Problem 1.

a.



**Theorem 1.a** *The shift cipher for messages of length 1 over  satisfies the definition of perfect secrecy.*

**Proof** Fix some distribution over *M* and fix an arbitrary  and . The key observation is that for the shift-cipher,

  

Since this holds for all distributions and all *m*, we have that for every probability distribution of *M*, everyand every:



This implies perfect indistinguishability (Lemma 2.3 of Katz, Lindell), we conclude that the encryption scheme is perfectly secret.

b.

**Theorem 1.b** *The largest message space M* *for which the mono-alphabetic shift-cipher provides perfect secrecy is 26! (Assuming the use of the English alphabet). Let (Gen, Enc, Dec) be an encryption scheme over a message space* M *for which* |M| = |K| = |C|. *The scheme is perfectly secret if and only if:*

1. *Every key*  *is chosen with equal probability*  *by algorithm Gen.*
2. *For every  and every , there exists a unique key such that  outputs c.*

**Proof** Since the maximum possible length of the key , and the message , can be no longer than 26, the total key space is of size

26! (******). A brute force attack would be infeasible even using the most powerful computer known today. Since |M| = |K| = |C| we can use Theorem 1.b (Shannon’s Theorem)

For every and  there exists at most one key **such that **= *c* .



We conclude that keys are chosen according to the uniform distribution.

To prove the other direction of the theorem, for every probability distribution over M:



We conclude with the satisfaction of indistinguishable secrecy, which implies perfect secrecy in Katz, Lindell lemma 2.3.

**Appendix B**

***Definition 2.1*** *An encryption scheme over a message space M is perfectly secret if for every probability distribution over M, every message , and every ciphertext for which* :



***Lemma 2.2*** *An encryption scheme* *over a message space M is perfectly secret if and only if for every probability distribution over M, and every message* , *and every ciphertext :*



**Proof** Fix a distribution over *M* and arbitrary **and *.*

Suppose that:

.

Multiplying both sides of the equation by  gives:



***Lemma 2.3*** *An encryption scheme*  *over a message space M is perfectly secret if and only if for every probability distribution over M, every , and every *

**

**Proof**

Assume that the encryption scheme is perfectly secret and fix messages  and a ciphertext *.* By Lemma 2.2 we have

 ,

Completing the proof of the first direction.

Assume next that for every distribution over *M,* it holds that: .

Define *p*: 



****

Since  was arbitrary, we have shown that  for all. Applying Lemma 2.2, we conclude that the encryption scheme is perfectly secret.

**Definition 2.4** *An encryption scheme*  *over a message space M is perfectly secret if for every adversary* A *it holds that:*

* .*

*The eavesdropping Indistinguishability experiment:*

1. *The adversary* A *outputs a pair of messages .*
2. *A random key k is generated by running* (Gen)*, and a random bit  is chosen. (These are chosen by some imaginary entity that is running the experiment with* A*.) Then, a ciphertext  is computed and given to* A*.*
3. A *outputs a bit .*
4. *The output of the experiment is defined to be* 1 *if *= *b, and* 0 *otherwise. We write if the output is* 1 *and in this case we say that* A **succeeded.**

**References**

[1] J. Katz, Y. Lindell. *Introduction to modern cryptography: principles and protocols.* Chapman & Hall / CRC, 1st edition, 2008.