Cryptography I, winter 2005/06

JOACHIM VON ZUR GATHEN, MICHAEL NÜSKEN

5. Exercise sheet
Hand in before Monday, 2005/12/05, 14^{00} in b-it 1.22.

Exercise 5.1 (Chinese Remainder Theorem). (10 points)

(i) Consider $21 = 3 \cdot 7$ and, as we did in the course, produce a table indicating the relation betweeen $\mathbb{Z}_{21}$ and $\mathbb{Z}_7 \times \mathbb{Z}_3$. $\boxed{1}$

(ii) Pick two elements $x, y \in \mathbb{Z}_{21}$ (to make it interesting: the sum of the representing integers shall be larger than 21). First, add them in $\mathbb{Z}_{21}$ and then map to $\mathbb{Z}_7 \times \mathbb{Z}_3$. Second, map both to $\mathbb{Z}_7 \times \mathbb{Z}_3$ and add afterwards. What do you observe? $\boxed{1}$

(iii) Pick two elements $x, y \in \mathbb{Z}_{21}$ (to make it interesting: the product of the representing integers shall be larger than 21). First, multiply them in $\mathbb{Z}_{21}$ and then map to $\mathbb{Z}_7 \times \mathbb{Z}_3$. Second, map both to $\mathbb{Z}_7 \times \mathbb{Z}_3$ and multiply afterwards. What do you observe? $\boxed{1}$

(iv) Mark all the invertible elements in $\mathbb{Z}_7$, $\mathbb{Z}_3$, and $\mathbb{Z}_{21}$. Do you note a relationship? $\boxed{1}$

Now consider $a, b \in \mathbb{Z}_{\geq 2}$ coprime.

(v) Suppose you are given $x \bmod ab, y \bmod ab \in \mathbb{Z}_{ab}$. Prove that $\boxed{2}$

$$(xy \bmod a, xy \bmod b) = ((x \bmod a) \cdot (y \bmod a), (x \bmod b) \cdot (y \bmod b)) .$$

(You might want to do, say, the first component first.) For short: the map $\mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b,\ x \bmod ab \mapsto (x \bmod a, x \bmod b)$ preserves the multiplication.

(vi) Suppose $u = x \bmod ab \in \mathbb{Z}_{ab}$ is invertible. Prove that $x \bmod a$ is invertible in $\mathbb{Z}_a$ and $x \bmod b$ is invertible in $\mathbb{Z}_b$. $\boxed{1}$

(vii) Now suppose that $x \bmod a$ in $\mathbb{Z}_a$ and $x \bmod b$ in $\mathbb{Z}_b$ are both invertible. Prove that then $x \bmod ab$ in $\mathbb{Z}_{ab}$ is invertible. $\boxed{1}$

(viii) Conclude that $\mathbb{Z}_{ab}^\times \to \mathbb{Z}_a^\times \times \mathbb{Z}_b^\times,\ x \bmod ab \mapsto (x \bmod a, x \bmod b)$ is well-defined and bijective. $\boxed{1}$

(ix) Derive that $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. $\boxed{1}$

Exercise 5.2 (An application). (4+2 points)

For RSA we consider a lot of numbers modulo $N = p \cdot q$. Since p and q are required to be different primes they are clearly coprime. Thus by the Chinese Remainder Theorem we know that $\mathbb{Z}_N$ is *isomorphic* to $\mathbb{Z}_p \times \mathbb{Z}_q$.

$\boxed{2}$ (i) Prove that we can compute $z := y^d \text{ rem } N$ by computing $z_1 := y^d \text{ rem } p$ and $z_2 := y^d \text{ rem } q$ and combining these into $z = (z_1 tq + z_2 sp) \text{ rem } N$ where $sp + tq = 1$.

Suppose that in a given implementation a multiplication modulo an k-bit number takes $\mathcal{O}(k^2)$ bit operations. Let p and q be both $n/2$-bit numbers.

$\boxed{1}$ (ii) How much time do we need to compute $z = y^d \text{ rem } N$?

$\boxed{1}$ (iii) How much time do we need to compute z as in (i)? (Do not count the computation of s and t because this can be done in a precomputation. So assume that sp and tq are given.)

$\boxed{+2}$ (iv*) Bob encrypts x and sends $y = x^e \text{ rem } N$ to Alice. Now, say, she actually does the decryption of y using (i). What do you think about the security of this approach? (Consider what happens if Alice, or her computing device, does an error in computing z_2 and gets z_2' instead of the correct value. How do x and $z' = z_1 tq + z_2' sp$ differ?)

Exercise 5.3 (Birthdays). (0+3 points)

$\boxed{+2}$ (i) Write a procedure that draws 23 random numbers from $\{1, 2, \ldots, 365\}$. Let it output 1 if it drew a number twice and 0 otherwise.

$\boxed{+1}$ (ii) Run the procedure, say, a thousand times, and derive the frequency with which a collision occured.

[As stated before: hand in printouts of your programs and their output.]