Cryptography, winter 2013/2014

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

6. Exercise sheet
Hand in solutions until Saturday, 07 December 2013, 23:59:59

Exercise 6.1 (An example of Pollard's ρ method). (7 points)

(i) Complete the table below, which represents a run of Pollard's ρ algorithm for $N = 100181$ and the initial value $x_0 = 399$, up to $i = 6$. $\boxed{3}$

i	x_i rem N	x_i rem 17	y_i rem N	y_i rem 17	$\gcd(x_i - y_i, N)$
0	399	8	399	8	100181
1	...	...	...	...	...

(ii) The smallest prime divisor of N is 17. Describe the idea of the algorithm by looking at x_i rem 17 and y_i rem 17 and in particular, why we stopped at $i = 6$. $\boxed{2}$

(iii) Complete the factorization of N using Pollard's ρ algorithm. $\boxed{2}$

Exercise 6.2 (Decryption with AES). (8 points)

(i) Given the output of the function SubBytes, how can you find the corresponding input? $\boxed{2}$

(ii) Verify that the product of the polynomial $d = \mathtt{0B}y^3 + \mathtt{0D}y^2 + \mathtt{09}y + \mathtt{0E}$ and the polynomial $c = \mathtt{03}y^3 + \mathtt{01}y^2 + \mathtt{01}y + \mathtt{02}$ is equal to $\mathtt{1}$ in the ring $\mathbb{F}_{256}[y]/\langle y^4 + 1\rangle$. $\boxed{2}$

(iii) Formulate the AES decryption algorithm. $\boxed{4}$

Exercise 6.3 (One round of AES). (12 points)

In this exercise we compute the first round of AES by hand. We start with an input matrix

$$\begin{pmatrix} 01 & 11 & 21 & 31 \\ 02 & 12 & 22 & 32 \\ 03 & 13 & 23 & 33 \\ 04 & 14 & 24 & 34 \end{pmatrix}$$

and a key

$$\begin{pmatrix} AA & BB & CC & DD \\ AA & BB & CC & DD \\ AA & BB & CC & DD \\ AA & BB & CC & DD \end{pmatrix}$$

where all entries are in hexadecimal representation.

$\boxed{2}$ (i) Compute `AddRoundKey` for the first two bytes.

$\boxed{4}$ (ii) Compute `SubByte` for the two bytes that result in (i).

$\boxed{2}$ (iii) After step (ii) the matrix looks like

$$\begin{pmatrix} * & * & 55 & CE \\ C2 & D3 & 28 & DF \\ D3 & C2 & DF & 28 \\ E4 & 79 & 9B & 1E \end{pmatrix}$$

Compute `ShiftRows` of this matrix.

$\boxed{4}$ (iv) Compute `MixColumns` for the last column of the matrix that results in (iii).