Week 5: The RSA Cipher

Hans Georg Schaathun

12th November 2015

Period 16–22 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.

1 Wedneday 16 September

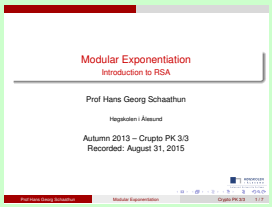
Today, we will explore the RSA cryptosystem. My advice is that you watch the three theory videos once only, and prioritise understanding the worked examples.

Related reading: Stein *et al.* 123–128 or Rosen p. 253–254 and 295–298

THEORY

Whenever we have multiplication, we can have exponentiation; at least with non-negative integer exponents. The following definition applies to any ring; the same definition holds whether we have $\alpha \in \mathbb{R}$ or $\alpha \in \mathbb{Z}_n$.

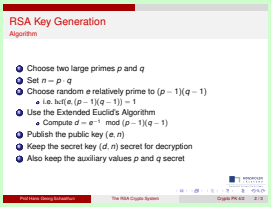
Definition 1 *When i is non-negative integer, we define the ith power α^i of any element α as the product $\alpha \cdot \alpha \cdot \ldots \cdot \alpha$ where α occurs i times as a factor.*



OGG MP4 Slides

THEORY

RSA is the most well-known public key cipher. This video gives the basic definitions.



OGG

MP4

Slides

Exercise 1.1 *Calculate*

1. $5^8 \mod 12$
2. $11^7 \mod 17$
3. $2^{12} \mod 21$

How many multiplications do you need for each calculation?

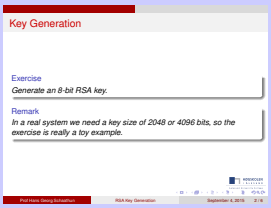
Exercise 1.2 *Consider the encryption function* $e_k(x) = x^k$ *in* $\mathbb{Z}_{29}$.

1. *What is the corresponding decryption function (key)?*
2. *Why did we not consider* $\mathbb{Z}_{26}$ *which corresponds so neatly to the English alphabet?*

WORKED EXAMPLE

Problem 1.1 *Generate an 8-bit RSA key.*

Remark 1 *In a real system we need a key size of 2048 or 4096 bits, so the exercise is really a toy example.*



OGG

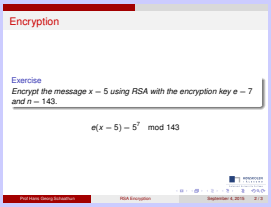
MP4

Slides

Exercise 1.3 *Generate an RSA key, using* $n = 7 \cdot 13$ *as the modulus.*

WORKED EXAMPLE

Problem 1.2 *Encrypt the message* $x = 5$ *using RSA with the encryption key* $e = 7$ *and* $n = 143$.



OGG

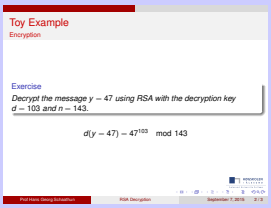
MP4

Slides

Exercise 1.4 *Encrypt the plaintext* $x = 4$ *with RSA using the encryption key* $(5, 91)$.

WORKED EXAMPLE

Problem 1.3 *Decrypt the message* $x = 47$ *using RSA with the encryption key* $e = 103$ *and* $n = 143$.



OGG

MP4

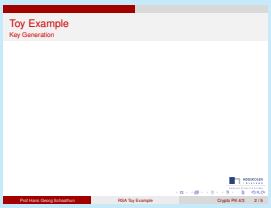
Slides

Exercise 1.5 *Decrypt the ciphertext $x = 10$ with RSA using the decryption key $(7, 91)$.*

Exercise 1.6 *Tabulate the values 2^i for $i = 0, 1, 2, \ldots$ for each of the rings $\mathbb{Z}_{13}$ and $\mathbb{Z}_{15}$. How many distinct elements do you get in each ring before the values start repeating? What can you say about these numbers?*

EXERCISE EXAMPLE

If you want another worked example, you can try this one; recorded in 2013.



OGG

MP4

Slides

2 Thursday 17 September

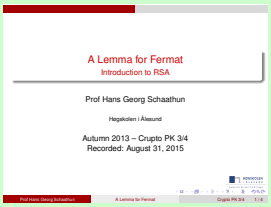
2.1 Some theory

Exercise 1.6 illustrates Fermat's little theorem (not to be confused with Fermat's last theorem). This celebrated result is important for the proof of RSA, so we will give two videos to state and prove it.

Related reading: Stein *et al.* p. 125–127 or Rosen p. 279 and 282 (Ex. 13)

THEORY

Lemma 1 *For any prime number p and any non-zero $a \in \mathbb{Z}_p$, the operation $x \mapsto a \cdot x$ is a permutation (bijection) on $\mathbb{Z}_p$.*



OGG

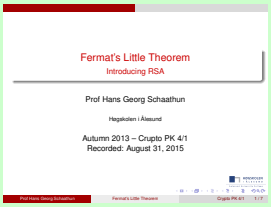
MP4

Slides

THEORY

Lemma 2 *For every prime p and any positive integer x which is not a multiple of p, we have*

$$x^{p-1} \equiv 1 \pmod{p}$$



OGG

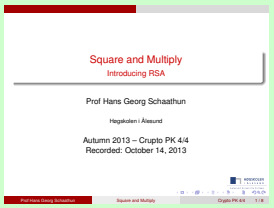
MP4

Slides

2.2 Fast Exponentiation

THEORY

```
1        Algorithm SquareNmultiply(x, e, n)
2        if e = 1, return x
3        y := SquareNmultiply(x, ⌊e/n⌋, n)
4        y' := y^2 mod n
5        if e mod 2 = 1,
6            y'' := y' · x mod n
7        else
8            y'' := y'
9        return \Tg<mrow>y''
```



OGG MP4 Slides

Related reading: Stein *et al.* 136–138 or Rosen p. 253–254

Exercise 2.1 *Calculate the following*

1. $3^{32} \mod 100$
2. $5^{42} \mod 50$
3. $6^{29} \mod 100$

Exercise 2.2 *Calculate*

1. $7^{11} \mod 11$
2. $10^{12} \mod 13$

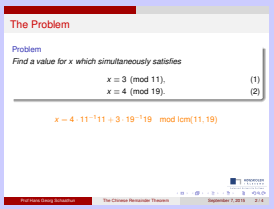
How many multiplications do you need for each calculation?

2.3 Chinese Remainder Theorem

WORKED EXAMPLE

Problem 2.1 *Find a value for x which simultaneously satisfies*

$$x \equiv 3 \pmod{11}, \quad (1)$$
$$x \equiv 4 \pmod{19}. \quad (2)$$



OGG MP4 Slides

Related reading: Rosen p. 275–277

Exercise 2.3 *Solve the following sets of equations:*

1. $x \equiv 2 \pmod 7$ *and* $x \equiv 4 \pmod 9$
2. $x \equiv 3 \pmod{12}$ *and* $x \equiv 10 \pmod{25}$

3. $x \equiv 10 \pmod{11}$ *and* $x \equiv 0 \pmod{5}$

Exercise 2.4 *Solve the following set of equations:*

$$\begin{aligned} 2x &\equiv 5 \pmod{7} \\ 3x &\equiv 1 \pmod{8} \end{aligned}$$

Exercise 2.5 *Solve the following set of equations:*

$$\begin{aligned} 2x - 5 &\equiv 0 \pmod{9} \\ 3x + 1 &\equiv 2 \pmod{5} \end{aligned}$$

Exercise 2.6 (Special Challenge) *It is possible to generalise the Chinese Remainder Theorem to solve a system of three or more equations:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

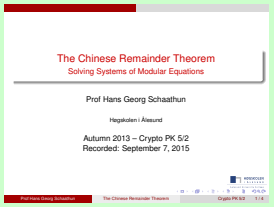
1. *We introduced the inverse n' of n modulo m. When there are more than two equations, we need an inverse m'_i which satisfies $m'_i m_i \equiv 1 \pmod{m_j}$ for each $j \neq i$. Define $M_i = \prod_{j \neq i} m_j$ and use M_i as a modulus. How do you define m'_i to satisfy the requirement?*
2. *Using m'_i as you defined it above. What is the solution to the set of congruences?*
3. *Prove that hypothesised solution is correct.*

THEORY

Theorem 1 (The Chinese Remainder Theorem) *If m and n are relatively prime integers, and $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$, then the set of equations*

$$x \mod m = a, \tag{3}$$
$$x \mod n = b \tag{4}$$

has exactly one solution for an an integer $x \in \mathbb{Z}_{mn}$.



OGG MP4 Slides

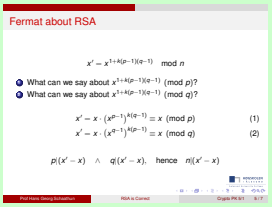
Related reading: Rosen p. 275–277

3 Last Lectures of the Week

THEORY

Before we want use a crypto system, we require an irrefutable proof that the decryption function correctly returns the original plain text.

Related reading: Stein *et al.* p. 129–131



OGG

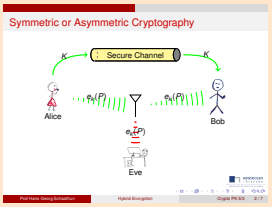
MP4

Slides

SUPPORTING THEORY

In practice public key ciphers are used in conjunction with symmetric (secret key) ciphers. Let's see how.

Related reading: Rosen p. 299–300



OGG

MP4

Slides

4 Compulsory Assignment (Tuesday 22 September)

Exercise 4.1 *Calculate*

1. $6^3 \mod 9$
2. $6^3 \mod 11$

Exercise 4.2 *Calculate*

1. $6^{30} \mod 100$
2. $7^{42} \mod 50$

Exercise 4.3 *Calculate* $4^{25} \mod 13$. *Discuss what tricks you can use to simplify the problem.*

Exercise 4.4 *Consider the primes 7 and 17.*

1. *Which candidates exist for* e*?*
2. *Choose the smallest possible* e*, and calculate* $d = e^{-1}$.
3. *Encrypt the message* $x = 2$*, to get a ciphertext* c.
4. *Decrypt the ciphertext* c *from the previous question.*

Show your calculations. You will probably need a calculator on the fourth question, but nevertheless, please show how you can do the solution step by step.

Exercise 4.5 *Solve the following set of congruences:*

$$x \equiv 1 \pmod 9, \tag{5}$$
$$x \equiv 1 \pmod{11}. \tag{6}$$

Exercise 4.6 *Solve the following set of congruences:*

$$2x \equiv 5 \pmod{9}, \tag{7}$$

$$3x \equiv 8 \pmod{11}. \tag{8}$$