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 $\mathtt{B}$?

Solution:
There are only two ways this can occur: either $M = \mathtt{a}$ and $K = 1$, or $M = \mathtt{z}$ and $K = 2$. By independence of M and K, we have

$$\Pr[M = \mathtt{a} \land K = 1] = \Pr[M = \mathtt{a}] \Pr[K = 1] = 0.7 \cdot \frac{1}{26}$$

Similarly, $\Pr[M = \mathtt{z} \land K = 2] = 0.3 \cdot \frac{1}{26}$. Therefore,

$$\begin{aligned}\Pr[C = \mathtt{B}] =& \Pr[M = \mathtt{a} \land K = 1] + \Pr[M = \mathtt{z} \land K = 2] \\ =& 0.7 \cdot \frac{1}{26} + 0.3 \cdot \frac{1}{26} = 1/26.\end{aligned}$$

(b) What is the probability that the message $\mathtt{a}$ was encrypted, given that we observe ciphertext $\mathtt{B}$?

Solution:
Using Bayes Theorem (Theorem A.8 of the Book) we have

$$\begin{aligned}\Pr[M = \mathtt{a} | C = \mathtt{B}] &= \frac{\Pr[C = \mathtt{B} | M = \mathtt{a}] \cdot \Pr[M = \mathtt{a}]}{\Pr[C = \mathtt{B}]} \\ &= \frac{0.7 \cdot \Pr[C = \mathtt{B} | M = \mathtt{a}]}{1/26}\end{aligned}$$

Note that $\Pr[C = \mathtt{B} | M = \mathtt{a}] = 1/26$, since if $M = \mathtt{a}$, then the only way $C = \mathtt{B}$ can occur is if $K = 1$ (which occurs with probability $1/26$). We conclude that

$$\Pr[M = \mathtt{a} | C = \mathtt{B}] = 0.7.$$

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 $C = \mathsf{DQQ}$?

Solution:
The only way this ciphertext can occur is if $M = \mathsf{ann}$ and $\mathcal{K} = 3$, or $M = \mathsf{boo}$ and $K = 2$, which happens with probability $0.2 \cdot 1/26 + 0.3 \cdot 1/26 = 1/52$.

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

Solution:
A calculation as in the previous exercise using Bayes Theorem gives

$$Pr[M = \mathsf{ann}|C = \mathsf{DQQ}] = 0.4$$

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

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

Solution:
For all probability distribution over $\mathcal{M}$, $\forall m \in \mathcal{M}$, $\forall c \in \mathcal{C}$ with $\Pr[\mathcal{C} = c] > 0$, we have from the definition of perfect secrecy:

$$\Pr[M = m|C = c] = \Pr[M = m] \tag{1}$$

From equation (1) and using the Bayes Theorem, we have

$$\begin{aligned}\Pr[M = m] &= \Pr[M = m|C = c] \\ &= \frac{\Pr[C = c|M = m] \cdot \Pr[M = m]}{\Pr[C = c]},\end{aligned}$$

which gives us

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

(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.

Solution:
Let us fix arbitrary $m, m' \in \mathcal{M}$ and $c \in \mathcal{C}$. For part (a) of this exercise we know that

$$\Pr[C = c | M = m] = \Pr[C = c] = \Pr[C = c | M = m']. \tag{2}$$

Additionally note that for every $m^* \in \mathcal{M}$ it holds,

$$\Pr[C = c | M = m^*] = \Pr[\mathsf{Enc}_K(M) = c | M = m^*] = \Pr[\mathsf{Enc}_K(m^*) = c]. \tag{3}$$

The probabilities above are taken over the choice of K and randomness of Enc. We conclude the proof using Equations (2) and (3) as:

$$\Pr[\mathsf{Enc}_K(m) = c] \overset{(3)}{=} \Pr[C = c | M = m] \overset{(2)}{=} \Pr[C = c | M = m'] \overset{(3)}{=} \Pr[\mathsf{Enc}_K(m') = c].$$

(c) Π is perfectly indistinguishable.

Solution:
Consider an adversary $\mathcal{A}$. We state the adversarial indistinguishability experiment $\mathbf{PrivK}^{eav}_{\mathcal{A},\Pi}$ as follows

1. The adversary $\mathcal{A}$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.
2. A key k is generated using Gen, and a bit $b \in \{0, 1\}$ is chosen uniformly at random. Ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. We refer to c as the challenge cipher text.
3. $\mathcal{A}$ on input c outputs a bit b'.
4. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. Formally, $\mathbf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$, if output of the experiment is 1 and in this case $\mathcal{A}$ succeeds.

For every $m \in \mathcal{M}$ let us define the following set:

$$\mathcal{C}_m := \{c \in \mathcal{C} \colon \exists k \in \mathcal{K} \text{ s.t. } \Pr[c = \mathsf{Enc}_k(m)] > 0\}$$

$$
\begin{aligned}
\Pr[\mathbf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1] =& \Pr[\mathcal{A}(\mathsf{Enc}(m_b)) = b] \\
=& \Pr[b = 0] \cdot \Pr[\mathcal{A}(\mathsf{Enc}(m_0)) = 0] + \Pr[b = 1] \cdot \Pr[\mathcal{A}(\mathsf{Enc}(m_1)) = 1] \\
=& \frac{1}{2}\Bigg(\sum_{c \in \mathcal{C}_{m_0}} \Pr[\mathcal{A}(c) = 0 | \mathcal{C} = c] \cdot \Pr[\mathcal{C} = c] \\
&+ \sum_{c \in \mathcal{C}_{m_1}} \Pr[\mathcal{A}(c) = 1 | \mathcal{C} = c] \cdot \Pr[\mathcal{C} = c] \Bigg) \\
=& \frac{1}{2}\Bigg(\sum_{c \in \mathcal{C}_{m_0}} \Pr[\mathcal{A}(c) = 0 | \mathcal{C} = c] \cdot \Pr[\mathcal{C} = c] \\
&+ \sum_{c \in \mathcal{C}_{m_1}} \Big(1 - \Pr[\mathcal{A}(c) = 0 | \mathcal{C} = c]\Big) \cdot \Pr[\mathcal{C} = c] \Bigg) \qquad (4)
\end{aligned}
$$

Now we need to prove that $\mathcal{C}_{m_0} = \mathcal{C}_{m_1} = \mathcal{C}$. For the sake of contradiction let us consider that $\exists c^* \in \mathcal{C} \setminus \mathcal{C}_{m_b}$. This implies

$$\Pr[c^* = \mathsf{Enc}(m_b)] = 0.$$

But then, using part (b) of this exercise, for every $m \in \mathcal{M}$ it holds that $\Pr[c^* = \mathsf{Enc}(m)] = 0$ which implies that $\Pr[C = c^*] = 0$. This is a contradiction with our assumption that $\Pr[C = c] > 0$ for every $c \in \mathcal{C}$.
We can now continue with the simplification of equation (4)

$$
\begin{aligned}
\Pr[\mathbf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1] =& \frac{1}{2}\Bigg(\sum_{c \in \mathcal{C}} \Pr[\mathcal{A}(c) = 0 | \mathcal{C} = c] \cdot \Pr[\mathcal{C} = c] \\
&+ \sum_{c \in \mathcal{C}} \Big(1 - \Pr[\mathcal{A}(c) = 0 | \mathcal{C} = c]\Big) \cdot \Pr[\mathcal{C} = c] \Bigg) \\
=& \frac{1}{2} \cdot \sum_{c \in \mathcal{C}} \Pr[\mathcal{C} = c] \\
=& \frac{1}{2} \cdot 1 = \frac{1}{2}
\end{aligned}
$$

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

Solution:
Assume for the sake of contradiction that $|\mathcal{K}| < |\mathcal{M}|$.
Let us fix a key $k_0 \in \mathcal{K}$ and message $m_0 \in \mathcal{M}$ and let $c \leftarrow \mathsf{Enc}_{k_0}(m_0)$. Let us define a set D_c as follows

$$D_c := \{m \in \mathcal{M} \colon \exists k \in \mathcal{K} \text{ s.t. } m = \mathsf{Dec}_k(c)\}$$

Since the algorithm Dec is deterministic, we have that $|D_c| \leq |\mathcal{K}|$ and hence

$$|D_c| < |\mathcal{M}|.$$

This implies that there exists $m_1 \in \mathcal{M}$ such that $m_1 \notin D_c$. In other words, $\Pr[m_1 = \mathsf{Dec}_K(c)] = 0$, where the probability is taken over the choice of K. Consequently,

$$\Pr[c = \mathsf{Enc}_K(m_1)] = 0,$$

since otherwise the correctness of the encryption is scheme would not be satisfied. Since $c \leftarrow \Pr[c = \mathsf{Enc}_K(m_0)] > 0$, we have a contradiction with part (b) of this exercise. The probabilities above were taken over the choice of K and randomness of Enc.

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.

Solution:
Let us fix arbitrary $c \in \mathcal{C}$ and an arbitrary $m \in \mathcal{M}$. Then the following holds:

$$\begin{aligned}\Pr[\mathsf{Enc}_K(m) = c] &= \Pr[m + K = c \mod 26] \\ &= \Pr[K = c - m \mod 26] = \frac{1}{26}\end{aligned}$$

Since the above statement holds for all m, we have that for every $c \in \mathcal{C}$ and every $m_0, m_1 \in \mathcal{M}$

$$\Pr[\mathsf{Enc}_K(m_0) = c] = \frac{1}{26} = \Pr[\mathsf{Enc}_K(m_1) = c]$$

which by Lemma 1 from the lecture concludes the proof.

(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.

Solution:
Let Π' be a encryption scheme with ciphertext space $\mathcal{C} = \mathbb{Z}_{26}^n$ and key space is $\mathcal{K} = \mathbb{Z}_{26}^n$. Let $\Pr[K = k] = \frac{1}{26^n}$ for every $k \in \mathcal{K}$. The encryption of a message $m = (m_1, \ldots, m_n) \in \mathbb{Z}_{26}^n$ using the key $k = (k_1, \ldots, k_n) \in \mathbb{Z}_{26}^n$ works as follows:

$$\mathsf{Enc}_k(m) = (k_1 + m_1 \mod 26, \ldots, k_n + m_n \mod 26).$$

The decryption of a ciphertext $c = (c_1, \ldots, c_n) \in \mathbb{Z}_{26}^n$ using the key $k = (k_1, \ldots, k_n) \in \mathbb{Z}_{26}^n$ works as follows:

$$\mathsf{Dec}_k(c) = (c_1 - k_1 \mod 26, \ldots, c_n - k_n \mod 26).$$

Intuitively, each character $m_i \in \mathbb{Z}_{26}$ is encrypted using a key $k_i \in \mathbb{Z}_{26}$ chosen uniformly at random.

Correctness: Let us fix an arbitrary key $k \in \mathbb{Z}_{26}^n$ and an arbitrary message $m \in \mathbb{Z}_{26}^n$. Then we have

$$\begin{aligned}\mathsf{Dec}_k(\mathsf{Enc}_k(m)) &= \mathsf{Dec}_k((k_1 + m_1 \mod 26, \ldots, k_n + m_n \mod 26)) \\ &= (k_1 + m_1 - k_1 \mod 26, \ldots, k_n + m_n - k_n \mod 26) \\ &= (m_1, \ldots, m_n),\end{aligned}$$

which completes the proof of correctness.

Perfect security: Analogous as for part (a) of this exercise.

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?

Solution:

First of all, from Exercise 3(c) we know that for a cipher to have perfect secrecy it is required that $|\mathcal{K}| \geq |\mathcal{M}|$.
Let $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^l$ be respectively the set of keys, messages and ciphertexts. By applying the proposed improvement, i.e., by removing 0^l from the keyspace, we get

$$|\mathcal{K}| = |\mathcal{M}| - 1 < |\mathcal{M}|$$

breaking the definition of perfect secrecy. Therefore the resulting cipher is not 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.

Solution:

The used encryption scheme is the "Mono-alphabetic substitution cipher" and the used key is:

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
Ciphertext	m	f	a	n	x	i	w	p	b	s	h	g	l

Plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	t	c	q	k	v	r	j	u	d	y	z	e	o

This is the first ciphertext of the The Cipher Challenge included in the book "The Code Book" by Simon Singh. The challenge consisted of ten separate messages encrypted using a series of different encryption schemes and promised £10,000 to the first person to break all ten ciphertexts. It took one year and one month before all ten ciphertexts were decrypted.

If you are interested in the rest of The Cipher Challenge, visit `www.simonsingh.net/cryptography/cipher-challenge/`.