Kryptographie

SS 2010

Timo Hanke
Templergraben 64, 2.Stock, Raum 227
email: hanke@math.rwth-aachen.de

Veranstaltungswebseite:
`http://www.math.rwth-aachen.de/~Timo.Hanke/krypto/`

Ciphertext:

```
yifqfmzrwqfyvecfmdzpcvmrzwnmdzvejbtxcddumj
ndifefmdzcdmqzkceyfcjmyrncwjcszrexchzunmxz
nzucdrjxyysmrtmeyifzwdyvzvyfzumrzcrwnzdzjj
xzwgchsmrnmdhncmfqchzjmxjzwiejyucfwdjnzdir
```

Bestimme in dieser Reihenfolge:
`E,D,N,H,T,A,I,O,S,R.`

Neuer Ciphertext:

```
OiRqRIENDqROveARISEpAvINEDHISEveTbtxASSuIT
HSiReRISEASIqEkAeORATIONHADTAsENexAhEuHIxE
HEuASNTxOOsINtIeOiREDSOvEvOREuINEANDHESETT
xEDgAhsINHIShHAIRqAhETIxTEDieTOuARDSTHESiN
```

Rate jetzt: `U,F,C,W,L,K`

Neuer Ciphertext:

```
OURFRIENDFROveARISEpAvINEDHISEveTbtLASSWIT
HSUReRISEASIFEkAeORATIONHADTAKENeLACEWHILE
HEWASNTLOOKINtIeOUREDSOvEvOREWINEANDHESETT
LEDgACKINHISCHAIRFACETILTEDUeTOWARDSTHESUN
```

Rate jetzt: `M,P,G`

Neuer Ciphertext:

```
OURFRIENDFROMPARISEpAMINEDHISEMPTbGLASSWIT
HSURPRISEASIFEkAPORATIONHADTAKENPLACEWHILE
HEWASNTLOOKINGIPOUREDSOMEMOREWINEANDHESETT
LEDBACKINHISCHAIRFACETILTEDUPTOWARDSTHESUN
```

Raten jetzt: `X,V`
Schlüssel: `CGHWZQTNM*SXVRYE*FDJIKUPB*`
Kommen nicht vor: `J,Q,Z`

1	2	3	4	5
S	I	H	F	C
’	R	F	E	S
T	I	F	R	Z
C	S	T	I	H
I	R	C	F	S
F	E	S	H	I
E	H		C	

4	2	1	5	3
F	I	S	C	H
E	R	’	S	F
R	I	T	Z	F
I	S	C	H	T
F	R	I	S	C
H	E	F	I	S
C	H	E		

Ziele:

1. Vertraulichkeit
   (=Geheimhaltung bzw. Zugangsbeschränkung)

2. Integrität (=Nicht-Veränderbarkeit)

3. Authentizität (=Urheberschaft),
   evtl. sogar beweisbar (=Unterschrift)

4. Anonymität
   (=Geheimhaltung von Absender/Empfänger)

Darauf aufbauend: Identifikation, . . .

Die primitiven $f \in \mathbb{F}_2[X]$ mit $\deg f = 8$:

$$
\begin{aligned}
&X^8 + X^7 + X^6 + X^5 + X^4 + X^2 + 1,\\
&X^8 + X^7 + X^6 + X^5 + X^2 + X + 1,\\
&X^8 + X^7 + X^6 + X^3 + X^2 + X + 1,\\
&X^8 + X^7 + X^6 + X + 1,\\
&X^8 + X^7 + X^5 + X^3 + 1,\\
&X^8 + X^7 + X^3 + X^2 + 1,\\
&X^8 + X^7 + X^2 + X + 1,\\
&X^8 + X^6 + X^5 + X^4 + 1,\\
&X^8 + X^6 + X^5 + X^3 + 1,\\
&X^8 + X^6 + X^5 + X^2 + 1,\\
&X^8 + X^6 + X^5 + X + 1,\\
&X^8 + X^6 + X^4 + X^3 + X^2 + X + 1,\\
&X^8 + X^6 + X^3 + X^2 + 1,\\
&X^8 + X^5 + X^3 + X^2 + 1,\\
&X^8 + X^5 + X^3 + X + 1,\\
&X^8 + X^4 + X^3 + X^2 + 1.
\end{aligned}
$$

AES ohne Rundenschlüssel.

	00000000000000000000000000000001
sub:	63636363636363636363636363637C
shift:	6363637C63636363636363636363
mix:	7C7C425D6363636363636363636363
sub:	10102C4CFBFBFBFBFBFBFBFBFBFBFB
shift:	10FBFBFBFBFBFB4CFBFB2CFBFB10FBFB
mix:	361010DD4C4C398E2C994E2CDD361010
sub:	05CACAC12929121971EE2F71C105CACA
shift:	05292FCA29EECAC17105CA19C1CA1271
mix:	94EC3786706A10C63E27D06EBF09BC62

$$F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

$$F^*(x,y,z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$$

$$\frac{\partial F^*}{\partial x} = a_1yz - 3x^2 - 2a_2xz - a_4z^2$$
$$\frac{\partial F^*}{\partial y} = 2yz + a_1xz + a_3z^2$$
$$\frac{\partial F^*}{\partial z} = y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2$$