Symmetrische Kryptografie

Stromchiffren

Ein kurzer Einblick

Martin

Chaos Computer Club Cologne e.V.
https://koeln.ccc.de

19. Oktober 2015

Gliederung

Stromchiffren

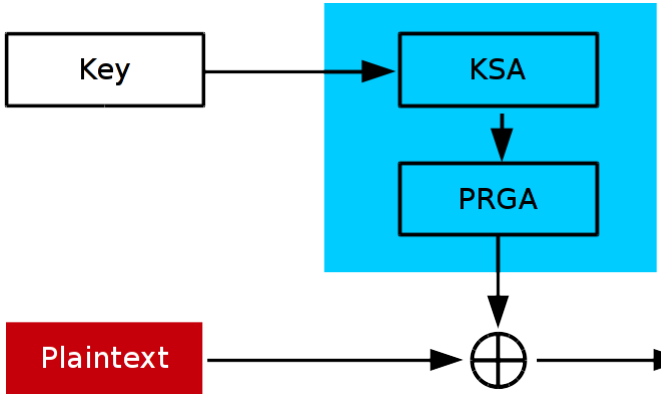
- operieren Bitweise (keine Blöcke)
- schnell
- wenig Hardware

Gliederung

Daten und Fakten

- Stromchiffre (Stramcipher)
- “Rivest Cipher 4” (Rivest **R**SA)
- 1987 entwickelt
- 1994 geleaked
- proprietär RSA Security
- schnell in Software
- besser nicht mehr verwenden
- wird aber noch verwendet (2013 BEAST Attack auf AES-CBC in SSL/TLS)

RC4 - Funktionsweise



KSA - Key Scheduling Algorithm

RC4 KSA

```
for i in range(0, 256):
    s[i] = i

j = 0
for i in range(0, 256):
    j = ( j + s[i] + ord(key[i % len(key)]) ) % 256
# 256 ^= 2^8; keylength in byte
    swap(i, j)
```

PRGA - Pseudo-Random Generator Algorithm

RC4 PRGA

```
i = 0
j = 0
while(counter > 0):
    i = (i + 1) % 256
    j = (j + s[i]) % 256
    swap(i, j)
    cipher_stream = s[ (s[i] + s[j]) % 256 ]
    print(cipher_stream),  # represent as bits and xor
    counter -= 1
```

Fluhrer, Mantin and Shamir Attack

- Sicherheit des Systems hängt von der Geheimhaltung des internen Status (S-Box) ab
- die ersten Ausgaben von Status basierten Systemen lassen auf den internen Status schließen
- 2001 Fluhrer, Mantin and Shamir (R**S**A) Attack
- unter anderem betroffen WEP

Klein's Attack

- 2005 Andreas Klein
- Mehr statistische zusammenhänge zwischen Key und Cipherstream
- **Pseudo**-Random Generator Algorithm...
- WEP-Angriffe wie wir sie heute kennen (Laufzeit unter 5 Minuten)

NOMORE Attack

- **N**umerous **O**ccurence **Mo**nitoring & **R**ecovery **E**xploit
- 2015 Katholieke Universiteit Leuven, Belgien (Rijmen, Daemen haben dort studiert...)
- TKIP (WPA) in 1 Stunde
- Cookie stealing in RC4 gesicherten SSL/TLS Verbindung (70 Stunden)

laut englischer Wikipedia “RC4” vom 18.10.2015

Gliederung

Daten und Fakten

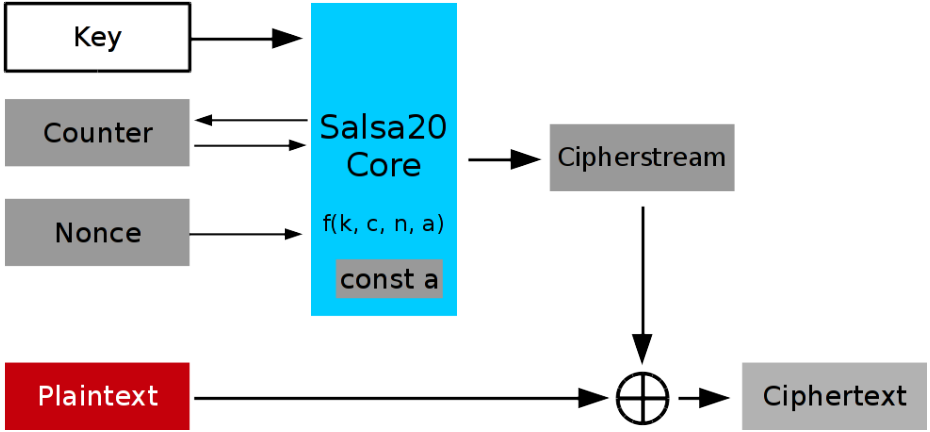
- 2005 von Daniel “djb” Julius Bernstein
- USA “export” Kryptografie - Hashfunktionen nicht beschränkt
- auch bekannt als Snuffle 2005
- beschreibt eine Familie Salsa20/8, Salsa20/10, Salsa20/12, Salsa20/20, XSalsa20/20, ChaCha...
- http://cr.yp.to/snuffle.html

Worte

Wort

In diesem Zusammenhang entspricht ein Datenwort 32 bit, also 4 Bytes.

Übersicht

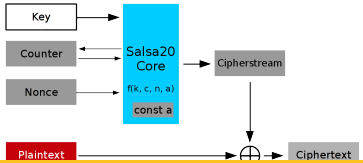

Key
Counter
Nonce
Salsa20
Core
f(k, c, n, a)
const a
Cipherstream
Plaintext
Ciphertext

Funktionsweise

Salsa20 Core

$\text{Salsa20/x}(k, n, c) \rightarrow b$

- *Key k (8 Worte) (empfohlene Länge 256 Bit bzw. 32 Byte)*
- *Counter c (2 Worte)*
- *Nonce n (2 Worte)*
- *Konstante a (4 Worte)*
- *Ergebnis-Block b (16 Worte bzw. 64 Byte)*



Salsa20 Core

Salsa Status und Rundenfunktion

- *Salsa20/x hat x Runden*
- *Quarter-round:* $b \oplus = (a \boxplus c) \lll d$
  - *Addition mod* $2^{32} (\boxplus)$
  - *Rotation* $(\lll)$
  - XOR $(\oplus)$
- *16 Wort-Status (Key, Counter, Nonce, Konstante)* $\rightarrow$ *16 Wort Status*
- $4 \times 4 = 16$ *... kann man als Matrix schreiben*
  - *gerade Runde: Quarter-round auf alle 4 Zeilen anwenden*
  - *ungerade Runde: Quarter-round auf alle 4 Spalten Spalten*

Salsa Quarter-round

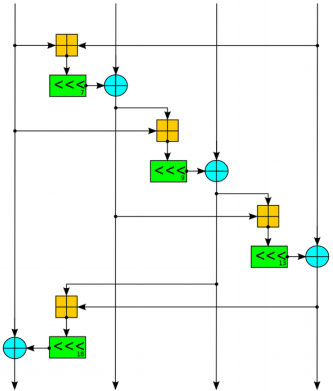


Abbildung: Sissssou; Wikipedia
https://en.wikipedia.org/wiki/File:Salsa_round_function.svg

Salsa Status und Rundenfunktion

- *Addition mod* $2^{32}(\boxplus)$
- *Rotation* $(\lll)$
- XOR $(\oplus)$

Sicher?

- Bester Angriff auf Salsa20/8 mit 2^{250} Operationen (2012) cr.yp.to/snuffle.html
- djb empfiehlt 256bit (32 Byte) Key

Ende

Fragen?