AES-Tests

-

Abschlussprojekt Modul „Assemblerprogrammierung“

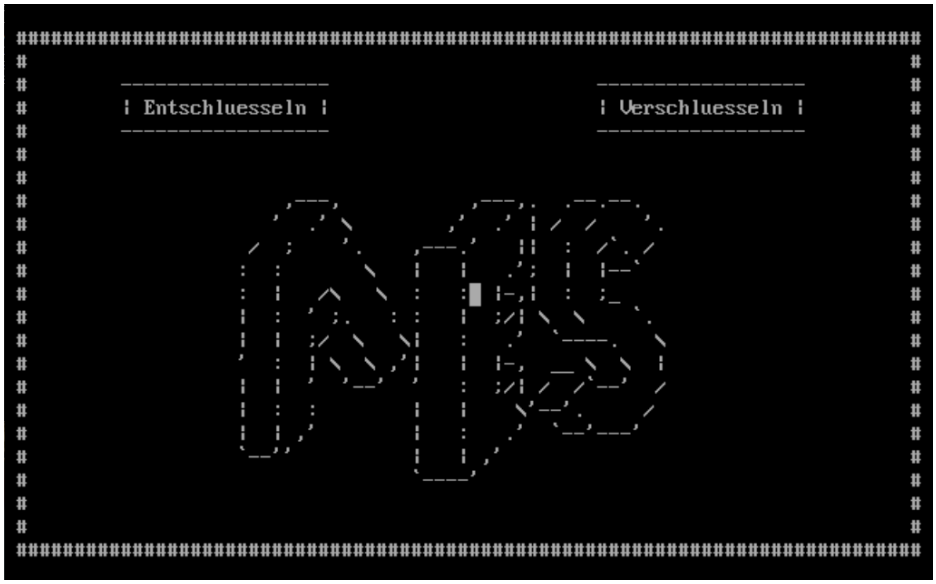
von Konstantin Blechschmidt & Tim M. Kretzschmar

Inhalt:

Testfall 1 – Bildschirmwechsel per Mausklick	Erfolgreich	✅
Testfall 2 – SBOX-Substitution bei Ver- und Entschlüsseln	Erfolgreich	✅
Testfall 3 – ShiftRow & Inverse	Erfolgreich	✅
Testfall 4 – ShiftColumn	Erfolgreich	✅
Testfall 5 – ShiftColumn Invers	Fehlgeschlagen	❌
Testfall 6 – SchluesselAnwenden (PROC)	Erfolgreich	✅

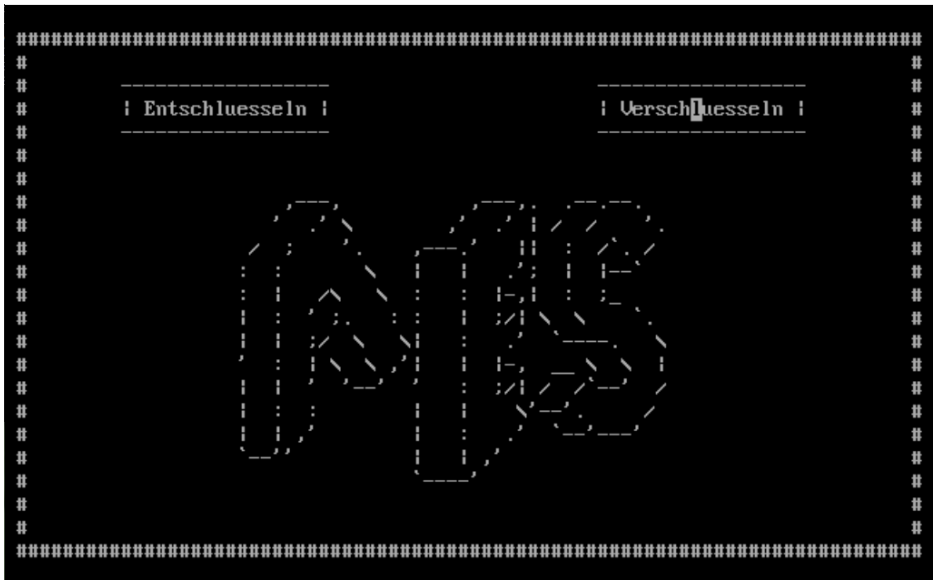
Testfall 1 – Bildschirmwechsel per Mausklick

Hauptbildschirm:



Cursor befindet sich in der Bildschirm-Mitte

Maus über der Verschlüsselung:

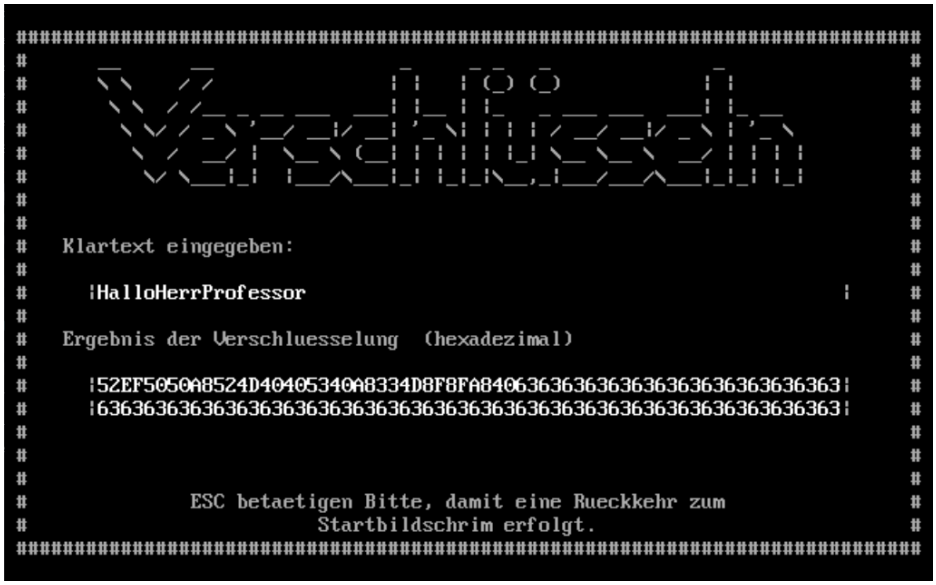


Cursor über der Schaltfläche „Verschluesseln“

Nach dem Klick:

Testfall 2 – SBOX-Substitution bei Ver- und Entschlüsseln

Eingabe Verschlüsselung

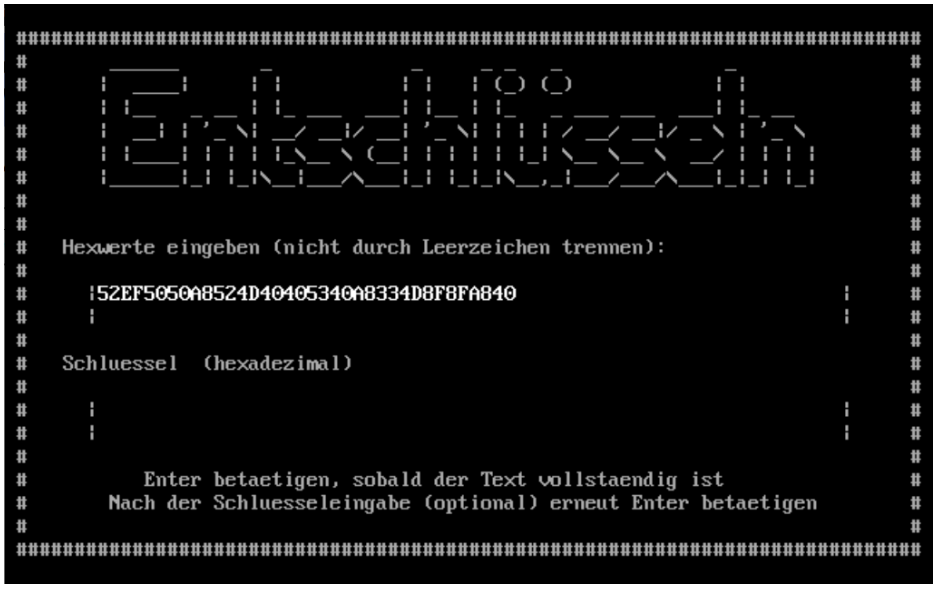


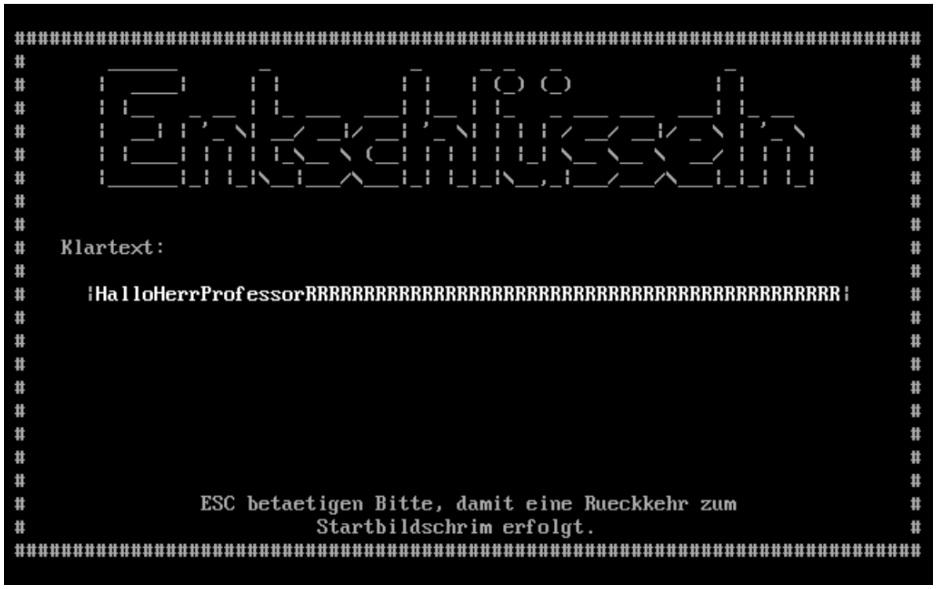
Beweis:

Buchstabe	HexWert (ASCII)	Substitutionswert	
H	48_{hex} (72_{dez})	52_{hex}	✅
a	61_{hex} (97_{dez})	EF_{hex}	✅
l	$6C_{hex}$ (108_{dez})	50_{hex}	✅
l	$6C_{hex}$ (108_{dez})	50_{hex}	✅
o	$6F_{hex}$ (111_{dez})	$A8_{hex}$	✅
H	48_{hex} (72_{dez})	52_{hex}	✅
e	65_{hex} (101_{dez})	$4D_{hex}$	✅
r	72_{hex} (114_{dez})	40_{hex}	✅
r	72_{hex} (114_{dez})	40_{hex}	✅
P	50_{hex} (80_{dez})	53_{hex}	✅
r	72_{hex} (114_{dez})	40_{hex}	✅
o	$6F_{hex}$ (111_{dez})	$A8_{hex}$	✅
f	66_{hex} (102_{dez})	33_{hex}	✅
e	65_{hex} (101_{dez})	$4D_{hex}$	✅
s	73_{hex} (115_{dez})	$8F_{hex}$	✅
s	73_{hex} (115_{dez})	$8F_{hex}$	✅
o	$6F_{hex}$ (111_{dez})	$A8_{hex}$	✅
r	72_{hex} (114_{dez})	40_{hex}	✅
„0“ (Nicht die ASCII 0)	00_{hex}	63_{hex}	✅

Die große Menge an „63“ nach der Nachricht erscheinen durch den Hintergrund, dass der *TastaturBuffer* (das Array zum Zwischenspeichern) mit 0 initialisiert ist und somit alle nicht überschriebenen Werte eine 0 innehaben.

Gegeneingabe Entschlüsseln

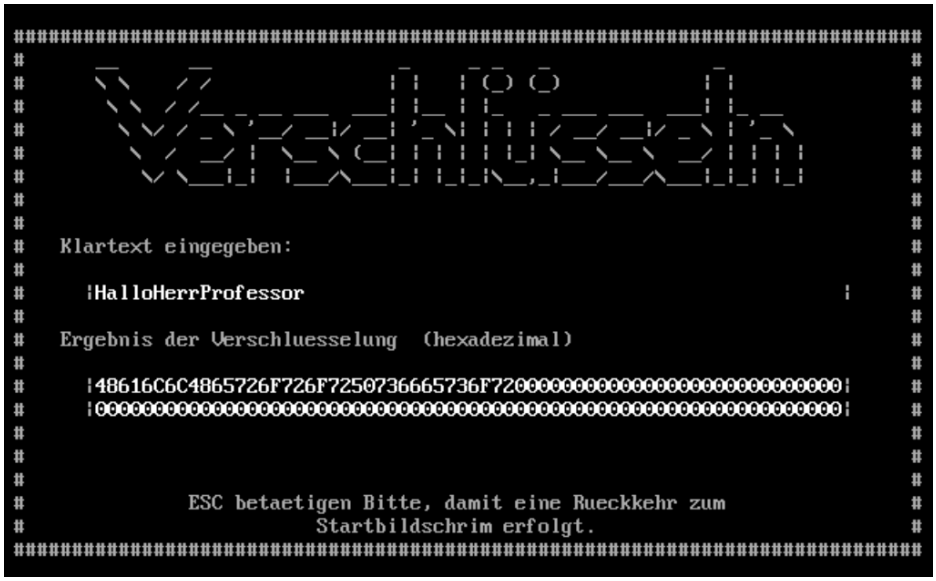




Die ganzen „R“ entstehen wieder durch die fehlende Eingabe (0 bei der invertierten SBox ist 52_{hex} und dies entspricht dem großen R.

Testfall 3 – ShiftRow & Inverse

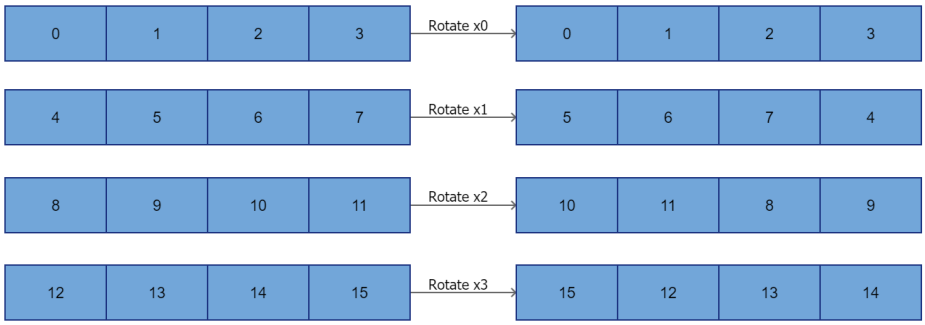
Eingabe Verschlüsselung



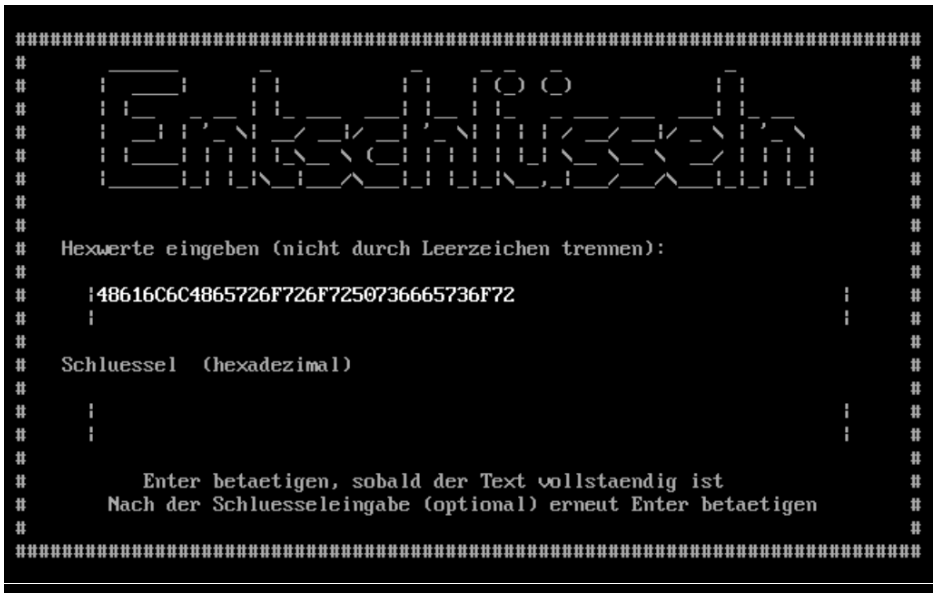
Beweis:

Buchstabe	HexWert (ASCII)	Verschoben	Blöcke	
H	48_{hex} (72_{dez})	48_{hex} (72_{dez})	1	✅
a	61_{hex} (97_{dez})	61_{hex} (97_{dez})	1	✅
l	$6C_{hex}$ (108_{dez})	$6C_{hex}$ (108_{dez})	1	✅
l	$6C_{hex}$ (108_{dez})	$6C_{hex}$ (108_{dez})	1	✅
o	$6F_{hex}$ (111_{dez})	48_{hex} (72_{dez})	2	✅
H	48_{hex} (72_{dez})	65_{hex} (101_{dez})	2	✅
e	65_{hex} (101_{dez})	72_{hex} (114_{dez})	2	✅
r	72_{hex} (114_{dez})	$6F_{hex}$ (111_{dez})	2	✅
r	72_{hex} (114_{dez})	72_{hex} (114_{dez})	3	✅
P	50_{hex} (80_{dez})	$6F_{hex}$ (111_{dez})	3	✅
r	72_{hex} (114_{dez})	72_{hex} (114_{dez})	3	✅
o	$6F_{hex}$ (111_{dez})	50_{hex} (80_{dez})	3	✅
f	66_{hex} (102_{dez})	73_{hex} (115_{dez})	4	✅
e	65_{hex} (101_{dez})	66_{hex} (102_{dez})	4	✅
s	73_{hex} (115_{dez})	65_{hex} (101_{dez})	4	✅
s	73_{hex} (115_{dez})	73_{hex} (115_{dez})	4	✅
o	$6F_{hex}$ (111_{dez})	$6F_{hex}$ (111_{dez})	1	✅
r	72_{hex} (114_{dez})	72_{hex} (114_{dez})	1	✅
„0“ (Nicht die ASCII 0)	00_{hex}	00_{hex}	1	✅

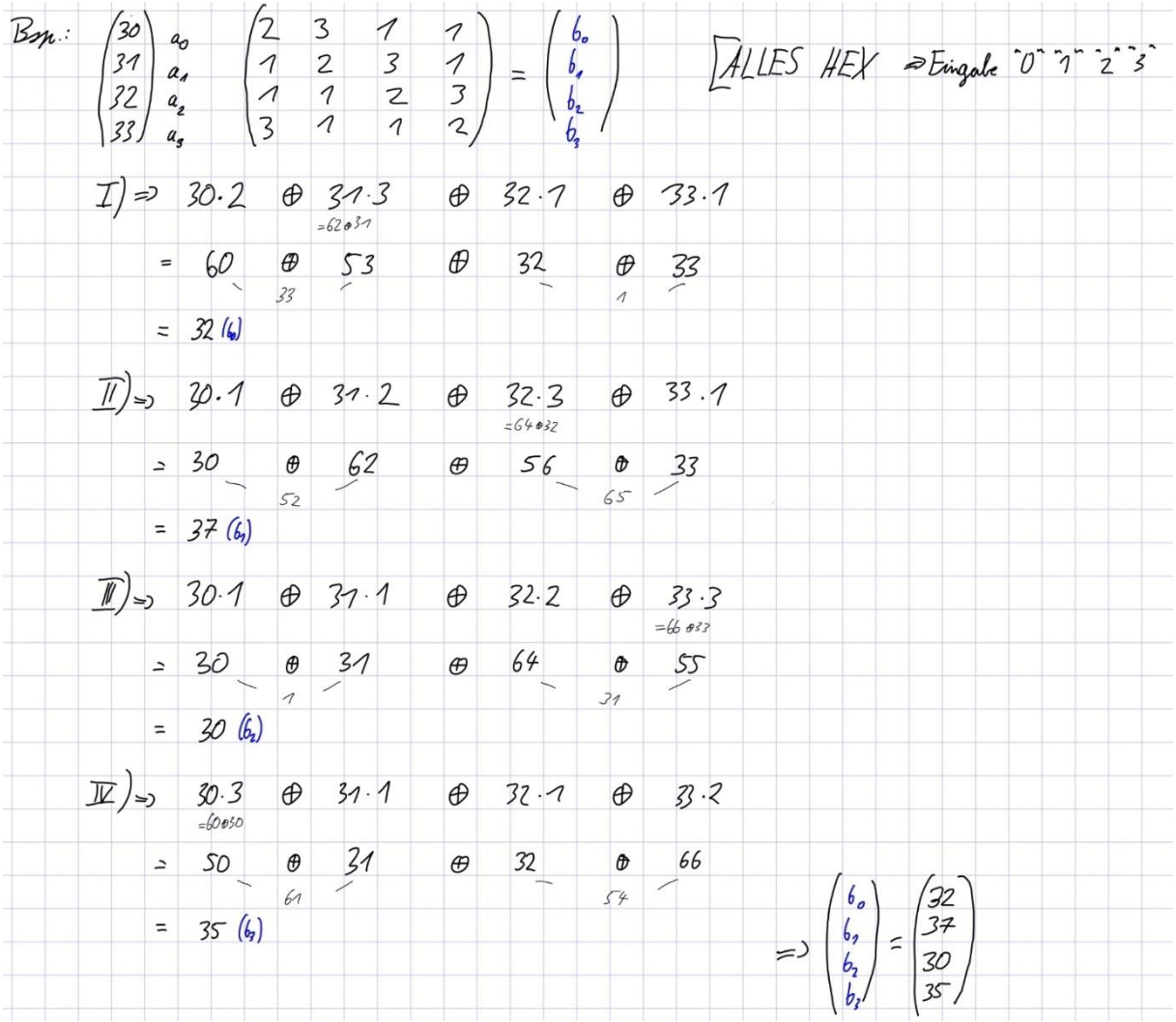
Schema (Verschlüsselung ShiftRow):



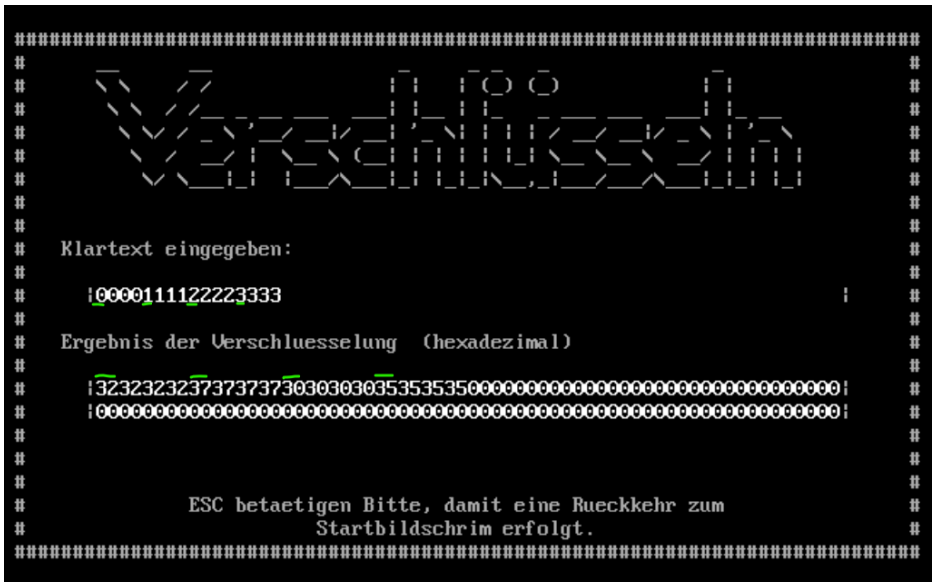
Gegeneingabe Entschlüsselung:



Testfall 4 - ShiftColumn



Screenshot:



Testfall 5 – ShiftColumn Invers

Bsp.: $\begin{pmatrix}32\\37\\30\\35\end{pmatrix}$ $\begin{matrix}a_0\\a_1\\a_2\\a_3\end{matrix}$ $\begin{pmatrix}E & B & D & 9\\9 & E & B & D\\D & 9 & E & B\\B & D & 9 & E\end{pmatrix} = \begin{pmatrix}b_0\\b_1\\b_2\\b_3\end{pmatrix}$ ALLES HEX

I) $\Rightarrow (32 \cdot E) \oplus (37 \cdot B) \oplus (30 \cdot D) \oplus (35 \cdot 9)$

$= 2BC \oplus 25D \oplus 270 \oplus 1DD$ (E1, 3AD)

$= 34C_{(b_0)}$ falsch Soll: 30

II) $\Rightarrow (32 \cdot 9) \oplus (37 \cdot E) \oplus (30 \cdot B) \oplus (35 \cdot D)$

$= 1C2 \oplus 302 \oplus 210 \oplus 2B1$ (2C0, A1)

$= 261_{(b_1)}$ falsch Soll: 31

III) $\Rightarrow (32 \cdot D) \oplus (37 \cdot 9) \oplus (30 \cdot E) \oplus (35 \cdot B)$

$= 28A \oplus 1EF \oplus 2A0 \oplus 247$ (365, E7)

$= 382_{(b_2)}$ falsch Soll: 32

IV) $\Rightarrow (32 \cdot B) \oplus (37 \cdot D) \oplus (30 \cdot 9) \oplus (35 \cdot E)$

$= 226 \oplus 2CB \oplus 1B0 \oplus 2E6$ (E20, 356)

$= 3BB_{(b_3)}$ falsch Soll: 33

$\Rightarrow \begin{pmatrix}b_0\\b_1\\b_2\\b_3\end{pmatrix} = \begin{pmatrix}34C\\261\\382\\3BB\end{pmatrix}$ TEST FEHLGESCHLAGEN

Testfall 6 – SchluesselAnwenden (PROC)

Es wird hier der implementierte Standardschlüssel ohne Expansion verwendet zur Demonstration.

Theoretisch:

Buchstabe	HexWert (ASCII)	Schlüsselwert	XOR Ergebnis	
H	48_{hex} (72_{dez})	51_{hex}	19_{hex}	✅
a	61_{hex} (97_{dez})	DB_{hex}	BA_{hex}	✅
l	$6C_{hex}$ (108_{dez})	AD_{hex}	$C1_{hex}$	✅
l	$6C_{hex}$ (108_{dez})	CF_{hex}	$A3_{hex}$	✅
o	$6F_{hex}$ (111_{dez})	83_{hex}	EC_{hex}	✅
H	48_{hex} (72_{dez})	$9F_{hex}$	$D7_{hex}$	✅
e	65_{hex} (101_{dez})	BD_{hex}	$D8_{hex}$	✅
r	72_{hex} (114_{dez})	27_{hex}	55_{hex}	✅
r	72_{hex} (114_{dez})	$B7_{hex}$	$C5_{hex}$	✅
P	50_{hex} (80_{dez})	FF_{hex}	AF_{hex}	✅
r	72_{hex} (114_{dez})	25_{hex}	57_{hex}	✅
o	$6F_{hex}$ (111_{dez})	$8A_{hex}$	$E5_{hex}$	✅
f	66_{hex} (102_{dez})	$1F_{hex}$	79_{hex}	✅
e	65_{hex} (101_{dez})	$A6_{hex}$	$C3_{hex}$	✅
s	73_{hex} (115_{dez})	$B3_{hex}$	$C0_{hex}$	✅
s	73_{hex} (115_{dez})	91_{hex}	$E2_{hex}$	✅
o	$6F_{hex}$ (111_{dez})	FB_{hex}	94_{hex}	✅
r	72_{hex} (114_{dez})	$9C_{hex}$	EE_{hex}	✅

Screenshot als Beweis: