Introduction to Cryptography - Exercise session 1

Prof. Sebastian Faust

October 24, 2018

The purpose of this exercise session is to consolidate the basic knowledge about Private Key Encryption, like the one of *Shift Cipher* and *Perfect Secrecy*, introduced in Chapters 1 and 2 of the book.

Exercise 1 (Shift cipher 1)

Let us consider an example of *shift cipher* following the definition given at Slide 25 of the lecture notes, where $\mathcal{K} = \{0, ..., 25\}$ with $\Pr[K = k] = 1/26$ for each $k \in \mathcal{K}$. Say we are given the following distribution over $\mathcal{M}$:

$$\Pr[M = \mathtt{a}] = 0.7 \text{ and } \Pr[M = \mathtt{z}] = 0.3.$$

(a) What is the probability that the ciphertext is B?

(b) What is the probability that the message a was encrypted, given that we observe ciphertext B?

Exercise 2 (Shift cipher 2)

Consider again a *shift cipher*, where $\mathcal{K} = \{0, ..., 25\}$ with $\Pr[K = k] = 1/26$ for each $k \in \mathcal{K}$. This time consider the following distribution over $\mathcal{M}$:

$$\Pr[M = \mathsf{kim}] = 0.5, \Pr[M = \mathsf{ann}] = 0.2, \Pr[M = \mathsf{boo}] = 0.3.$$

(a) What is the probability that $C = \mathsf{DQQ}$?

(b) What is the probability that ann was encrypted, conditioned on observing the ciphertext DQQ?

Exercise 3 (Perfect secrecy)

Let Π be a perfectly secure encryption scheme with message space $\mathcal{M}$, key space $\mathcal{K}$ and ciphertext space $\mathcal{C}$. Assume that $\Pr[C = c] > 0$, for every $c \in \mathcal{C}$. Prove that following statements hold:

(a) $\forall m \in \mathcal{M}, \forall c \in \mathcal{C}$:

$$\Pr[C = c] = \Pr[C = c | M = m].$$

(b) $\forall m, m' \in \mathcal{M}, \forall c \in \mathcal{C}$:

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[\mathsf{Enc}_K(m') = c],$$

where the probability is taken over the choice of K and randomness of Enc.

(c) Π is perfectly indistinguishable.

(d) $|\mathcal{K}| \geq |\mathcal{M}|$

Exercise 4 (Vernam cipher)

(a) Consider a *shift cipher* Π as defined on the lecture and additionally assume that $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$ and $\Pr[K = k] = 1/26$ for each $k \in \mathcal{K}$. Prove that Π is a perfectly secure encryption scheme.

(b) Design a perfectly secure encryption scheme Π' such that $\mathcal{M} = \mathbb{Z}_{26}^n$ for $n > 1$. In other words, design a perfectly secure scheme that encrypts messages consisting of n character. Prove that your scheme is an encryption scheme (i.e. satisfies correctness) and that it is perfectly secrure.

Exercise 5 (One-Time Pad)

When using the one-time pad encryption scheme, it can occur that $k = 0^l$. In this case, since $k \oplus m = m$, the ciphertext is equal to the plaintext and the message is sent in the clear! It has been suggested to improve the one-time pad by only choosing non-zero keys, namely keys such that $k \neq 0^l$. Is the proposed version of One-Time-Pad still perfectly secret?

Exercise 6 (Cryptanalysis - Voluntary homework exercise)

Decrypt the following ciphertext (Hint: the plaintext is in English)

```
BT JPX RMLX PCUV AMLX ICVJP IBTWXVR CI M LMTR PMTN, MTN YVCJX CDXV MWMBTRJ
JPX AMTNGXRJBAH UQCT JPX QGMRJXV CI JPX YMGG CI JPX HBTWR QMGMAX; MTN JPX HBTW
RMY JPX QMVJ CI JPX PMTN JPMJ YVCJX. JPXT JPX HBTWR ACUTJXTMTAX YMR APMTWXN,
MTN PBR JPCUWPJR JVCUFGXN PBL, RC JPMJ JPX SCBTJR CI PBR GCBTR YXVX GCCRXN,
MTN PBR HTXXR RLCJX CTX MWMBTRJ MTCJPXV. JPX HBTW AVBXN MGCUN JC FVBTW BT JPX
MRJVCGCWXVR, JPX APMGNXMTR, MTN JPX RCCJPRMEXVR. MTN JPX HBTW RQMHX, MTN RMBN
JC JPX YBRX LXT CI FMFEGCT, YPCRCXDXV RPMGG VXMN JPBR YVBJBTW, MTN RPCY LX JPX
BTJXVQVXJMJBCT JPXVXCI, RPMGG FX AGCJPXN YBJP RAMVGXJ, MTN PMDX M APMBT CI WCGN
MFCUJ PBR TXAH, MTN RPMGG FX JPX JPBVN VUGXV BT JPX HBTWNCL. JPXT AMLX BT MGG
JPX HBTW'R YBRX LXT; FUJ JPXE ACUGN TCJ VXMN JPX YVBJBTW, TCV LMHX HTCYT JC JPX
HBTW JPX BTJXVQVXJMJBCT JPXVXCI. JPXT YMR HBTW FXGRPMOOMV WVXMJGE JVCUFGXN,
MTN PBR ACUTJXTMTAX YMR APMTWXN BT PBL, MTN PBR GCVNR YXVX MRJCTBRPXN. TCY
JPX KUXXT, FE VXMRCT CI JPX YCVNR CI JPX HBTW MTN PBR GCVNR, AMLX BTJC JPX
FMTKUXJ PCURX; MTN JPX KUXXT RQMHX MTN RMBN, C HBTW, GBDX ICVXDXV; GXJ TCJ JPE
JPCUWPJR JVCUFGX JPXX, TCV GXJ JPE ACUTJXTMTAX FX APMTWXN; JPXVX BR M LMT BT JPE
HBTWNCL, BT YPCL BR JPX RQBVBJ CI JPX PCGE WCNR; MTN BT JPX NMER CI JPE IMJPXV
GBWPJ MTN UTNXVRJMTNBTW MTN YBRNCL, GBHX JPX YBRNCL CI JPX WCNR, YMR ICUTN BT
PBL; YPCL JPX HBTW TXFUAPMNTXOOMV JPE IMJPXV, JPX HBTW, B RME, JPE IMJPXV, LMNX
LMRJXV CI JPX LMWBABMTR, MRJVCGWXVR, APMGNXMTR, MTN RCCJPRMEXVR; ICVMRLUAP MR
MT XZAXGGXTJ RQBVBJ, MTN HTCYGXNWX, MTN UTNXVRJMTNBTW, BTJXVQVXJBTW CI NVXMLR,
MTN RPCYBTW CI PMVN RXTJXTAXR, MTN NBRRCGDBTW CI NCUFJR, YXVX ICUTN BT JPX RMLX
NMTBXG, YPCL JPX HBTW TMLXN FXGJXRPMOOMV; TCY GXJ NMTBXG FX AMGGXN, MTN PX YBGG
RPCY JPX BTJXVQVXJMJBCT. JPX IBVRJ ACNXYCVN BR CJPXGGC.
```