همگان (حتی مهاجم)
  - تابع جانشینی: S-box یا S
  - تابع جایگشت: P-box یا P
  - کلید در ابتدای هر دور با مقدار ورودی XOR می‌شود.

sooraac.ir

یک دور از SPN



۱. XOR کلید

۲. اِعمال S-BoX

۳. اِعمال P-BoX

مزایا و معایب SPN

- **مزیت:** امکان موازی‌سازی و در نتیجه افزایش کارایی
  - در هر دور می‌توان S-Boxها را به طور موازی اجرا نمود.
- **عیب ۱:** محدودیت طراح در انتخاب S-Box
  - S-Boxها باید برگشت‌پذیر باشد تا بتوان رمزگشایی نمود.
  - دست طراح در انتخاب S-Box بسته است.
- **عیب ۱:** الگوریتم رمزگشایی با رمزگذاری متفاوت است.
  - افزایش حجم پیاده‌سازی، به ویژه در سخت افزار

sooraac.ir

پایان