Applied Computer Sciences and Biosciences

HOCHSCHULE MITTWEIDA
University of Applied Sciences

RC4 Algorithmus

Quentin Stickler, B.Sc.

April 7, 2024

Agenda

1. Benutzerdefinierte Anpassungen
2. FAQ

The Rise and Fall of RC4

Why it's not really used anymore

- Stream cipher with variable key-size length
- Used to be most wiedely used stream cipher in Software applications
- Invented in 1987 by Ron Rivest for RSA security
- Kept secret but got leaked in 1994
- Easy to implement and quite fast
- ...but also very vulnerable

RC4 Algorithm

How does it work?

- Consists of two parts
- Part 1: Initialization
- Part 2: Keystream Generator
- S-Box (Array) with length of 256
- Two 8-byte sized counters i and j

RC4 Initialization

Part One: Filling S-Box and T-Box

- S-Box with length 256
- Counters i and j set to 0
- Linear filling of the S-Box from 0 to 255 (S[0] = 0, S[1] = 1…)
- Following loop will be run:

```
for x in range(256):    ###Initilaze S-Box and T-Box
S[x] = x
T[x] = asciikey[x % keylength]
```

Initialization

Example

- Text = "TestText"
- Key = "TestKey"
- S-Box = [0, 1, 2, 3 . . . , 255]
- Initialization of T-Box:
  - Keylength = 7
  - Ascii-Text = 84 101 115 116 75 101 121

84	101	115	116	75	101	121
84	101	115	116	75	101	121
. . .	. . .	. . .	. . .	. . .	. . .	. . .
. . .	. . .	. . .	84	101	115	116

RC4 Initialization

Part Two: Permutation

- Permutate S-Box based on given key
- We always use modulo n = 256 because of the given length

```
j = 0
for i in range(256):
  j = (j + S[i] + T[i]) % 256
  currentvalue = S[i]
  S[i] = S[j]
  S[j] = currentvalue
```

- At the end: (Pseudo-)randomly generated S-Box

Permutation Example

- S-Box Initialization:

0	1	2	3	4	5	6
...	...	...	...	...	...	...
249	250	251	252	253	254	255

- i = 0
- j = (j + S[i] + T[i] mod(256))
- j = (84 + 0 + 84) mod(256) = 168 mod (256) = 168
- Swap S[i] (0) and S[j] (84)
- S[i] = 84, S[j] = 0

Permutation Example Cont'd

84	1	2	3	4	5	6
...	...	...	...	...	...	...
80	81	82	83	0	85	86
...	...	...	...	...	...	...
249	250	251	252	253	254	255

- i = 1
- j = (j + S[i] + T[i] mod(256))
- j = (186 + 1 + 101) mod(256) = 288 mod (256) = 32
- Swap S[i] (1) and S[j] (186)
- S[i] = 186, S[j] = 1

Permutation Example Cont'd

84	186	2	3	4	5	6
...	...	...	...	...	...	...
80	81	82	83	0	85	86
...	...	...	...	...	...	...
249	250	251	252	253	254	255

- i = 2
- j = (j + S[i] + T[i] mod(256))
- j = (47 + 2 + 115) mod(256) = 126 mod (256) = 126
- Swap S[i] (1) and S[j] (47)
- S[i] = 47, S[j] = 2

Final Permutation

84	186	47	208	12	95	222	212	71	9	26	246	103	38	28	165
138	68	130	10	50	143	72	155	39	139	112	16	79	78	196	146

Thank You

Quentin Stickler, B.Sc.

qstickle@hs-mittweida.de

Hochschule Mittweida
University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Applied Computer Sciences and Biosciences

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de