Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
Summer 2017

Cryptography

Exercise Sheet 1

Exercise 1-1 A substitution cypher is a slight generalisation of the shift cypher from the lectures. The key is a permutation π on the set of letters $\{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$. A message is encoded by applying the permutation to each letter individually; decoding works by applying the inverse of the permutation. For example, if the permutation π maps `a` to `b`, `b` to `a` and all characters to themselves, then the message `abcda` encodes to `bacdb`.

Decrypt the following cyphertext (from the Katz-Lindell-book), which comes from the encryption of English text.

```
jgrmqoyghmvbjwrwqfpwhgffdqgfpfzrkbeebjizqqocibzklfafgqvfzfwwe
ogwopfgfhwolphlrlolfdmfgqwblwbwqolkfwbylblylfsfljgrmqbolwjvfp
fwqvhqwffpqoqvfpqocfpogfwfjigfqvhlhlroqvfgwjvfpfolfhgqvqvfile
ogqilhqfqgiqvvosfafgbwqvhqwijvwjvfpfwhgfiwihzzrqgbabhzqocgfhx
```

Hint: The average frequencies of letters in English are as follows (in percent): `a`: 8.2, `b`: 1.5, `c`: 2.8, `d`: 4.2, `e`: 12.7, `f`: 2.2, `g`: 2, `h`: 6.1, `i`: 7, `j`: 0.1, `k`: 0.8, `l`: 4, `m`: 2.4, `n`: 6.7, `o`: 7.5, `p`: 1.9, `q`: 0.1, `r`: 6, `s`: 6.3, `t`: 9, `u`: 2.8, `v`: 1, `w`: 2.4, `x`: 2, `y`: 0.1, `z`: 0.2.

Exercise 1-2 Decrypt the text file `vigenere.txt` from the course homepage, which contains English text encoded using the Vigenère cypher from the lecture.

Exercise 1-3 Consider an encryption scheme with message space $M = \{a, b, c\}$, key space $K = \{k_1, k_2, k_3\}$ and cyphertext space $C = \{0, 1, 2\}$.

Assume the probabilities of the messages are $P(M = a) = 0.5$ and $P(M = b) = 0.25$. The key generation function produces keys with probabilities $P(K = k_1) = P(K = k_2) = 0.3$. As usual, the random variables M and K are assumed to be independent.

The encryption function itself is specified by the table below.

	a	b	c
k_1	0	2	1
k_2	2	1	0
k_3	1	0	2

a) Compute the probability distribution of the random variable C, i.e. the probabilities $P(C = i)$.

b) Compute the conditional probabilities $P(M = m \mid C = c)$ for all m and c.

1-3 a) $P(C=0) = P(K=k_1 \wedge M=a) + P(K=k_3 \wedge M=b) + P(K=k_2 \wedge M=c)$

K, M indep. $\nearrow = P(K=k_1)P(M=a) + P(K=k_3)P(M=b) + P(K=k_2)P(M=c)$

$= .3 \cdot .5 + .4 \cdot .25 + .3 \cdot .25$

$= .325$

$P(C=1) = P(k_3)P(a) + P(k_2)P(b) + P(k_1)P(c)$

$= .4 \cdot .5 + .3 \cdot .25 + .3 \cdot .25$

$= .35$

$P(C=2) = P(\neg(C=0 \vee C=1)) = 1 - P(C=0 \vee C=1)$

$= 1 - P(C=0) - P(C=1) = .325$

1-3b) Kolmogorov: $P(A \mid B) = P(A \wedge B) / P(B)$

$P(M=m \mid C=c) = P(m \wedge c)/P(c) = P(K=k \text{ s.t. } M=m \Rightarrow C=c)\, P(M=m) / P(c)$

c \ m	a	b	c
0	.461	.307	.230
1	.571	.214	.214
2	.461	.230	.307

Note that $\neg \exists q \in R\ \forall m, c\ P(M=m \mid C=c) = q$,
because $\neg \exists q' \in R\ \forall k\ P(K=k) = q'$

1-4 Given a set of n Permutations $\pi_n : \{0, \dots, n-1\} \to \{0, \dots, n-1\}$
of $\{0, \dots, n-1\}$ s.t. $\forall i, j \in \{0, \dots, n-1\}\ \forall m \in \{0, \dots, n-1\} : \pi_i(m) = \pi_j(m) \Rightarrow i = j$ $(*)$
(i.e. a latin square of order n):
Define a random variable $K \in \{0, \dots, n-1\}$ s.t. $\forall k \in \{0, \dots, n-1\} : P(K=k) = \frac{1}{n}$, the key.
Given a random variable $M \in \{0, \dots, n-1\}$ with some probability distribution:
Take C, the cipertext, to be $C = \pi_K(M)$.

For perfect security it suffices to show, that:
- Given K and C there exists a method to reconstruct M:
  By $(*)$
- $\forall m, c \in \{0, \dots, n-1\} : P(M=m \mid C=c) = P(M=m)$

$P(C=c) = \sum_i P(K=i)\, P(M = \pi_i^{-1}(c)) = \frac{1}{n} \cdot \underbrace{\sum_i P(M = \pi_i^{-1}(c))}_{\text{by } (*) \text{ and pidgeon hole } = \sum_i P(M=i)} = \frac{1}{n}$

$\forall m, c : P(K=k \text{ s.t. } M=m \Rightarrow C=c) \overset{(*)}{=} P(K=k \text{ s.t. } \pi_K(m) = c) = \frac{1}{n}$

$P(M=m \mid C=c) \overset{1\text{-}3b}{=} P(K=k \text{ s.t. } M=m \Rightarrow C=c)\, P(M=m) / P(C=c) = \frac{1}{n} \cdot P(M=m) / \frac{1}{n} = P(M=m)$ $\square$

Exercise 1-4 A Latin square of size n is a square filled with numbers from $\{0, \dots, n-1\}$, such that each number appears exactly once in each row and in each column. An example of size 3 has already appeared in the previous exercise:

$$\begin{matrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{matrix}$$

Show how each Latin square can be used to define a perfectly secret encryption scheme. Give a full proof of perfect secrecy of this scheme for arbitrary n.