



**DES Tool**  
**Zum händischen Encrypten/Decrypten mit 3DES**

iDTRONIC GmbH  
Ludwig-Reichling-Straße 4  
67059 Ludwigshafen  
Germany/Deutschland

Issue 0.1  
– 23. June 2023 –

Phone: +49 621 6690094-0  
Fax: +49 621 6690094-9  
E-Mail: [info@idtronic.de](mailto:info@idtronic.de)  
Web: [idtronic.de](http://idtronic.de)

Subject to alteration without prior notice.  
© Copyright iDTRONIC GmbH 2023  
Printed in Germany

## Inhalt

<b>1</b>	<b>Überblick.....</b>	<b>4</b>
<b>2</b>	<b>Beispiele.....</b>	<b>5</b>
2.1	Entschlüsseln des Application Keys aus Kapitel 2.4 .....	5
2.2	Verschlüsseln des Key für Dateizugriff aus Kapitel 2.8 .....	5

# 1 Überblick



The screenshot shows a software window titled "DES 算法工具" (DES Algorithm Tool). It has a menu bar with "加解密" (Encrypt/Decrypt), "MAC运算" (MAC Operation), "XOR运算" (XOR Operation), "分散运算" (Dispersion Operation), and "关于" (About). Below the menu is a "算法选择" (Algorithm Selection) section with three radio buttons: "DES(单倍长)" (DES Single Length), "3DES(双倍长)" (3DES Double Length), and "3DES(空倍长)" (3DES Empty Length). To the right of these buttons is a small cartoon image of Snoopy. Below the algorithm selection are three input fields: "密钥 Key (24 Bytes)" (Key), "数据 Data (8 Bytes)" (Data), and "结果 Result (8 Bytes)" (Result). To the right of the "Key" field is a small box labeled "长度" (Length). Below the input fields are two buttons: "Encrypt" (加密) and "Decrypt" (解密). At the bottom left, there is a checkbox labeled "总在最上" (Always on top).

## KEY (24 Byte)

In der ersten Zeile die 24 Bytes = 48 hexadezimale Zeichen des 3DES-Passwortes eingeben. Die passende Länge von 48 wird rechts daneben angezeigt.

## Data (8 Byte)

Geben Sie hier die zu verarbeiteten Nutzdaten ein.

## [Encrypt]/[Decrypt]

Bitte wählen Sie die gewünschte Funktion aus.

Encrypt: Verschlüssele die Nutzdaten mit dem 3DES-Passwort

Decrypt: Entschlüssele die Nutzdaten mit dem 3DES-Passwort

## 2 Beispiele

### 2.1 Entschlüsseln des Application Keys aus Kapitel 2.4

#### Application Key setzen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 13 2E 60 04 5F FE 9D	First Frame Telegramm 013 = es folgen 19 Bytes Nutzlast 2E = Write Data by identifier 60 04 = Send Key
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 40 02 0E 79 5A EC 1E	Consecutive Frame mit Inhalt
4	1BC00036	22 D0 2D 6B 26 CA B0 AA	Consecutive Frame mit Inhalt
5	1BC1B000	03 6E 60 04	Bestätigung vom RFID-Schloss

5F FE 9D 40 02 0E 79 5A EC 1E D0 2D 6B 26 CA B0 ist der Key 760B470545394C0B405F3D3D3457745A (16 Bytes)



Den 3DES-Schlüssel finden Sie in Kapitel „2.1 2DES Key setzen“

### 2.2 Verschlüsseln des Key für Dateizugriff aus Kapitel 2.8

#### Key für Dateizugriff setzen

#	Adresse	Inhalt	Funktion
1	1BC00036	10 13 2E 60 14 05 7E F3	First Frame Telegramm 013 = es folgen 19 Bytes Nutzlast 2E = Write Data by identifier 60 14 = Send Key
2	1BC1B000	30 00 0A	Flow Control: keine Einschränkung bei der Blockzahl, 10 ms Pause
3	1BC00036	21 20 6C 6B D5 EE 8A 74	Consecutive Frame mit Inhalt
4	1BC00036	22 73 E6 79 08 72 E4 AA	Consecutive Frame mit Inhalt
5	1BC1B000	03 6E 60 14	Bestätigung vom RFID-Schloss

05 7E F3 20 6C 6B D5 EE 8A 74 73 E6 79 08 72 E4 ist der Key 5075254A26530F354A5866324234464D

DES 算法工具

加解密 | MAC 运算 | XOR 运算 | 分散运算 | 关于

算法选择  
☐ DES(单倍长) ☐ 3DES(双倍长) ☒ 3DES(四倍长)

密钥 Key (24 Bytes)  
AF706A243F717E4B7D2A5E8B3B3538325A2D73D3975D786D 长度 48

数据 Data (8 Bytes)  
5075254A26530F354A5866324234464D 32

结果 Result (8 Bytes)  
057EF3206C6BD5EE8A7473E6790872E4

Encrypt  
加密

Decrypt  
解密

☐ 总在最上