Applied Computer Sciences and Biosciences

HOCHSCHULE MITTWEIDA
University of Applied Sciences

# RC4 Algorithmus

Quentin Stickler, B.Sc.

April 5, 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]
```

# 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

# 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