Security on the Internet, winter 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

4. Exercise sheet
Hand in solutions until
Monday, 24 November 2008, 11^{59}am (deadline!).

Any claim needs a proof or an argument.

Exercise 4.1 (Tool: Groups). (8 points)

In this exercise you will get comfortable with the concept of a group. Always remember: Don't PANIC. Which of the following sets, together with the given operation form a group? Check for each property (Proper, Associative, Neutral, Inverse, Commutative) if it is well-defined, and if so if it is fulfilled or not:

(i) $(\mathbb{Z}, -)$: The integers $\mathbb{Z}$ with subtraction. 1

(ii) $(\mathbb{N} \setminus \{0\}, \hat{})$: The positive integers $\mathbb{N} \setminus \{0\}$ with exponentiation. 1

(iii) $(\mathbb{B}, \vee)$: The set $\mathbb{B} := \{\top, \bot\}$ with operation $\vee$ (the logical OR), defined as: 1

$\vee$	$\top$	$\bot$
$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$

(iv) $(\mathbb{B}, \oplus)$: The set $\mathbb{B}$ with operation $\oplus$ (the logical XOR), defined as: 1

$\oplus$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$

(v) $(4\mathbb{Z} + 1, \cdot)$: The set $4\mathbb{Z} + 1 := \{z \in \mathbb{Z} \mid z = 1 \text{ in } \mathbb{Z}_4\}$ with multiplication. 1

(vi) $(\{\mathbb{Z}_7 \to \mathbb{Z}_7\}, \circ)$: The set $\{\mathbb{Z}_7 \to \mathbb{Z}_7\} := \{f : \mathbb{Z}_7 \to \mathbb{Z}_7\}$ with concatenation $\circ$ of functions. An example: If $g_1, g_2 : \mathbb{Z}_7 \to \mathbb{Z}_7$ are two functions then $(g_1 \circ g_2)(x) := g_1(g_2(x))$ for all $x \in \mathbb{Z}_7$. 1

(vii) The elliptic curve $E\colon y^2 = x^3 + x$ has four points over $\mathbb{F}_3$. Namely we have $E = \{(0,0), (-1,1), (-1,-1), \mathcal{O}\}$. We define an addition on E via the following table: 2

$+$	$\mathcal{O}$	$(0,0)$	$(-1,1)$	$(-1,-1)$
$\mathcal{O}$	$\mathcal{O}$	$(0,0)$	$(-1,1)$	$(-1,-1)$
$(0,0)$	$(0,0)$	$\mathcal{O}$	$(-1,-1)$	$(-1,1)$
$(-1,1)$	$(-1,1)$	$(-1,-1)$	$(0,0)$	$\mathcal{O}$
$(-1,-1)$	$(-1,-1)$	$(-1,1)$	$\mathcal{O}$	$(0,0)$

Exercise 4.2 (Diffie Hellman key exchange). (6 points)

Perform a toy example of a Diffie Hellman key exchange: Fix $p = 47$ and $g = 2 \in \mathbb{Z}_p^\times$.

(i) Show that the order of g is 23, i.e. $g^{23} = 1$ but $g^k \neq 1$ for $1 \leq k < 23$. 1
[If you are clever then you only need to calculate g^{23}.] 1

1 (ii) Choose $x \in \mathbb{Z}_{23}$ (take $x \notin \{0, 1\}$ to get something interesting) and calculate $h_A := g^x$.

1 (iii) Choose $y \in \mathbb{Z}_{23}$ (take $y \notin \{0, 1, x\}$ to get something interesting) and calculate $h_B := g^y$.

2 (iv) Now compute h_B^x and h_A^y and compare.

Exercise 4.3 (Beware of the group!). (6 points)

The Joker proposes to perform the Diffie-Hellman key exchange in the group $(\mathbb{Z}_p, +)$. Explain why this is insecure:

3 (i) Prove that the discrete logarithm problem is easy here.

3 (ii) Show that the above proposal makes the key exchange completely insecure.

Exercise 4.4 (Square and multiply – the fancy way). (5 points)

Use paper and pencil for this exercise. How many multiplications do you need to compute x^{382}?

1 (i) Find an algorithm that uses 14 multiplications.

2 (ii) Find an algorithm that uses 12 multiplications.

2 (iii) Can you find an algorithm that uses 11 multiplications?

Some side calculations: $382 = 101111110_2 = 112011_3 = 11332_4 = 3012_5 = 1434_6 = 1054_7 = 576_8$, $382 = 2 \cdot 191$, $190 = 2 \cdot 5 \cdot 19$, $189 = 7 \cdot 3^3$.

Exercise 4.5 (Birthday? Paradox.). (3 points)

3 Compute the probability that in a group of 23 randomly chosen people, (at least) two have the same birthday. Provide a meaningful formula to justify your computation. (You may assume, that birthdays are uniformly distributed among 366 days in a year.)