MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
June 2, 2005

Crypto Contest / Preisaufgabe

for the students of the course Cryptography, SS 2005

The problem is to decrypt the following cipher text:

```
FFFD610E C549A7E0 250FFDB7 91DDBF24 8AA7D9CE 2002A4A2 9301D514 208D9DB6
84DB3225 7B4BA4DB 982DB862 EA444A12 E46C82E3 0EEE25F0 D8AE3FC1 85BD59DD
ECA611CE E2459E7D 434A671D 445899EC 93600D40 7EA70A7A 39397EE1 79C6AF61
512C3B63 FEFB2B4F FAF0C78A F127E5A3 7B055C50 982DB862 F2EE6CF1 394B4026
9A641AD3 127D925F C8D17B2B C8B0DFBA 38B96D28 BD9009F8 F16BD858 38519AD3
A6A50A21 BCF72E49 7720E01A 1AA51DCF 5F1AB677 127D925F 09FFA083 F11EF8A0
6EC0F9A4 D765FEE9 986A17BA B83B58F3 D4667A56 48324C78 2AEC50AA 2BD6EAD1
7EA70A7A F70744A3 B9ED5C59 BEF06499 A2168848 F4D02761 C598149B 2E32BC07
D3A1685B 3AE0C84F 7A0AB270 589B168C E66E2A24 F4FCB7E1 0BE3530C 4A0E8909
BF8AF5F3 296DA49A 798E67F6 512F4824 7E884F72 8B96221A ED6CCFF1 73972068
9188DEDE 59F28BC3 7EA70A7A 940BB8CF 0714FDD3 7F1B86F7 D254F27E 4329A899
B4C004D8 9D7DAAF9 127D925F 2FAC2EF6 BB74BE56 830530F5 29A0C1C9 21612FFF
AF4C37DB 1FD7A597 EF49F2D7 D66F0757 B55477F1 1D2C6C19 DB11AD0B 6D6768F7
765EDFB2 56652FA5 CDF17CFA 769DFB83 A047AD0F 9D1F329B F17D5AE3 AABD8311
A4EFFA62 CBDB2BC1 E7CCA6B9 CA8B2A83 E4355B2B
```

This cipher text was obtained from an English ASCII plaintext using a block cipher in ECB mode with a block length of 4 bytes (32 bits) and a 4-byte key (a_1, a_2, a_3, a_4). The encryption algorithm consists of 4 rounds, where a_i serves as the i-th round key $(i = 1, \ldots, 4)$. A detailed description of the round function can be found overleaf.

Solutions, together with a short explanation of the method used, should be sent by Email as soon as possible, but not later than July 4, 2005, 24:00 h to

`forster@mathematik.uni-muenchen.de`

Winner is who first returns the correct solution. The winner (or the winning team) receives 32 extra marks and a modest prize.

To save you typing, a data file containing the cipher text can be downloaded from the homepage of the course

`http://www.mathematik.uni-muenchen.de/~forster/vorlA5s_cry.html`

You might also be interested to have a look at the three previous crypto contests in 1996, 1999 and 2002.

Wishing you a successful decoding

Otto Forster

---

p.t.o.

Description of the round function

$$F : \mathbb{Z}_2^{32} \times \mathbb{Z}_2^8 \to \mathbb{Z}_2^{32}, \quad (x, a) \mapsto F(x, a).$$

The round function makes use of the binary operation

$$\boxtimes : \mathbb{Z}_{256} \to \mathbb{Z}_{256}, \quad (x, y) \mapsto x \boxtimes y$$

(cf. problem 17), which is defined by $x \boxtimes y := \phi^{-1}(\phi(x) \cdot \phi(y))$, where '$\cdot$' denotes multiplication in the field $\mathbb{F}_{257}$ and $\phi : \mathbb{Z}_{256} \to \mathbb{F}_{257}^*$ is the bijective map defined by $\phi(x) = x$ for $0 < x < 256$ and $\phi(0) = 256$.

For an element $x = (x_1, x_2, x_3, x_4) \in \mathbb{Z}_{256}^4 \cong \mathbb{Z}_2^{32}$ and a round key $a \in \mathbb{Z}_{256} \cong \mathbb{Z}_2^8$ we define

$$g(x, a) := (y_1, y_2, y_3, y_4) := (a \boxtimes x_4, \overline{a} \boxtimes x_3, a \oplus x_2, \overline{a} \oplus x_1).$$

Here $\overline{a}$ denotes the bitwise complement of a and $\oplus$ is the bitwise `xor`.

The result $y = (y_1, y_2, y_3, y_4)$ is interpreted as an element

$$y = (y_1 \cdot 2^{24} + y_2 \cdot 2^{16} + y_3 \cdot 2^8 + y_4) \bmod 2^{32} \in \mathbb{Z}/2^{32}\mathbb{Z}$$

and subjected to the map

$$f : \mathbb{Z}/2^{32}\mathbb{Z} \longrightarrow \mathbb{Z}/2^{32}\mathbb{Z}, \quad y \mapsto f(y) = y(1 + 2y).$$

$\mathbb{Z}/2^{32}\mathbb{Z}$ is again identified with $\mathbb{Z}_2^{32}$. We then define the round function by

$$F(x, a) := f(g(x, a)).$$

Some test vectors to check your implementation (hexadecimal notation):

x	a	$F(x, a)$
00000000	00	04FBFD01
00000000	A5	0919ECA2
04FBFD01	00	6F754C2D
0919ECA2	A5	2702C225
74686520	A5	058D35B6
058D35B6	5A	3DC41FA0