Exercises Week 11
Advanced Encryption Standard

Hans Georg Schaathun

4th January 2016

Period 28 October – 3 November 2015

Reading Stein *et al.* do not cover this material. You should read the AES Standard from NIST, and you can read more about finite fields in Rosen.

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.

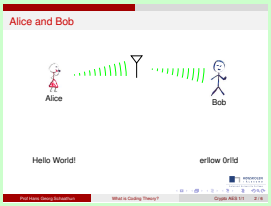
1 Wednesday 28 October 2015

Please watch the videos *once* before class. It may be helpful to peek at the exercises between the videos. You should not worry if you do not understand them after the first run. We will discuss the exercises in class, and if that does help you start to understand, then you are allowed to worry.

1.1 Matrix calculations over finite sets

THEORY

Coding theory studies how to encode information to make it robust against noise. This is essential to any communication system.



OGG

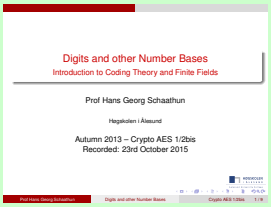
MP4

Slides

Related reading: Rosen p. 817–819

THEORY

Decimal numbers are written with base 10, binary numbers with base 2. It is also common to write numbers with base 8 (octal) or base 16 (hexadecimal).



OGG

MP4

Slides

Related reading: Rosen p. 245–249

Exercise 1.1 *Write the following numbers in Hexadecimal:*

1. *1024*
2. *129*
3. *721*

Exercise 1.2 *Write the following numbers in Octal:*

1. *1024*
2. *129*

Exercise 1.3 *Write the following hexadecimal numbers in decimal:*

1. *FF*
2. *17A*
3. *111*

Exercise 1.4 *Rewrite hexadecimal A9 in binary.*

Exercise 1.5 *Write 0155 (octal) in decimal.*

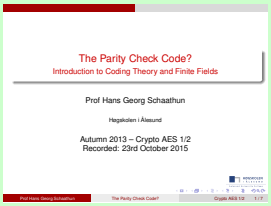
THEORY

Definition 1 *The parity check code encodes a seven-bit (ASCII) character by taking the binary representation and multiply by the following matrix*

$$G = \begin{bmatrix} 1100000 \\ 1010000 \\ 1001000 \\ 1000100 \\ 1000010 \\ 1000001 \end{bmatrix}.$$

The matrix G is called the generator matrix.

Related reading: Rosen p. 287–289



OGG

MP4

Slides

Exercise 1.6 *Take the word 'Try', find the ASCII number for each letter, write it in binary form, and encode it using the parity check code.*

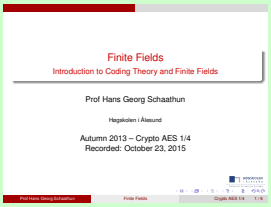
1.2 Theory of finite fields

THEORY

A set F, with operations $+$ and $\cdot$ is called a *field* if the following axioms hold

1. $(F, +)$ is an Abelian group:
   - associtativity of addition
   - commutativity of addition
   - Neutral element (0)
   - Inverse $(-x)$
2. $(F \backslash \{0\}, \cdot)$ is an Abelian group:
   - associtativity of multiplication
   - commutativity of multiplication
   - Neutral element (1)
   - *Inverse (x^{-1}) for every (non-zero) element x*
3. $x \cdot (y + z) = x \cdot y + x \cdot z$ (distributive law)

Related reading: Rosen p. 808–811



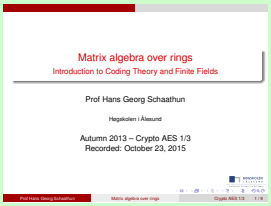
OGG

MP4

Slides

THEORY

Matrix addition and multiplication is defined over finite fields just as they are over other fields, such as the real numbers.



OGG

MP4

Slides

Related reading: Rosen Chapter 2

Exercise 1.7 *Calculate the following over* $\mathbb{Z}_2$*:*

$$[101] + [110] = \tag{1}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} = \tag{2}$$

Exercise 1.8 *Calculate the following over* $\mathbb{Z}_2$*:*

$$[101] \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \tag{3}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \tag{4}$$

Exercise 1.9 *Calculate the following over* $\mathbb{Z}_3$*:*

1. $[121] + [210] =$
2. $$[201] \cdot \begin{bmatrix} 1 & 1 \\ 2 & 0 \\ 0 & 1 \end{bmatrix} = \tag{5}$$
3. $[121] \cdot [210] =$
4. $$\begin{bmatrix} 1 & 2 & 0 \\ 0 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 2 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \tag{6}$$

2 Thursday 29 October 2014

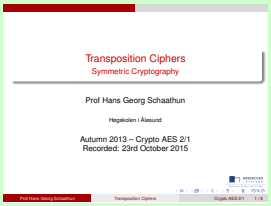
2.1 Transposition ciphers

THEORY

Tihs esnetnec ie snrcytpew diht a rtas-npsoiitoc nihpe.r

By the way, the key is $k = (1, 3, 2)$. Learn to decipher in the video.

Related reading: Rosen p. 294



OGG

MP4

Slides

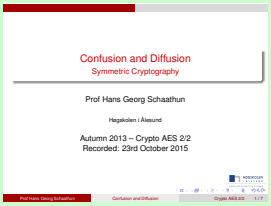
Exercise 2.1 *Decipher the message given above (in the green theory box).*

Exercise 2.2 *Write down the decryption key for the following transposition encryption key* $k = (3, 1, 2)$.

2.2 Advanced Encryption Standard (AES)

THEORY

Modern ciphers combine two principles: *diffusion* and *confusion*. Cæsar's cipher and many other classic ciphers only perform *substitution* of letters or blocks of letters. This gives confusion, but no diffusion. A *transposition* cipher on the other hand, does diffusion and no substitution. Neither one suffices on its own.



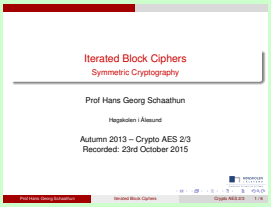
OGG

MP4

Slides

THEORY

Iterative Ciphers use the following procedure iterates the same *round function* with different round keys. The round function combines substitution and transposition, and iteration makes the two closely entangled.



OGG

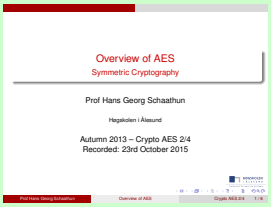
MP4

Slides

THEORY

AES is a symmetric cipher, standardised by NIST. It is an iterative cipher where the round function combines

1. Shift Rows (`ShiftRows`) — transposition
2. Substitute Bytes (`SubBytes`) — non-linear substitution
3. Mix Columns (`MixCol`) — linear substitution
4. Add the key (mod 2) (`AddRoundKey`) — keyed transform



OGG

MP4

Slides

Remark 1 *We do not yet have all the mathematical foundations required by AES. This week we work with matrix algebra over the field $\mathbb{Z}_p$ for p prime. In AES we need matrix algebra over a field with 256 elements, but $\mathbb{Z}_{256}$ is not a field. We will learn next week how to construct a field with 256 elements.*

2.3 More on matrices and numbers

Remember 1 *Remember that the inverse A^{-1} of a matrix A is the unique matrix with the property that $A^{-1} = I$, where I is the identity matrix.*

The identity matrix has all zeros except on the main diagonal which is all one.

EXERCISE EXAMPLE

Problem 2.1 *Consider the matrix A over $\mathbb{Z}_3$:*

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & 1 \end{bmatrix} \tag{7}$$

OGG

MP4

Slides

Find A^{-1}.

Exercise 2.3 *Find the inverse matrices over $\mathbb{Z}_2$ for*

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \tag{8}$$

You can use Gaussian ellimination in the same way as you would over the reals.

Exercise 2.4 *Find the inverse matrices over $\mathbb{Z}_2$ for*

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \tag{9}$$

You can use Gaussian ellimination in the same way as you would over the reals.

Exercise 2.5 *Write recursive algorithms to take a number N and*

1. *... write it as a string in binary representation.*
2. *... write it as a string using Base b.*

3 Extra problems with solution

Exercise 3.1 *Calculate the following over* $\mathbb{Z}_2$*:*

$$[101] \cdot [111] = \tag{10}$$

$$[101] \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \tag{11}$$

Exercise 3.2 *Write down the decryption keys for the following transposition encryption keys:*

1. $(4, 5, 1, 3, 2)$
2. $(7, 4, 6, 1, 5, 3, 2)$

4 Compulsory Problems (Tuesday 3 November)

Exercise 4.1 *Write 841 in Hexadecimal.*

Exercise 4.2 *Write 917 in Octal.*

Exercise 4.3 *Write AC (hexadecimal) in decimal.*

Exercise 4.4 *Write 0321 (octal) in decimal.*

Exercise 4.5 *Calculate the following over* $\mathbb{Z}_2$*:*

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \tag{12}$$

Exercise 4.6 *Using the key* $(4, 5, 1, 3, 2)$*, encrypt the message* 'transposition ciphers use permutations'*.*

Exercise 4.7 *Find the inverse matrices over* $\mathbb{Z}_5$ *for*

$$\begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix} \tag{13}$$

You can use Gaussian ellimination in the same way as you would over the reals.