Week 3: Cryptography and Modular Arithmetics

Hans Georg Schaathun

12th November 2015

Period 2–8 September 2015

Reading Stein *et al* cover this material in Chapter 2.

Programme This document details the programme for the week, including exercises and pointers to other material. It is available in two versions:

1. as a PDF document.
2. as a web site. This depends on MathML and may require firefox/iceweasel to display correctly.

The web version includes inline video. The pdf version shows a still image from the video, providing a hyperlink directly to the video on the web site.

Warning! Stein *et al* are misleading on page 93 when they say that

> *In general, any scheme that uses a codebook — a secretly agreed-upon (possibly complicated) code — suffers from these drawbacks.*

Firstly, the drawbacks described need not be detrimental. Symmetric ciphers (which seems to be effectively what they mean by a codebook) are still in use with several sound and trust-worthy industry standards available. Secondly, public-key cryptosystems, which is the alternative to symmetric/codebook-based ciphers, share the very same drawbacks.

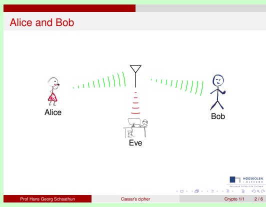
Extra videos The videos in this document have been made rather concise, because I believe that the material is better learnt by discussing problems in class, and supplementing with extra exercises in your own time. If you disagree, and think that longer and more elaborate lectures would help you, please consult the «Extra material» tab on the web pages.

1 Wedneday 2 September

Related reading: Stein *et al* p. 89–93 or Rosen p. 291–294

THEORY

Ciphers are used to communicate secret messages. We take the classic cipher of Iulius Cæsar as an introductory example.



OGG

MP4

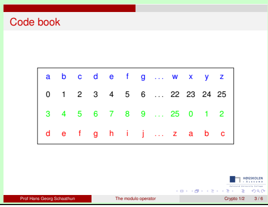
Slides

Problem 1.1 (Cæsar's cipher) *Consider the original Cæsar's cipher ($k = 3$).*

1. *Encrypt the plaintext:* `I did this`
2. *Decrypt the ciphertext:* `Juhdw zrun`

THEORY

Cryptography is a mathematical discipline. Without mathematics, cryptography is *ad hoc*, inflexible, and impossible to generalise. Mathematics enables generalisation, which in turn allows reusable and secure solutions.



OGG

MP4

Slides

Problem 1.2 (Cæsar's cipher via numbers) *Consider the plaintext* `peculiar` *to be encrypted using Cæsar's cipher. Show how you encrypt the message step by step, mapping to integers, using modular arithmetrics, and then mapping back to the alphabet.*

THEORY

Auguste Kerckhoffs (1883) introduced the then controversial principle of requiring a *secret key* to secure a cipher, which should not otherwise require secrecy. This principle has become the cornerstone of modern cryptography.

OGG

MP4

Slides

Problem 1.3 *The generalised Cæsar's cipher with a key $k = 13$ is known as rot13 and a classic in Internet communication (Usenet in particular). Using rot13:*

1. *Encrypt the plaintext:* `Interesting`
2. *Decrypt the ciphertext:* `Interesting`
3. *Comment on the result.*

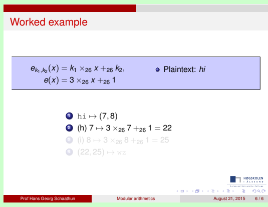
THEORY

Using a set of arithmetic operations on the integers modulo n, we get a set of building blocks for new ciphers, such as the affine cipher

Definition 1 *The affine cipher is defined by the encryption function*

$$e_{k_1,k_2}(x) = k_1 \times_{26} x +_{26} k_2$$

for a key (k_1, k_2).



OGG MP4 Slides

Problem 1.4 *Encrypt the message* `new idea`*, using the affine cipher with each of the following keys:*

1. $(3, 1)$
2. $(5, -5)$

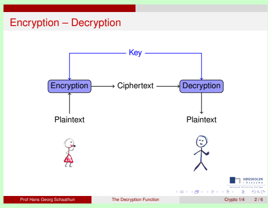
Problem 1.5 *Calculate the following expressions*

- $2 + 3 \mod 4$
- $7 \cdot 3 \mod 6$
- $6 \cdot 7 - 1 \mod 10$

Problem 1.6 *Encrypt the message* `an idea`*, using the encryption function* $e_{k_1,k_2}(x) = k_1 \times_{26} x +_{26} k_2$*, using the key* $(k_1, k_2) = (2, 2)$*. Comment on the result.*

THEORY

The decryption function $d_k(y) = e_k^{-1}(x)$ is the inverse of the encryption function e_k. Let's formalise the concept.



OGG

MP4

Slides

Problem 1.7 *Given the encryption function* $e_k(x) = x + k \mod 26$*; what is the decryption function* $e_k^{-1} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$*?*

2 Thursday 3 September

Today, we continue the study of cryptography. We will use fundamental theory from Week 1–2 to understand some key features of cryptography. If you get puzzled by questions about relations or counting, then please review Week 1–2 material as required.

Related reading: Stein *et al* p. 95–109. In Rosen, relevant material is scattered; see pp. 241, 243+, 273–275, 293, and 808+.

Problem 2.1 *A cipher establishes a relation R between the plaintext x and the ciphertext y. We write xRy if $y = e(x)$ is the result of encrypting x. Consider what happens if this relation is*

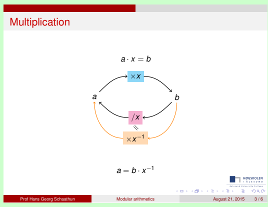
1. *one-to-one*
2. *one-to-many*
3. *many-to-one*
4. *many-to-many*

Describe the practical consequence of each type of relation. Which of the four alternatives are at all possible for a usable cipher?

THEORY

Can we have division in $\mathbb{Z}_n$?

Is x/y defined for $x, y \in \mathbb{Z}_n$?



OGG

MP4

Slides

Problem 2.2 *Consider the ring $\mathbb{Z}_{12}$. Write down a complete multiplication table, i.e. a 12×12 where cell (i, j) gives the product $i \cdot j$ for $i, j = 0, 1, \ldots, 11$. Using this table, answer the following questions:*

1. *Describe the patterns of repetition in the table.*
2. *Which are the zero divisors in $\mathbb{Z}_{12}$?*
3. *What is the inverse 5^{-1}? In other words, which number x solves the equation $5x \mod 12 = 1$?*
4. *Are there any number other than 5 for which you can find an inverse?*

THEORY

The size of the key space (set of possible keys) is critical for cryptographic security. If there are few possible keys, the enemy can guess it, or perform an exhaustive search. We talk about weak cryptography if the key space is small. Strong cryptography has large keyspaces.

OGG

MP4

Slides

Problem 2.3 *In Exercise 1.6 we saw that the affine cipher with key $(2, 2)$ did not give one-to-one encryption.*

1. *Which other keys do we have to avoid? (And why?)*
2. *Avoiding such keys, what is the size of the keyspace?*

Problem 2.4 *Consider the general monoalphabetic cipher, where every permutation (bijection) on $\mathbb{Z}_{26}$ is a key. What is the size of the key space?*

Problem 2.5 *The modulo operator establishes a relation on $\mathbb{Z}_n$, where x and y are related if*

$$x \mod n = y \mod n.$$

This relation is written

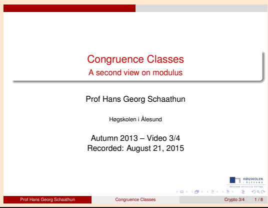
$$xn \equiv y \pmod{n},$$

and we read «x is congruent to y modulo n». Show that this congruence relation is an equivalence relation.

Supporting theory

The exercise above explored the equivalence relation known as congruence modulo n.

Related reading: Rosen p. 241



OGG

MP4

Slides

Problem 2.6 *The encryption function for Cæsar's cipher is $e_k(x) = x + k \mod 26$. In Exercise , we found the decryption function $d_k(x) = e_k^{-1}(x)$ for Cæsar's cipher with arbitrary k.*

It is possible to use the same function and implementation for d_k and e_k. For any k, we can find a value k' such that $d_k(x) = x + k' \mod 26 = e_{k'}(x)$. Find this k'

- *when $k = 5$*
- *when $k = 13$*
- *for (general) k*

3 Compulsory Assignment (Tuesday 8 September)

Problem 3.1 *Consider the affine cipher on $\mathbb{Z}_{26}$,*

$$e_{k_1,k_2}(x) = k_1 \cdot x + k_2,$$

with key $(k_1, k_2) = (7, 2)$. Encrypt the message

> *For he's a jolly good fellow, for he's a jolly good fellow.*

Problem 3.2 *Consider a polyalphabetic Cæsar (additive) cipher with key $k = (13, 2, 7)$. Encrypt the message*

> *For he's a jolly good fellow, for he's a jolly good fellow.*

Problem 3.3 *Compare the ciphertexts in Exercises 3.2 and 3.1. What do you see? Is the affine cipher monoalphabetic, polyalphabetic, or neither? Why?*

Problem 3.4 *Consider the ring* $\mathbb{Z}_{11}$. *Write down a complete multiplication table, i.e. a* 11×11 *where cell* (i, j) *gives the product* $i \cdot j$ *for* $i, j = 0, 1, \ldots, 10$. *For each number* $a = 0, 1, \ldots, 10$ *identify the inverse* a^{-1} *such that* $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Problem 3.5 *Consider a polyalphabetic Cæsar (additive) cipher with a block length of* $m = 3$. *What is the keyspace* $\mathcal{K}$*? What is the size* $\#\mathcal{K}$*? Give reasons for your answers.*

Problem 3.6 *Consider the affine cipher applied to the 29-letter Scandinavian alphabet:*

$$e_{k_1,k_2}(x) = k_1 \cdot x + k_2 \mod 29.$$

Which (if any) are the zero divisors of Z_{29}*? What is the size of the keyspace for the affine cipher modulo 29?*