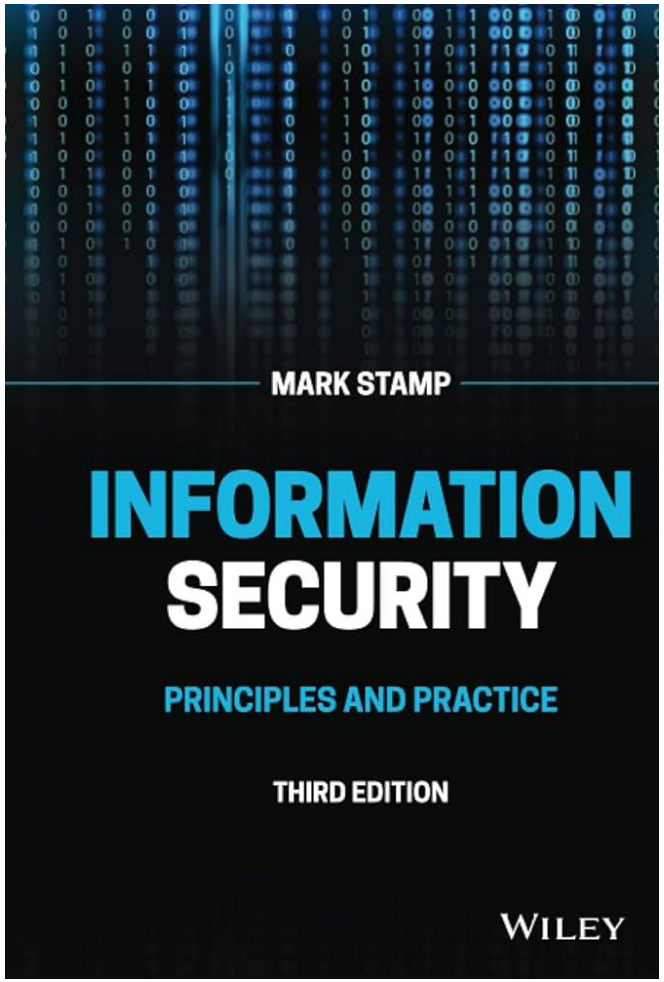
بسم الله الرحمن الرحیم

مبانی رایانش امن

جلسه ۴

مجتبی خلیلی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان


MARK STAMP
INFORMATION
SECURITY
PRINCIPLES AND PRACTICE
THIRD EDITION
WILEY

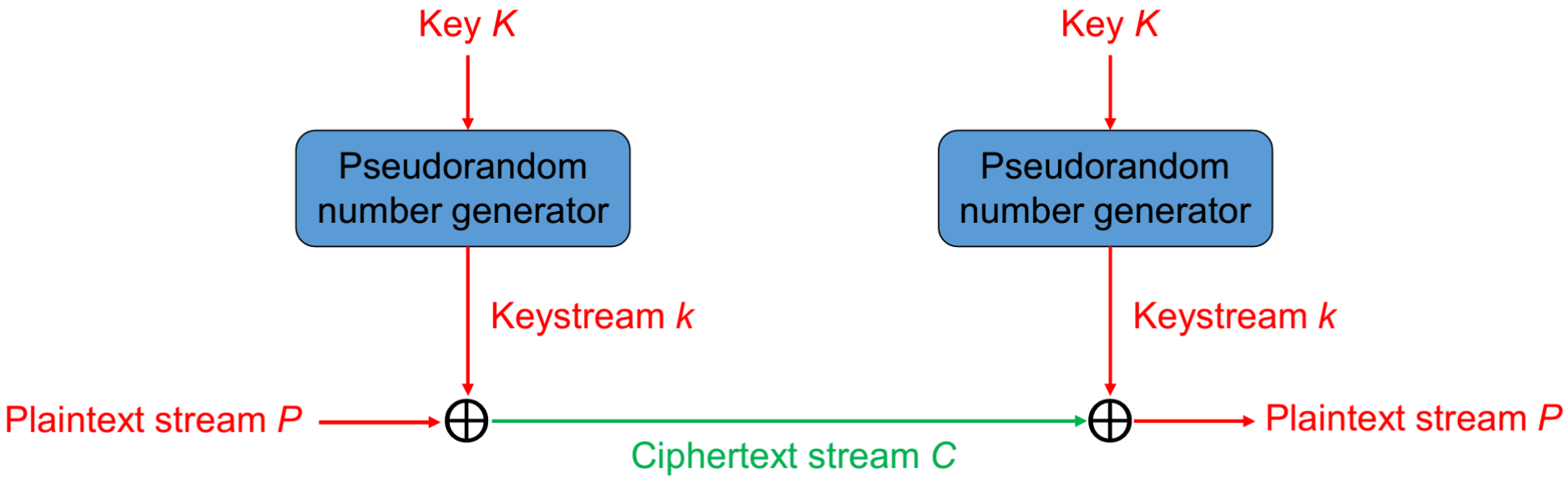
- فصل سوم کتاب

- **Cryptology** — The art and science of making and breaking "secret codes"
- **Cryptography** — making "secret codes"
- **Cryptanalysis** — breaking "secret codes"
- **Crypto** — all of the above (and more)

رمزنگاری متقارن (مدرن)

- در حالت کلی رمزنگاری متقارن (مدرن) به دو دسته کلی تقسیم میشوند:
  - الگوریتم‌های رمز جریان (Stream Cipher)
  - الگوریتم‌های رمز بلوکی (Block Cipher)

Stream Cipher

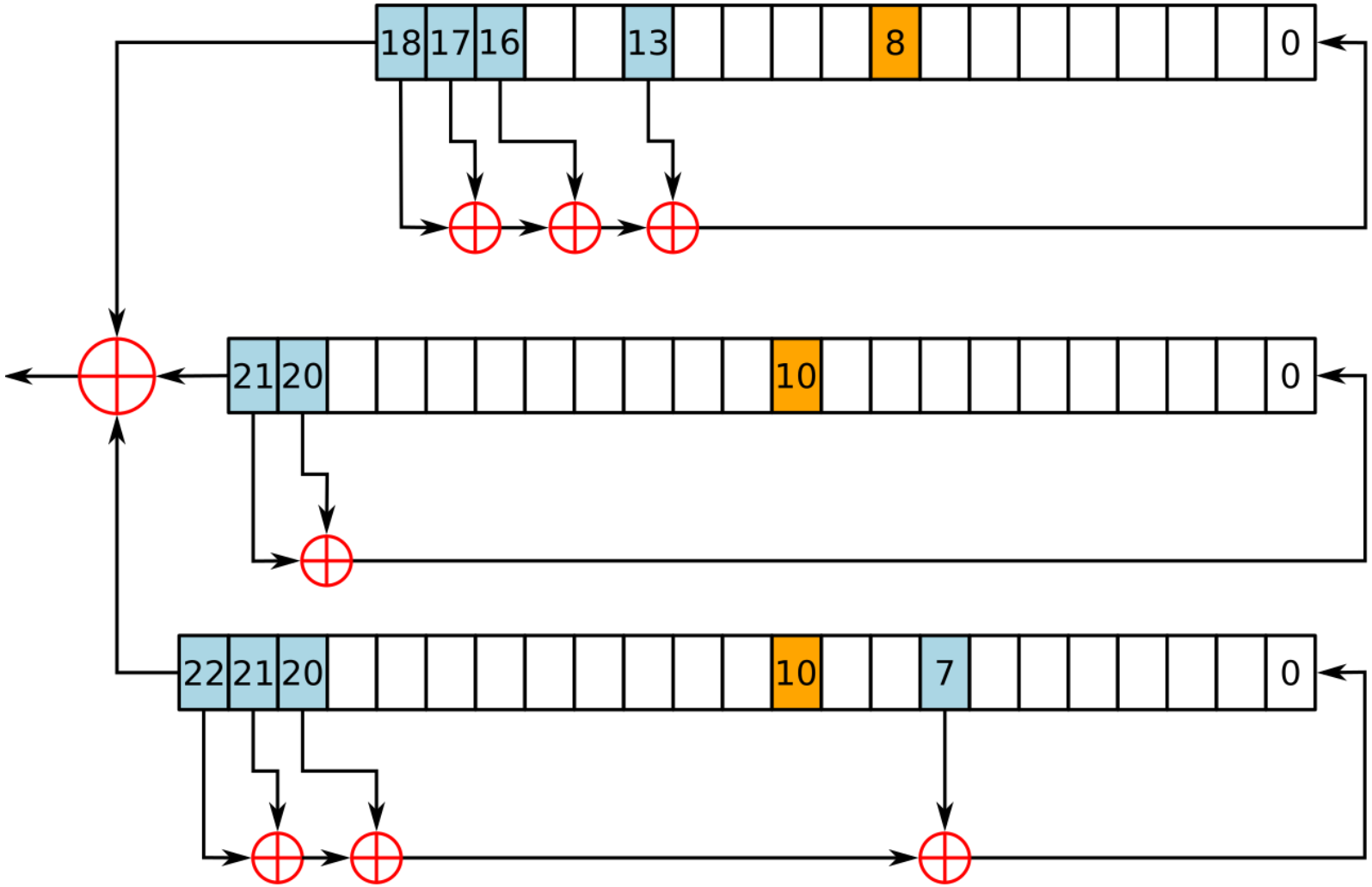


Stream Cipher

- هدف: عملی کردن OTP
- ایده: استفاده از کلید شبه تصادفی بجای یک کلید واقعا تصادفی

- دقت کنید همچنان کلید یک بار مصرف باقی بماند.

Stream Cipher (A5/1)



Stream Cipher

- ملاحظات طراحی:
  - دوره تناوب بزرگ بدون تکرار
  - به صورت آماری تصادفی بودن
- غالبا ساده و سریع هستند.

In September 2015, Microsoft announced the end-of-support of the RC4 cipher in Microsoft Edge and Internet Explorer 11 in early 2016. **[Updated] We initially announced plans to release this change in April 2016. Based on customer feedback, we now plan to delay disabling the RC4 cipher. We encourage customers to complete upgrades away from RC4 soon, as a forthcoming update will disable RC4 by default and RC4 will no longer be used for TLS fallback negotiations.**

There is consensus across the industry that RC4 is no longer cryptographically secure. With this change, Microsoft Edge and IE11 are aligned with the most recent versions of Google Chrome and Mozilla Firefox.

What is RC4?

RC4 is a stream cipher that was first described in 1987, and has been widely supported across web browsers and online services. Modern attacks have demonstrated that RC4 can be broken within hours or days.

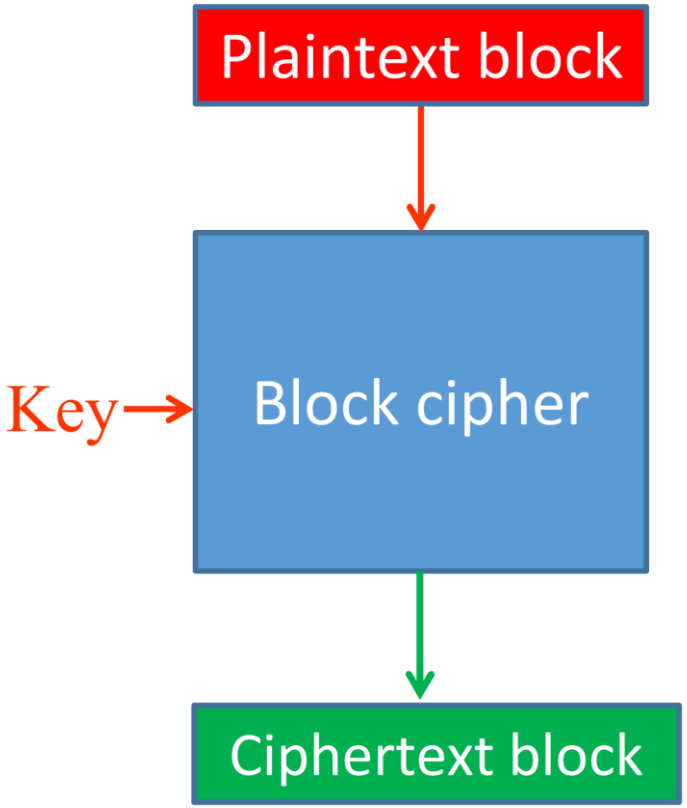
قوانین شانون

- برای پنهان کردن خصوصیات آماری پیام و کلید، شانون پیشنهاد داد پیام ها و کلیدها به اندازه کافی ترکیب شوند تا دو ویژگی زیر حاصل شوند:

  - Diffusion: خصوصیات آماری متن اصلی بر روی متن رمز شده پخش شده باشد.

  - Confusion: رابطه آماری بین متن اصلی و متن رمز شده تا حد ممکن از بین برود.

رمزهای بلوکی



- یک رمز بلوکی دارای دو پارامتر k و l است و همچنین دو الگوریتم قطعی (E,D) برای رمزگذاری و رمزگشایی دارد:

$$E : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$$
$$D : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$$

رمزهای بلوکی

- پیش از این دیدیم که در رمزهای کلاسیک از جایگشت و شیفت استفاده میکردیم.

- در روشهای مدرن رمزنگاری، علاوه بر شیفت و جایگشت، از جایگزینی و توابع ساده‌ای مثل XOR نیز استفاده میشود. بنابراین الگوریتم استفاده در هر round شامل اعمالی از این دست خواهد بود.

- در یک Block Cipher ایده‌آل انتظار داریم برای یک ورودی l بیتی تعداد حالات محتمل خروجی چندتا باشد؟

رمزهای بلوکی