ICMC USP
SÃO CARLOS

GANESH

Stream Ciphers

One-Time Pad

- Encriptação:
  - $E(k,m) = m \oplus k = c$
- Decriptação:
  - $D(k,c) = c \oplus k = m$
- E(k,m) e D(k,c) são determinísticos
  - XOR

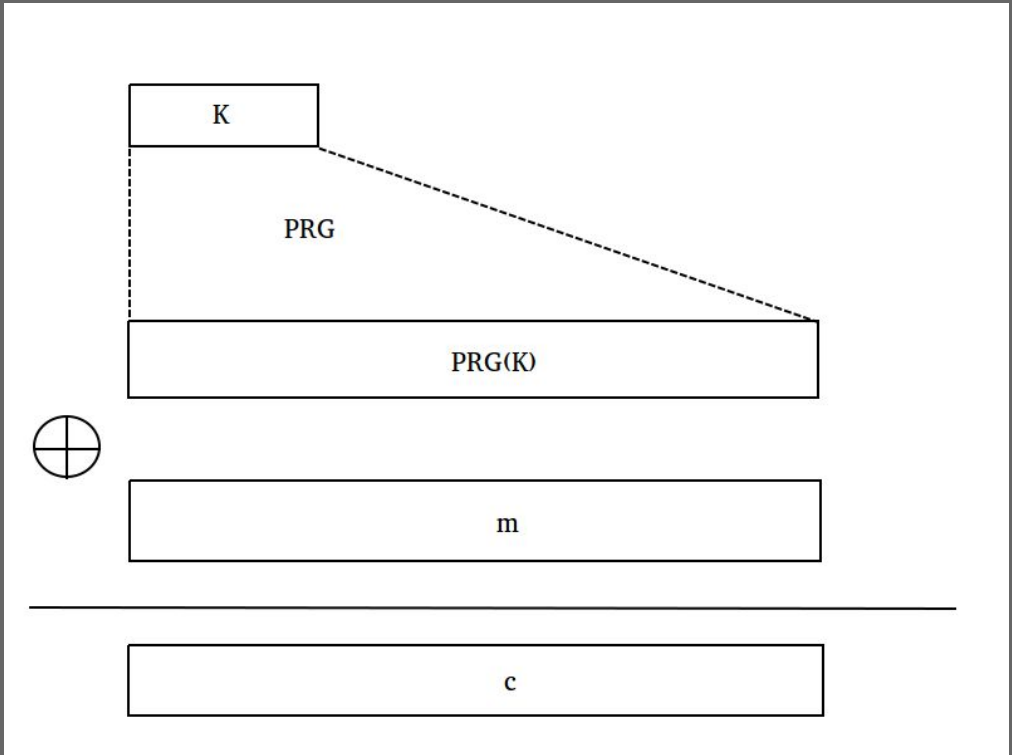
One-Time Pad

- Seguro porém impraticável na maioria dos casos
  - Chaves muito grandes e únicas
    - |k| >= |m|
  - Solução: Stream-Ciphers

Stream Ciphers

- Função geradora de números pseudo randômicos
  - Keystream (S)
  - PRG(k) = S, t.q.|S| ≥ |m|
- Semelhante ao OTP, trocando k por S

Stream Ciphers



Stream Ciphers

Stream Ciphers

- Encriptação:
  - $E(k,m) = m \oplus PRG(k) = c$
- Decriptação:
  - $D(k,c) = c \oplus PRG(k) = m$
- E(k,m), D(k,c) e PRG(k) são determinísticos

Stream Ciphers

- Não garante *perfect secrecy*
- A segurança depende do quão “boa” (randômica) é a função PRG(k)
- Deve ser imprevisível

Exemplos

- RC4 (SW)
  - WEP
  - Enviesamento
- CSS (HW)
  - DVD
  - Bluetooth (E0)

eSTREAM (2004-08)

- Profile 1: "Stream ciphers for software applications with high throughput requirements"
  - Salsa20
- Profile 2: "Stream ciphers for hardware applications with restricted resources such as limited storage, gate count, or power consumption."

Stream Ciphers Modernas

- PRG: $\{0,1\}^s \times R \dashrightarrow \{0,1\}^n$
- ascd
- Nonce: Um valor que não deve ser repetido para uma dada chave
- $E(k, m ; r) = m \oplus PRG(k ; r)$
  - O par (k, r) deve ser usado apenas uma vez

Salsa20

- Fácil em HW e rápida em SW
- $\{0,1\}^{128 \text{ ou } 256}$ x $\{0,1\}^{64}$ ---> $\{0,1\}^{n}$
- ChaCha

Salsa20

- Protocolos
  - DNSCurve
  - DNSCrypt
- Redes
  - cjdns (ipv6)
- SOs
  - Chromium OS
  - Linux Kernel
- https://ianix.com/pub/salsa20-deployment.html


KAHOOT!
0x0D

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br