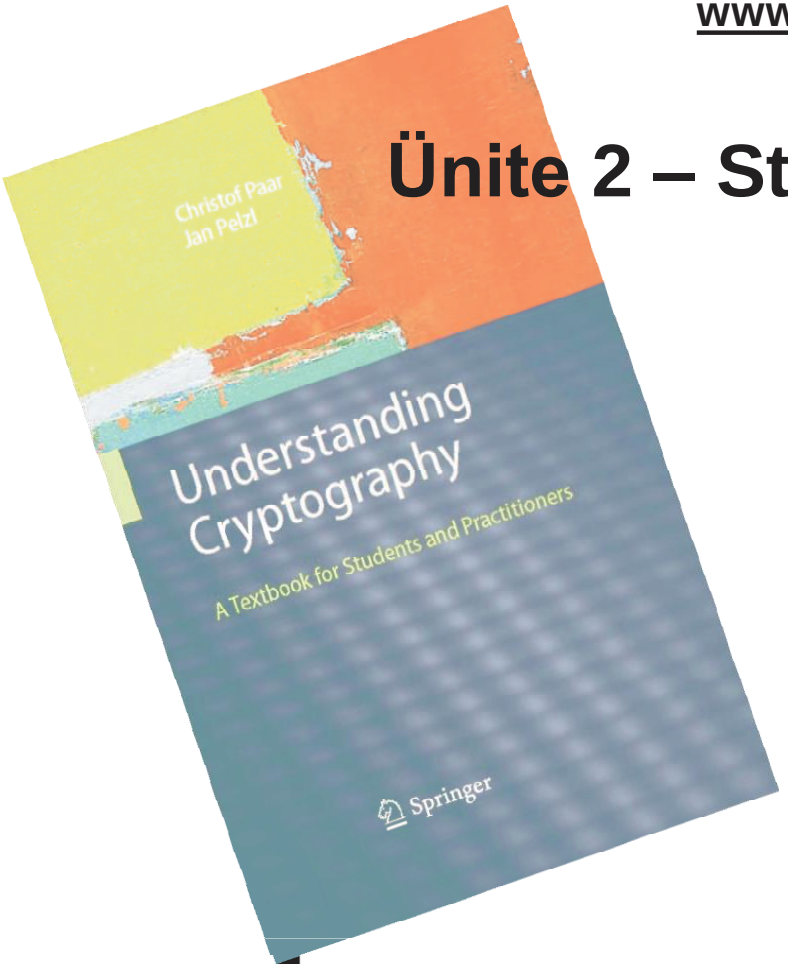
Understanding Cryptography Öğrenci ve Uygulamacılar İçin Ders kitabı

www.crypto-textbook.com



Ünite 2 – Stream(akan) Şifreleme

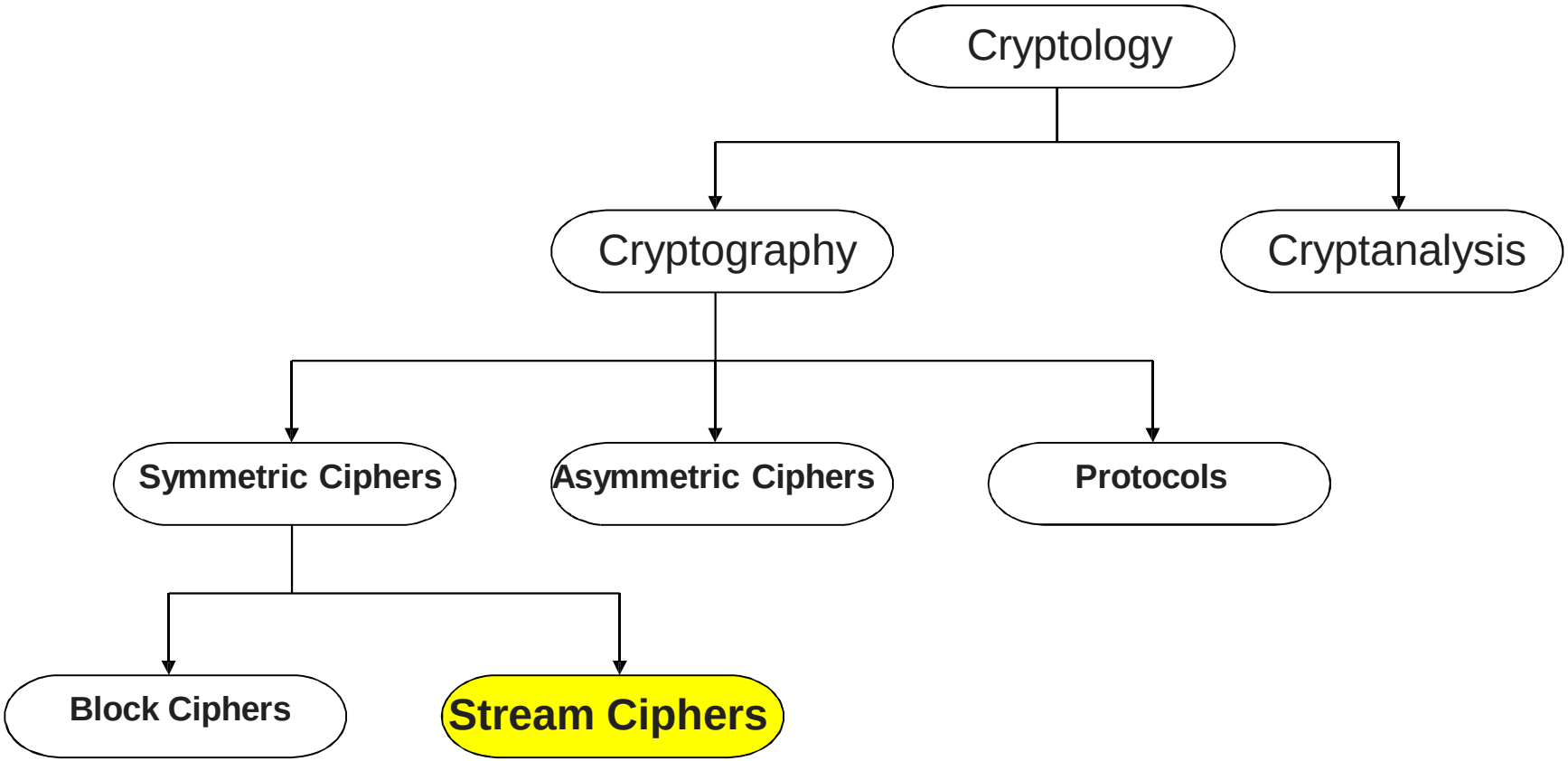
Ünite içeriği

- Akan (stream) şifrelemeye giriş
- Rastgele sayı üreteci (Random number generators (RNGs))
- Tek kullanımlık blok notlar(One-Time Pad (OTP))
- Lineer geri beslemeli kaymalı kaydediciler (Linear feedback shift registers (LFSRs))
- Trivium: a modern stream şifre

Ünite içeriği

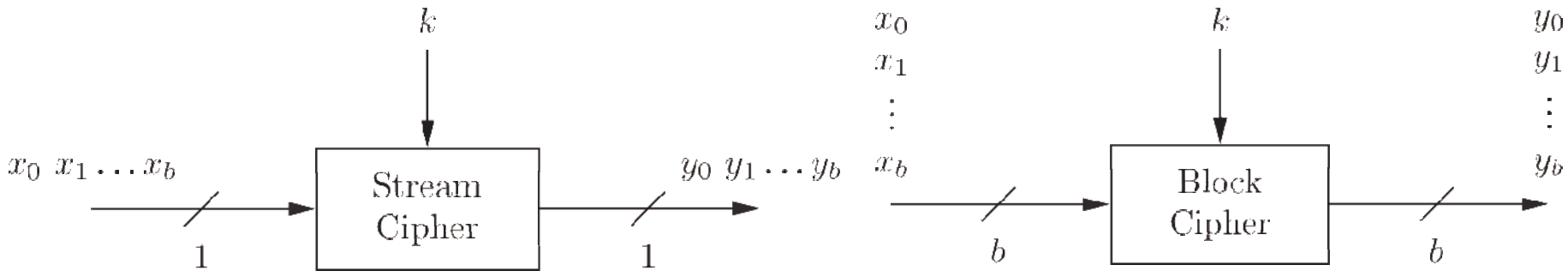
- **Stream şifrelemeye giriş**
- Rastgele sayı üreteci (Random number generators (RNGs))
- Tek kullanımlık blok notlar(One-Time Pad (OTP))
- Linear feedback shift registers (LFSRs)
- Trivium: a modern stream şifre

- **Şifrelemede Stream Şifrelemenin Yeri**



Stream Ciphers 1917 de Gilbert Vernam tarafından bulundu

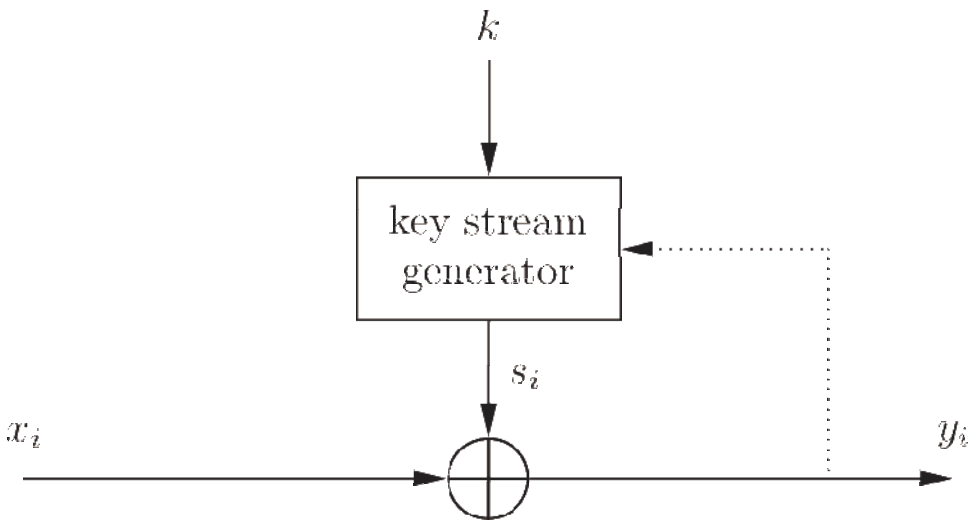
- **Stream şifreleme ve Blok şifreleme**



- **Stream Şifreler**
  - Bitler tek tek şifrelenir
  - Gömülü sistemlerde yaygındır genellikle küçük ve hızlıdır (e.g., A5/1 for GSM phones)

- **Block Şifreler:**
  - Her zaman blokun hepsini şifreler (birkaç bit)
  - İnternet uygulamaları için yaygındır.

- **Senkron ve Asenkron Stream Şifreleme**



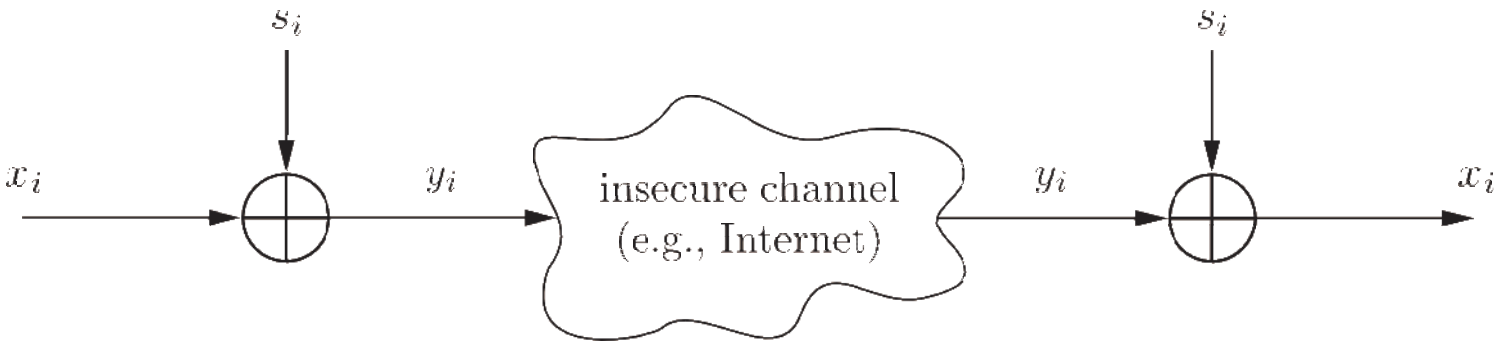
- s_i Anahtar üretiminin güvenliği tamamıyla anahtar değerine bağlıdır:
  - **Rastgele** olmalı , i.e., $\Pr(s_i = 0) = \Pr(s_i = 1) = 0.5$
  - Gönderici ve alıcı tarafından yeniden üretilebilmeli

- **Senkron Stream Şifreler**
  - Anahtar üretimi sadece anahtara bağlıdır(ve IV başlangıç değeri olabilir)

- **Asenkron Stream şifreler**
  - Anahtar üretimi şifreli metne de bağlıdır.

- **Stream şifreleme ile şifreleme ve şifre çözme**

Düz metin x_i, şifreli metin y_i ve stream anahtarı s_i tek tek bitlerden oluşur



- Şifreleme ve şifre çözme mod 2 de toplama işlemi gibidir (aka XOR)
- Şifreleme ve şifre çözme aynı fonksiyondur.

- **şifreleme:** $y_i = e_{si}(x_i) = x_i + s_i \bmod 2$ $\qquad x_i, y_i, s_i \in \{0,1\}$
- **Şifre çözme:** $x_i = e_{si}(y_i) = y_i + s_i \bmod 2$

- **Neden Mod 2 de Toplamak İyi Bir Şifreleme Fonksiyonudur?**

  - Mod 2 toplama işlemi XOR işlemine eşittir.

  - Mükemmel bir stream s_i ,anahtarı için her şifreli metin çıkış bitinin 0 veya 1 olma ihtimali 50% olmalıdır.

  - Ters çevrilmiş XOR basittir, çünkü XOR işleminin aynısıdır.

x_i	s_i	y_i
0	0	0
0	1	1
1	0	1
1	1	0

- **Stream Şifre: Çıktı**

Simetrik şifrelerin performans karşılaştırması (Pentium4):

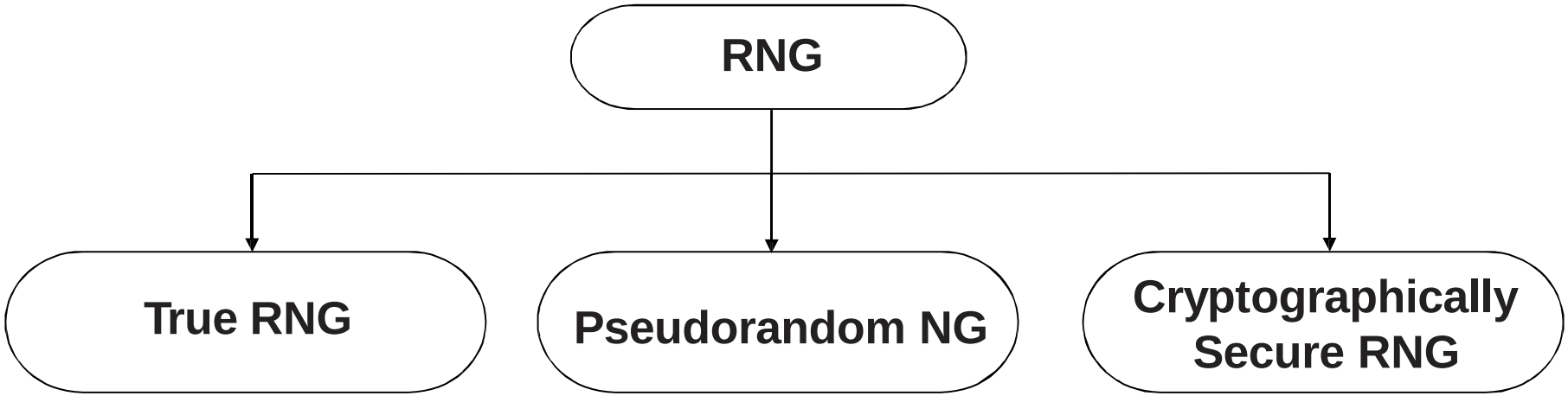
Cipher	Key length	Mbit/s
DES	56	36.95
3DES	112	13.32
AES	128	51.19
RC4 (stream cipher)	(choosable)	211.34

Source: Zhao et al., Anatomy and Performance of SSL Processing, ISPASS 2005

Ünite içeriği

- stream şifrelemeye giriş
- **Rastgele sayı üreteci (Random number generators (RNGs))**
- Tek kullanımlık blok notlar(One-Time Pad (OTP))
- Linear feedback shift registers (LFSRs)
- Trivium: a modern stream şifre

- **Rastgele Sayı Üreteci (RNGs)**



- **Gerçek Rastgele Sayı Üreteci(TRNGs)**

  - Fiziksel rastgele işlemlere dayanır: yarı iletken gürültüsü, radyoaktif kalıntılar, fare hareketleri
  - Çıkış stream s_i değeri iyi istatiksel özeliklere sahip olmalı:
    $\Pr(s_i = 0) = \Pr(s_i = 1) = 50\%$ (sıklıkla sonraki işlemlerle yapılır)
  - Çıkış değeri hem tahmin edilememeli hem de yeniden üretilememeli

Anahtarların üretimi için tipik kullanım, (sadece tek kullanımlık değerler kullanılır) ve başka bir çok amaç için

- **Sözde Rastgele Sayı (PRNG)**

- Başlangıç çekirdek değerinden bir zincir üretir.
- Tipik olarak, çıkış stream iyi istatiksel özelliklere sahiptir.
- Özyinelemeli yollarla çıkış değeri yeniden üretilebilir ve tahmin edilebilir :

$$s_0 = seed$$

$$s_{i+1} = f(s_i, s_{i-1}, \ldots, s_{i-t})$$

Örnek: *rand() function* in ANSI C:

$$s_0 = 12345$$

$$s_{i+1} = 1103515245 s_i + 12345 \bmod 2^{31}$$

birçok PRNG nin kötü şifreleme özellikleri vardır!

- **Basit bir PRNG nin kripto analizi**

Örnek PRNG: **Linear Congruential Generator**

$$S_0 = seed$$

$$S_{i+1} = AS_i + B \bmod m$$

Farz edelim

- *A*, *B ve* S_0 anahtar gibi bilinmiyor
- *A*, *B* ve S_i boyutu 100 bit
- Çıkışın 300 biti biliniyor, i.e. S_1, S_2 and S_3

çözüm

$$S_2 = AS_1 + B \bmod m \; S_3$$

$$= AS_2 + B \bmod m$$

… A ve B yi direk gösterir. bütün S_i kolaylıkla hesaplanabilir!

Birçok PRNG liner yapıda olduğundan şifreleme özellikleri kötüdür.

- **Kriptografik Olarak Güvenli Sözde Rastgele Sayı Üreticileri (CSPRNG)**
  - Ek özellikleriyle özel PRNG:
    - Çıkış kesinlikle tahmin edilememeli

Daha Doğrusu : s_i , çıkışından verilen sıralı n bit bir sonraki çıkış s_{n+1} de tahmin edilemez (polinom zamanda).

- Buna şifrelemede özellikle stream şifre yapısında ihtiyaç duyulur