

## Bonusaufgabe SPN

Gegeben sei das SPN mit folgenden Parametern:

- $r = 4$
- $n = 4$
- $m = 4$

- S-Box: 

$x$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Aus Darstellungsgründen ist in der Tabelle die Hexadezimalschreibweise verwendet worden. Der Bitstring 0010 entspricht etwa 2 und wird auf D abgebildet, was 1101 entspricht.

- Bitpermutation:

$x$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\beta(x)$	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15

- $s = 32$
- $K(k, i)$  bestehe aus den 16 aufeinanderfolgenden Bits von  $k$  beginnend bei Position  $4i$ .

Alice und Bob verwenden obiges SPN im CTR-Modus mit dem Schlüssel

0011 1010 1001 0100 1101 0110 0011 1111

um sich verschlüsselt Texte zuzusenden. Dabei wird ein Text zunächst ASCII kodiert. An den zugehörigen Bitstring wird eine 1 drangehängt und dann so viele Nullen, bis die Gesamtlänge des Bitstrings durch 16 teilbar ist. Dieser resultierende Bitstring wird dann im CTR-Modus verschlüsselt.

Bob empfängt den Chiffretext

```
000001001101001000001011101110000000001010001
111100011100111111101100000010100010100001110
10000000010011011001110010101110110000
```

den Sie auch in chiffre.txt finden. Wie lautet die zugehörige Nachricht?

### Hinweise:

- Sie können in Gruppen von bis zu drei Personen arbeiten.
- Schreiben Sie ein **kommentiertes** Java-Programm.
- Zum Testen ihrer Ver- bzw. Entschlüsselungsroutine des SPNs können Sie verwenden, dass  $x = 0001001010001111$  mit dem Schlüssel  $k = 000100010010100010001100000000$  zu  $y = 1010111010110100$  verschlüsselt wird (mit dem SPN).
- Bei Zusendung des Programms bis zum **29.03.2021** erhalten Sie einen Bonus von 0.3 auf die Note des ersten Tests. (Aus systemtechnischen Gründen kann aber die Erfahrungsnote am Ende nicht  $> 6$  sein.) **Schicken Sie die entschlüsselte Nachricht in ihrer Mail mit!** Am liebsten wäre es mir, wenn Sie das Programm so abgeben, dass ich es in Eclipse einfach importieren kann, ohne Pfade anpassen oder spezielle Pakete nachladen zu müssen.
- Beachten Sie, dass es sich um Bonuspunkte handelt. Damit können sich interessierte Studierende durch Zusatzarbeit einen kleinen Bonus verdienen. Eigentlich gehe ich davon aus, dass Sie aus Fairnessgründen diesen Studierenden gegenüber nicht versuchen, zu betrügen. Dennoch werde ich dies (auch mit Hilfe von Tools) kontrollieren. Falls dabei ein Täuschungsversuch festgestellt wird (also: (verschleierte) Kopien von Teilen existierender Programme), wird die Note des nächsten Tests auf 1.0 gesetzt.