13ra Clase 28/6/2023

75.43 Introducción a los Sistemas Distribuidos
95.60 Redes y Aplicaciones Distribuidas
TA048 Redes

Tema: Seguridad en Redes

Capítulo 8 de *Computer Networking: A Top-Down Approach. James Kurose and Keith Ross. Publisher: Pearson, Edition: 7th, 2016.*

Dr. Ing. J. Ignacio Alvarez-Hamelin

Clase de hoy

- Principios de Seguridad
- Problemas que enfrenta la seguridad
- Algunos elementos para generar seguridad
- ¿Redes Seguras?

Principios de Seguridad

- ¿Por qué las redes necesitan seguridad? (*hacking*)
- Confidencialidad
- Integridad de la Información
- Autenticación de los extremos
- Prevención y Detección de ataques que comprometan la seguridad

Problemas que enfrenta la seguridad

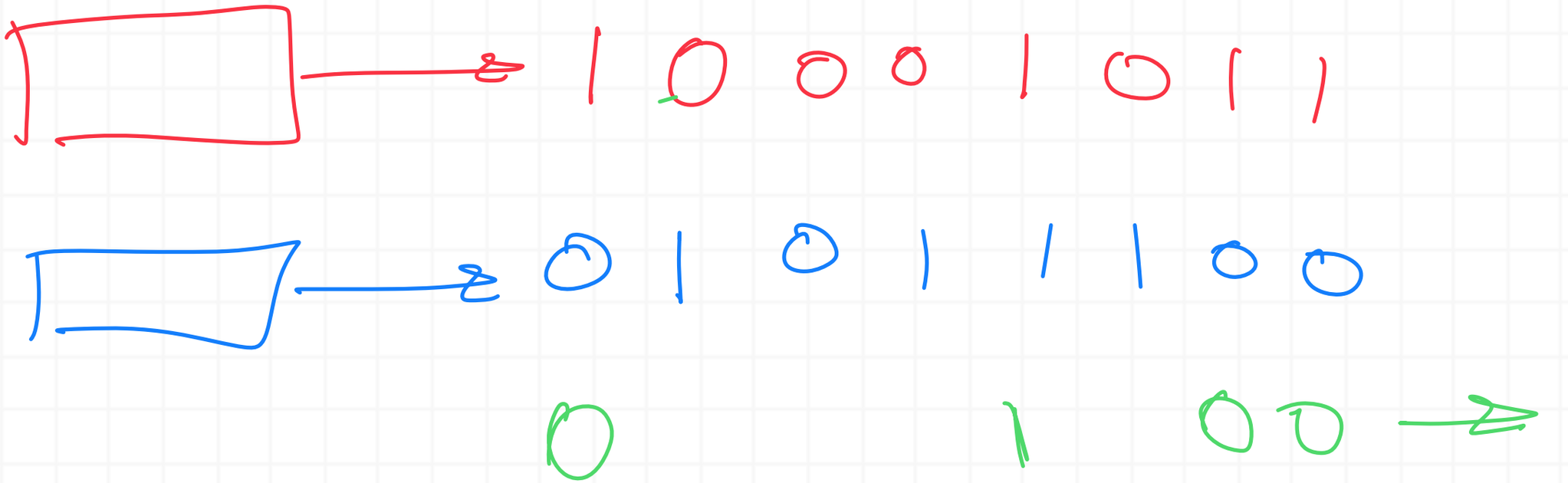
- Lógica de la seguridad (tipos de ataques)
- Eficiencia computacional (cifrado, *hashing,* etc.)
- Cripto-análisis
- Confianza

Last Rotor Machine

https://read.nxtbook.com/ieee/spectrum/spectrum_na_september_2021/the_last_rotor_machine.html

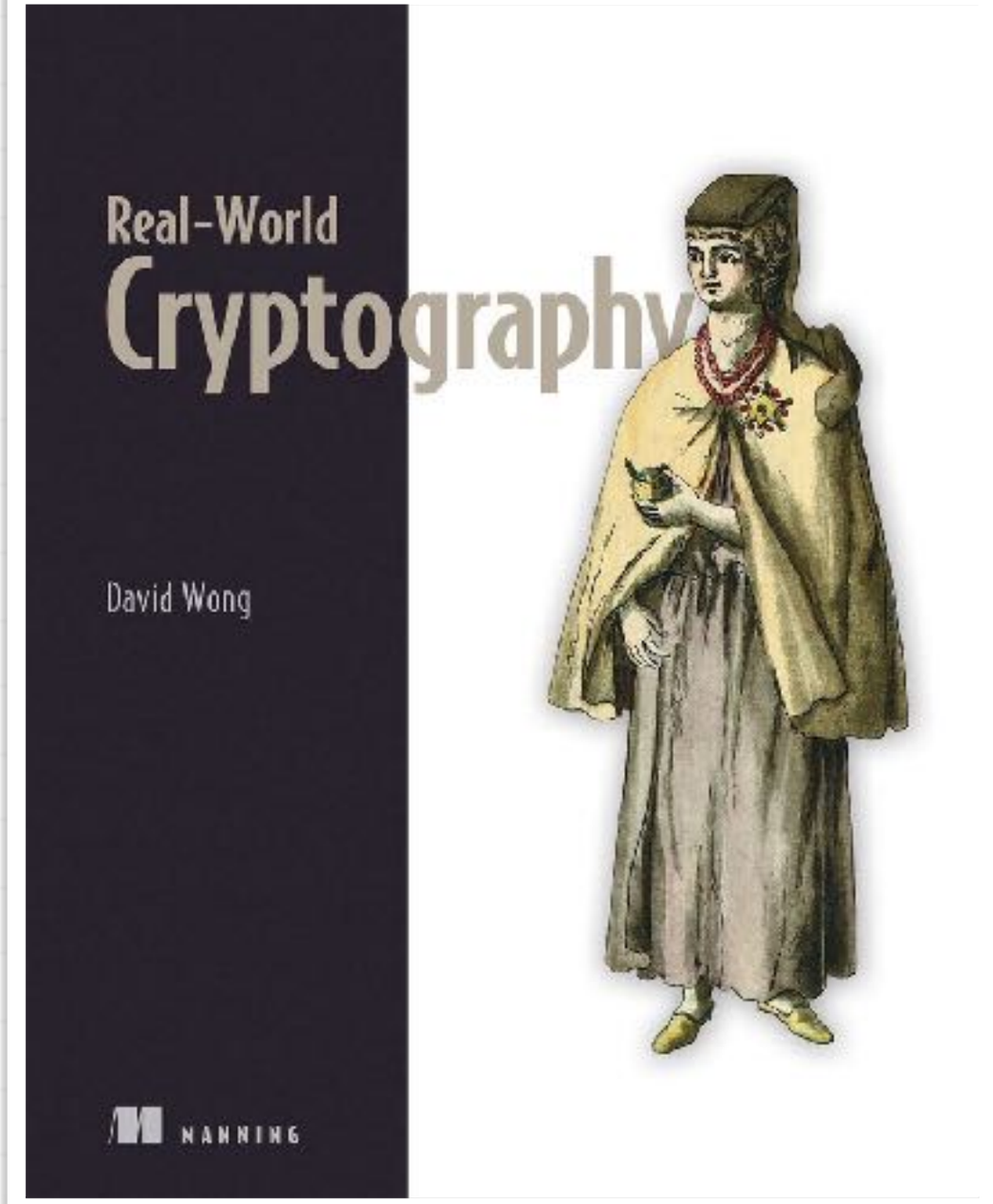
Algunos elementos para generar seguridad

- Clave pública y privada
- *XORing*
- *Shrinking Generator*



Our construction uses two sources of pseudorandom bits to create a third source of pseudorandom bits of (potentially) better quality than the original sources. Here quality stands for the difficulty of predicting the pseudorandom sequence. (In general, through this paper, we use the notion of pseudorandomness and predictability in a rather informal way, although we rigorously analyze and prove some of the random-like properties of the resultant sequences). The sequence we build is a subsequence from the first source where the subsequence elements are chosen according to the positions of '1' bits in the second source. In other words, let $a_0, a_1, \ldots$ denote the first sequence and $s_0, s_1, \ldots$ the second one. We construct a third sequence $z_0, z_1, \ldots$ which includes those bits a_i for which the corresponding s_i is '1'. Other bits from the first sequence are discarded. (Therefore, the resultant sequence is a "shrunken" version of the first one). Formally, for all $k = 0, 1, \ldots$, $z_k = a_{i_k}$, where i_k is the position of the k-th '1' in the sequence $s_0, s_1, \ldots$. We call the resultant pseudorandom generator, *the shrinking generator (SG)*.

Coppersmith D., Krawczyk H., Mansour Y. (1994) The Shrinking Generator. In: Stinson D.R. (eds) Advances in Cryptology — CRYPTO' 93. CRYPTO 1993. Lecture Notes in Computer Science, vol 773. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48329-2_3



Real-World Cryptography
David Wong

.

¿Redes Seguras?

- Aplicación: E-mail, ssh
- Transporte: SSL, TLS
- Red: IPsec
- Enlace: WiFi WEP, WPA, VLANs
- *middlewares: Firewalls, packet-filtering, DPI: Depth Packet Inspection (IDS: Intrusion Detection Systems, IPS: Intrusion Prevention Systems),*

IP tables @IP

@ Port

Protocolo

Establecida