Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 7

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen			**Gruppe**	**Tutor**
1	2	3	**Summe**	**bearbeitet**
2	2	3	5 Punkte=100%	

Man identifiziere im Folgenden Bitstrings $b_n \ldots b_0$ mit Vektoren $(b_n, \ldots, b_0) \in \mathbb{Z}_2^{n+1}$, mit natürlichen Zahlen $\sum_{i=0}^{n} b_i \cdot 2^i$ und mit Polynomen $\sum_{i=0}^{n} b_i X^i \in \mathbb{Z}_2[X]$.

Durch diese Identifikation wird die Ordnung der natürlichen Zahlen auf die obigen Polynome, Vektoren und Bitstrings übertragen.

Dokumentieren Sie nun sorgfältig Ihre Lösungswege.

1. Finden Sie das "nächste" irreduzible Polynom $f \in \mathbb{Z}_2[X]$, welches im Sinne obiger Ordnung auf X^{256} folgt.

Mit Hilfe dieses Polynoms konstruiert man den Körper $E := Z_2[X]/<f>$. Die Elemente dieses Körpers lassen sich gemäß obiger Vereinbarungen als 256bit-Bitstrings auffassen, die ggf. "links" mit Nullen aufzufüllen sind.

2. Interpretieren Sie die als Dezimalzahlen gegebenen Zahlenpaare
1919604824822619899693188064867867692206043376174897959078725617216144748692278130614133625033873861444084712146649035566502513960013243938546829392697069

5104770908063605316725295452636552409289320671701495631315192423163366359777598084178255618145165669074682802801106551688354443002990738714801915710712183

als "verteiltes Geheimnis", d.h. als Paare $(x_1, a \cdot x_1 + \text{key}), (x_2, a \cdot x_2 + \text{key}) \in E \times E$, eliminieren Sie das Element $a \in E$ und berechnen Sie nun das Element $\text{key} \in E$.

Das Geheimnis **key** wurde also in zwei "shares" aufgeteilt.

3. Fassen Sie **key** als 256 Bit AES-Schlüssel auf.

Informieren Sie sich über "Base-64-Codierung".
Installieren Sie das Programmpaket OpenSSL auf Ihrem Rechner.
Studieren Sie die Dokumentation.
Mit OpenSSL können Sie auch Base-64 codieren/decodieren.

Wandeln Sie **key** in eine Hexadezimalzahl und entschlüsseln Sie mit OpenSSL und mit diesem Hex-Key und mit dem Initialisierungsvektor iv=0 das folgende in Base-64 Codierung vorliegende mit AES256-cipher-block-chaining verschlüsselte Dokument.

```
9w/FdFMma0YFlP3SlRxoVdfARLjNDcee/KDnTgxzuyxJz2ZAzvmiQiSPzQ2N6qpb
aRgfD8xVdZJr3HmIe+uFJRK1VIbYjxndWrXWP9s+ERFdBEsS3+VhRC9S5jOmwPl1
KrPiBJYxeASdIChG+vMjzt/3Z7UFoovUxmwJ8Tc1tT1hLoF9HvdmkD9awHjelpAe
nGiX5iVJ3H0ms8nmj5yEDDMhb+uPTSej5o9Xv909vXVSZ01KoO73VSoen5Bstk7A
4Oh0KDHUPYuXj6m2wCWDJdDxJ8rXu3oyhgHgz31paCbDYi1Dw92jRrImsNqEujb5
37TZZwuzSoiEqnMwDaz24+McofhwTZzEfu9wOzGyPHsgybeOgGmNPgqEGh6bNQB2
EVY2p9DHUVKfDH+2Ibj7smh+UFScKgc1S1d9bEcjuTcI3/0b7es9a+jPXZ6szTUG
3G26qIPH/f1bjI/b4S57mnjLJ0IzYwuvoX/2VjfB0wsxlDJjH81R/c6ERxbah0Ts
oEer+4J0NeDSpOhtwa9ZuoIowuxnM2i7fVTvGKSy/kyi4LbFI3O2AwDrQmII8GXJ
n9ikwDHxwrLFl+FV1eKQKxFRUD6yBBktaOKCoGxoULqz+ouBMH8WMNbYJYqNzrF/
XIo2wu9REcwqUT2o4kWMjpiuyL8yAvn11Q8MiXWerub2xgj4sJDOwLMd7dxTtn6g
RYyPzGu0Nne7JsKmqfi79ZHxpjZyPp7+6LdVT0uiryjEMfn6ItdrBtmUvExbmioL
wFzWNR48e4esjYWYrp+3EEY7iGrxCtGB5mlL2s17GM2Nv3PES0gmwInddAknbY7X
Avu2ZjgO/reJSwIbLK6S6+xVmucQWlot4c0ehxOgw6UOY7ovD73IjQWIv9wEjuiu
Z6DiRzg+Hn+9bCb83vaPu3fvKfc92GJ90HOWXyTBttHk30eyDltt/9dtIvjlJ88g
k+ouc6XzqsRD6WFutL09ZJVcn2vWuxP0wRg8hZUSFe1rUE774F4cE/bIOLHCqu+S
x1w8zQD5Iof0F08i/H7ivm+tFc5syEcnGONqB68fChKfmzFNjiDqDkDyr8sojNbS
vKEDKjKtfHdhorlJ6TlDWg2x2LCRZ02cdhKwOhR/MNv1Ge9y5qC2ReEAFzPgahm6
15ElBkxRuLO0FfaL31d7eYHmxGaUuCbmhpu1ywcVjreqShTkMmFEIBGTOi5hpmIQ
4oIaJmRcgdt7n4gRa6ecrrOilBZ8C76YY2wFT9S6rNE+lUDGfjoHs37IIRYueuhp
JeVryX2RRa8plR4vkOtV0GOzG+xE0F0zBabLnrNd2W3IeFbwwjyjvWJQsjCYLGDP
UkgPuef7TZn4pckNfflGYopL+uVIidYbDhgB/zd7NZwpkzzjlWVA7C6/VbOHUq3y
dd3k2fnhtE7cnCshK2j7FlRtmNfZjoVLEEupp0fyFn86L0QWyLEU82dJdSuY5BZS
LGY266m31Q/y601v3fXlcdCeJFXwm/ZCAcrZCpHkEFrlNiMM1WuITrVSBm+l1Gx8
1inpZ3OzQBobIYfE8DaU0Y1DHVCbCz+zCnVwuRIYPbxjzWC/zWsfOOGEuM5oBuMm
YuzEp+lPX1CfgrfHD4WpnbI0LUIXu60wZqAfcJuAxjUslsTKy5PntREHuxTi473u
aJkXQVBRzoNjLKQeS4QMQqrs53zqGGKtHah7VOLitnH60sE3zMIMDFiwZAjXTWoK
dgFXXbPP3yrSy/gYLvpSpKUoD2q8m63MSK4vn0dGwM2n1f/NafJjPjApNVAXk4gG
iquU7xVVV9ZAhY4f3BwYDFlLU6TtSm0vC3duwj/p9SjRFpjDjAuDtLqUPXBDo/fh
Cj3V9cvMXjH91wZdXN9i5PMsh0+Zwbt6tA6k5JdfLfQWcZ/qe63VaI//3zjxXFfb
XQ4TV8fp2mmL/Q4s36b83Y0SlRLGsw+DK2N3uD/G8pFvI76xF5tdNBbMnn5WZN26
9vqPK6MmMkFt7m0hk+sr6/Vphz2ShyYpEkH7MZSbuffu9B05B5N/Na4ond6YSbar
z520fpgff1fpk6gKXsTsMLNLnwKaxwhRpyB2gKCB+yAD+KxKVK7Os8wXpqJIiKQt
MTXO6MsCv0JjxzQ3WBH1QyzAX9WvL/K7J42FPpU1XrfWwV3hch4PDsoeu4yOpcgl
ki0IdO9BerBPC7+Hz/oROtahnvT0Z21Ewg8CugwofrLw0FCQQ+aSFGVe7AgvidXF
zKFNcSaTADOvgv7MuTywpVCmUHszAPV/BYeHOiDQxpdXHs2kerHcNo9sYSAJiHFI
4IcPfsMVid/uDkLRUvMkimr+BSdQwfKxPA9G7kDXNvi+6DPK5Om8SrF74iEr6j2C
xplvLlBQA/dBiVs5YOu+maccqyg0D/YfBi6zb7957qyppCqBX2R42430ARJ1B6wY
d2u3HgL7ABSniNoZ76B9xxb0byTuutQACvarx6ftmZQTWD7nIHzXqbjQWeXpGZHR
QlYK2X39Fg+uB+EylknYu3jA9OJWBgiVxCFFigYHCC2pSDumNRR9JqVcOdcuqEN3
Er7+5rteVFo0Q/Syo5FnKSYQdfViI6ZO0wn/+jcLV0PPruR7S2uX5pk25Hd9gZTG
```

vj66XLZZ51iahyFqzRaEFso0dC+mEjYEQ54IW5YYyIIWKuvJjPAXgiQi5uq6pgqd
r43zWyvmaU+GHXRIj/dCf3yz+Oimsbf5JedEtEzNUlOx/u6aXBCCpMcWrot73ncM
9hH7NEWdt/XApWN3qF7VTjqm/hKiEvtSe0yqpNndyO1BS7zf9HjaOTb4RArqXiLM
PBf7ZOz1mw1hw09cUueZ1ujjKwSUlGMZdRk6OCGYwt97leuzjUOgAIPia/NHsUe2
/MJFqyOjlL1hluqUFaaLMtwjj2vANec+oR4NuC3Wrr7AO/JJng+8JUEmLD5VgS/7
4SotI0wYdLq1GdcpBx3eb0r3OWiqWrNgnzwAh3S+lH6eA/5eYbz21adp91kypOKn
G2FW4AfivYunhPnBVRmPJwB1dUY9lCMfiFvuAkOE9/qNyCaAFkt3HwKsPUae1rte
j5Lv+sS6pWQiFBjzipYBvY913OuI2isGW1lmIv6P5l8Kz5AIOEpydZ3fF8EsCo11
EW6HbGtJrjlTeTMVORmVBQsEvy7RA4z3P25/9BEanXV/jMlaB4tUSByfousu8cIL
hDseq4Nc/U3tSOFabsirVVbvyHjME2tebw81+N9HFJJ6bwKk18EYHqXpYlCxLgHh
Vw+5VhCVz9mTWcgxLD1+HKwuqDUucB/CY13w3GkqOGIKnSapegJlupEP/qhcPvMX
iVKX3jj7THDU2JO7d/Nzo64Dcj5jcPO4cuGpYBP31cCmS1dEBARSddHjUzQFelVy
LwCQCuF6ijHwDJSHrvsGZ/WgFSUwNErE+u274pToi8VVscmZn+gaC8vE8Iu1s3pG
aqwG5aqvCm4n7HapkZmmnErCadA9tk3JCWf3LgH/esfmShRcVNLpKvtI/vwykbkL
6m+ia2c3TmMEG6i/S13mEiEDCdJkExfLl6DfHHLxDIArfvAzwSi5XzEOHahHxKjZ
hs6eFhsSyIul9i5MB3rRoNgiQ9jO3QVvyuXtvOpW15YtdPiFxX+G5mNvkN+3coKo
JzbtI/KzV1vfhnh6Z1AcqxVcD0wnDqUEGdxVPnYU2hHi8cOboPmO9tUObZVXnfhb
1JesLMo0VxsE+tJNrsHHam2tVw9fByIbjs8OgWYBbIYfPr1gQuN3myB6bE9OHJSk
3TeZr1uy9/0IpcRXuz37TQ2ohyBDUE53hloOY47DgAr4qVD7m0CMJzypuWLh/9jN
oTq18iBPkOTEB4AE1zvclGua7LVd1TjlFbFAnvYR5MFjKgNoThkgyV45jVEL6crM
4x4NewO2BYY0M/j/E0NihdMT9iwxWPhgBf0zkjxcJoGuRC7xB98tV9SRuXhcgXq5
aJWHfQnw6BiepeCpH0UEc1GZ/ciRd16tgGMLMEDUFJVZKtx4fMS1x2iol7dvElbj
1m+MXoK1BnRHuXcvK5KiYR/ei2AiP1RVzzqm/MabJzpVuPhEfjkXpMeXdyzad1P4
ogRk9trBYBXGAzmVh1fiOQ9pA6aGJuAVZ0S2Tzs9dGtmPg4tqYzfiNjCHKqgmwSd
MIgGZ8OBcREUd7aScc+TdLwDoLF5lgoxuZeFllEf83w58OE7aKuGvcls0vdo10dJ
G2/JBRwqYQYBlSHXBQ06nJ9totFCR7kn3AXNPmYM+sZpxZ4uZxoWel2zImFFOTOV
L1r5mAG7a9LvvGxVQFugN3r2AMsjIYFR0JuyHRIA4NPH8M9oXAZWVoLkHe+8WGXj
XqbFwJpN8Q31eojAMdhqAvMU6h6OcYd/oH28dkLErYE2nWQT6XGPJUwh8XcjsNP2
GGuXfQFAq566OxchuBgWvWuy41T8PAOtCAr7JxJGppdGmoNXUkXaFL435p45zRNY
6fOM9iDFdgp/icTklt8KX95hGblkElDkZPCNFUhZXFYYFvWwPE2sSgtOdCj6dkDu
0kbruAaKGsS/KNHbSp8yvd/9LzSH0Q3WVP05Z8+Vf2wbaQcCQKvnnsxUlmghl/C6
5VzmP7hAiZGeN6wJEtdv8nGmnmReeroNwLhwxEjLX/QowbiDThJTI3DvlZDqgl1w
Dpfscm65sLmUExraz3RXp+yim/S0WCr+7nEoKxrEEB8mHhkOih1Gpyo/YWP0+NOE
CY9VOGh6EfefoDsLtrbc+RPopiNLlH+KRXKM2+hNi6l5sv7D7yZpvBlcZftDjwZC
+LRLSFNnvRuzFj3fE/XFVDoGxQkxLA96BcE2DjJEGl2a6xQtvIixZekhz1VLR4r5
7viehNGZY0dnxTtQiKARvy2LFSHGu4/LedH3L285DkirZZsBsmW/yftxV/Ds7ZWe
VB+AA3960oPr+ypXqP/N+/T3M5cqrv4cXIhbaULv+b8Q04X8e5990QBMEIECiPUb
xwSL7tDB0lt04fvlgXP95xe9HNokUshfbMH6ABIrEgQdKEbdKapSrmIh165mtUm1
N5l/YZ7iAskRMtyFu3SljPNXtFR/B04zxKzaOv9oxEtYDCxoiJqS6boh9q1Vp32k
HcZm16YMK4WymaOIRuVD+i6/DTzW+zRf0KDQx0SWw2w6TfXD17rjPn54bn2v9ppy
Xr33H+mE3AsI2zbWTRJDd1TetiiSWWIrJInjqER5rcbG6GaVE4cJ1kydm/mER3vY
wiJ2dvjMEYRMZkMHftoa4du4cH2Bjj7BYhE0nDFo+mijfedKxo6VY9POjXkEvhK4
6+otEuRfaYh/im5qlQbgcYBn2jWLIFVYLd6HKX5+MJ1uOd5PtjpJ1L9O7HBY0gZW
ezqpjW+GXSEIuLOPAIHlwfzJIKK0Kcd5i2hfBUz7w9N6A7Zz4kye2CT1tuQ3YGhX
zvx2qrgVuoq6YDn2hNxTt0bjxzciFgcrfX7A38i8iCI3Cj1X5I/cZxj57nFBK5LL
oVYABTaPdzmswdLraL6f5suyIafrvKuPRthy8sSGncPuqeud6ZaukbfS2pKnG3lx
KpT3/tWnlGEmW2u8UQ5ZFj5l54HCPvfC0bB6aUMA3cU7rEqy7OCnkRiIDNSYTYSk
gIR4GKNZd9dUhuh6+ADl2j6iuY0BVQWUnbTRB1/cMEIBzQAS1V1n998IiO5i4p4j
unNiqzS3bA/0moRVyQEDJ2PcgJyKs2LZxAHkOCJ7UpEjxLqUbbEiDHDqVHKkXArT
jt9U5kSAUEg7ZyS9JBSNvqAX0j3vAMOmhmNNFATWskinjySCw60wHIz5seksbda9
TE/5wGyxP9xfp68YvXyOaGlja9m/xT+u9xzXiuMzProcMP6WGwm63CHT5HXTCAvC
YkqxXUzgypBdJmyyjGuhGVUnWE4MsQlR/zuYYdJapPRk23Xr63T3ST7r8guDArai
qQ0vsZcnpFDyCIXxhCdJ2U0M+/I34vtggUckRwUnY0wBu6nEMCaw5SUmVFZxgstH

e+yjp78NOCm2QBHlltmwT4LRiWUPhKlT7OWSQzFcu6PgVsC4n+GXItKkPJa900on
PGd9jx2r5EsP+ZrUr7aNlpzKXXvXSRmNFWPMi6HAfL/WFchcmKlMNvfDbfN+376X
xicXWQ+uscwwOeE+SfwpaQ/BSgbePpbVAaJRkdj8iQfeAuikD6aUiKKbab4qivQ2
iCy1MD20F5soVQNVIE1TdgbtgdC18x+EVkeLqefcrvMxztg1PXNFVCAIYnZl97OP
bFi7JI+ucKChbzytfqDbMO5UA7TeK5ANgSPnPgUQfaT6BRtNF/P9XsWAavqbz8xd
CC+oJI3HebJAm4EZXFKtYb+DGoF5XcK6BfdgnmUP4aCXF7y6y4ubwD53PYN/s3y+
LnR0KOg6LPg6RYuIxkE8FGjSR+UTfJmWb9mLv0knz6n4PJtaAmPLlv8/meEeSLW7
zbbRXc288HcO4XzpfB1vvYMNbvt/eCQyHsMxwv8NC8ySiHhGlIpxtYoQB7N82H1c
qvSg+ZTWAQFpIC+ag/wrDTTSfgm6h2GZbwS4lsgQg7QwRevigDKtslJRcQe/lOQS
8tgOde8XNFI+48NCd8KOZcoSpIlOinn8gCL7eSuxjX9XteuN7r4/e9syZ7OnnfNO
4SLUYRLI5qzUAsfuPO2pXHcasUgYwazC6l29cH1afFHWBgXw2ljYqWLWJCAOGhf5
qdvOyfC5FsuvaRDYjg9sLEWqiQG8mVLZNIkh88RLdyTL4eamtDqi2EvtGVMRawWM
BKecZ12tv9gtzDe4Y/fmgfdNLuYohfmSVkr3egUDflS/2D9lZbldWp6sUzlZglRd
sRa7X6B3Y/vt9X4vysJ0dD09d/wBGZdFuwnf+IVRsmSciF2g6NtxKje5T5Npcwz7
oEzFXs2bekB9r5xGm3Jb/UaQ+vIwHFE4FVzOS1GZloPUJ4QHPTyzhKsrgUG0O9A/
+HsTV3TO9zusc+wxzFMg1Ddj0siWZBhehA5T29rea5LaZr489ar+pXWGRKi9mnA8
479mmnQiIbyW8OPY1VuKYg6368EXf7iz/I1sHxJk/bd202jkB2ZaibaJsV97q/Sx
X8ppzSZuzOPbqlLrOZFvFgyoCspeAd98nlunymC1rWV8Fed0V3nyPRi7KnK5m2g3
cP5bkObfKn1DMaPNefPZzBMPLsPPDHiH1AlmGnNPxSCwApQDHgtBg6V7FzGGD6YV
9oThHbDxgSdneOnTUtwRYxmHkG54A2+UD8OQ4W4V7o9XfeloSEjH1988Pn5vaCuT
k1ILXkDmRVyeVQFgzrVF4dAvQV0YelF9bwdV6IgEiiZ3PKalUdFYqjkKehOXivV6
7uWQGVOr7TueuO5CosT2wTMuqRKmIqzyzeiVAhOvD1wItd5XfjIfwAKTmIXbnup5
gNtTESvWgbEyB+uHUPTFn9riIdSBjhP5+C6xvoH5nHhWrId8gszJcoE7KpAtt99j
IHIEgPsNJu+yRahfersP2+VgKrTfgZbA7O1JiAb9xUpsZAPDfqW7lNfiavmlFuuN
uD2Q+Ig1cohtGEIN7i+XIFPt3CasNQ7vUfcm37pUxYJ23OPmJYGiCoO/XMF/eRMA
yzw+qf7rkJjDMPCGpQBXFlHsGORkzHcSXphTuXzHInylIFELak0BCPAmLsyOtJZi
8QlgnHSZ9/e76qVhpyRtIf09UCtxDgHQyVJw2y4Bru0sVhhJZWIjMMgdY0C86Ubq
v35uaqjcmgfeLP7k/DfskLxGjD461jPs0Vq4tJJvbUWlexJdMJVQEu6rp0jZWv0O
/kNuuJS8uEBKt/Nq0dMh5kT30AxLnkLEVdAkftJ9K7zuRGKjUobud4nzcj5QXQws
hgXpGNvYnzhOzYbSPntn3afX//CHAhlYvwOgi7IlmzefUsV6konc5d5Q62VRAPjE
2caK0JAjvHoaGqYCH3a/lwoP3fyVxFJRH7z4anrANTrSpVrMshwiUG+ZbGKcdUyw
81mcqI2x04uFJlvO1/V5mhQJItIQiLVCrdTgka94R+vLZ4/PWpCVGxGnMRPGFRge
lvRR0ezJSAGxVmhFPVvDY17pJ/BGCNCYJJHN/Imu8hYHD1kUS0zJBXkJf6svYMfU
pCn8BWrfaOXcxu+dEAG2CZ/GwCTLdoFi9i9Q4L+xueeIw1ZyGaeFA2N6JUOlsvps
NcPP7efGtQn7e8BS3l6GpC1aVCFUlXV4tbJMX+aAuqOnzmbdmY3cUacG6Ci7NncO
WmwsPyngdrFNPFXFxCRww9DmqiDDwD8dnpQVcH+xqXPE/x3GqyT8EdIW1XAvIY+g
KUmPxQ4erADT6dS40AdkqynmUxQyqP1LsmOtwIRcn7g1Sz2iTNL0O5UwVbh9LYwr
vc4VYy5JUTyK1FPPMAqMVw==