ETH Zürich, D-INFK
HS 2023, 24. November 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Solution 9

9.1 Diffie-Hellman

a) Let $g \in \langle \mathbb{Z}_n; \oplus \rangle$ be the generator, which Alice and Bob use as the basis. Alice chooses x_A at random from $\{0, \ldots, n-1\}$ and sends $y_A = R_n(g \cdot x_A)$. Analogously, Bob chooses x_B at random from $\{0, \ldots, n-1\}$ and sends $y_B = R_n(g \cdot x_B)$. The established shared key is $k_{AB} = R_n(g \cdot x_A \cdot x_B)$.

As shown in Example 5.27, we have $\gcd(g, n) = 1$. Therefore, Eve can use the Extended GCD algorithm to efficiently find an $a \in \mathbb{Z}$ such that $a \cdot g \equiv_n 1$. Then she can compute k_{AB} using the eavesdropped messages y_A and y_B as $k_{AB} = R_n(a \cdot y_A \cdot y_B)$. This is because

$$k_{AB} \equiv_n g \cdot x_A \cdot x_B \equiv_n g \cdot x_A \cdot (a \cdot g) \cdot x_B \equiv_n a \cdot (g \cdot x_A) \cdot (g \cdot x_B) \equiv_n a \cdot y_A \cdot y_B$$

b) Let us make Bob's argument more explicit: The Diffie-Hellman protocol using a cyclic group $G = \langle g \rangle$ is insecure if the discrete logarithm problem in G is easy. Since by Theorem 5.7 there exists an isomorphism $\varphi : G \to \mathbb{Z}_n$, one can compute x such that $g^x = h$ by instead computing x such that $\varphi(g)^x = \varphi(h)$. Since this can be done efficiently (both $\varphi(g)$ and $\varphi(h)$ are in $\mathbb{Z}_n$), Bob concludes that the discrete logarithm problem is easy in all cyclic groups.

Bob's argument is incorrect, because the above procedure is efficient only if the isomorphism φ can be efficiently computed, which is not always the case. For example, computing the isomorphism given in the proof of Theorem 5.7 requires solving the discrete logarithm problem in G (so Bob's procedure would give no advantage).

9.2 The Group $\mathbb{Z}_m^*$

a) The order of the group $\langle \mathbb{Z}_{36}^*; \odot \rangle$ is $\varphi(36)$. By Lemma 5.12,

$$\varphi(36) = (2-1) \cdot 2^{2-1} \cdot (3-1) \cdot 3^{2-1} = 2 \cdot 2 \cdot 3 = 12.$$

$\mathbb{Z}_{36}^*$ consists of all numbers in $\mathbb{Z}_{36}$ which are relatively prime with 36, that is, $\mathbb{Z}_{36}^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.

b) We will verify for each $a \in \mathbb{Z}_{11}^*$ whether it is a generator (but more efficiently than by computing $\langle a \rangle$). An $a \in \mathbb{Z}_{11}^*$ is a generator if and only if $\mathrm{ord}(a) = 10$. By Lagrange's Theorem, $\mathrm{ord}(a) \in \{1, 2, 5, 10\}$, so a is a generator if and only if $\mathrm{ord}(a) \notin \{1, 2, 5\}$, that is, if and only if $a \neq 1$, $a^2 \neq 1$ and $a^5 \neq 1$. We can now compute $R_{11}(a^2)$ and $R_{11}(a^5)$ for all $a \in \{2, \ldots, 10\}$. The generators are $2, 6, 7$ and 8.

Note. Another way to solve this exercise for any $\langle \mathbb{Z}_m^*; \odot \rangle$ is to first use Theorem 5.15 to determine whether $\langle \mathbb{Z}_m^*; \odot \rangle$ is cyclic. If so, it is isomorphic to $\langle \mathbb{Z}_{\varphi(m)}; \oplus \rangle$. Now we find one generator g of $\mathbb{Z}_m^*$ (by trying all possibilities) and prove that for any $i \in \mathbb{Z}_{\varphi(m)}$, g^i is a generator if and only if $\gcd(i, \varphi(m)) = 1$ (see Example 5.27).

c) We prove that $f : \mathbb{Z}_{nm}^* \to \mathbb{Z}_n^* \times \mathbb{Z}_m^*$, defined by $f(x) = (R_n(x), R_m(x))$ is an isomorphism. Throughout the proof we will use the fact that $\gcd(R_m(x), m) = \gcd(x, m)$ for any x, m, which follows from Lemma 4.2.

f **is a function.** We show that $f(x) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ for all $x \in \mathbb{Z}_{nm}^*$.
Let $x \in \mathbb{Z}_{nm}^*$, which means that $\gcd(x, nm) = 1$. Let $d = \gcd(x, n)$. Then, $d \mid x$ and $d \mid n$, which implies that $d \mid x$ and $d \mid nm$, so by the definition of $\gcd$, $d \mid \gcd(x, nm)$. Hence, $d \mid 1$, so $d = 1$. Therefore, $\gcd(R_n(x), n) = \gcd(x, n) = 1$, so $R_n(x) \in \mathbb{Z}_n^*$.
The proof that $R_m(x) \in \mathbb{Z}_m^*$ is analogous.

f **is surjective.** Take any $(a, b) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Since $\gcd(m, n) = 1$, by CRT, there exists an $x \in \mathbb{Z}_{nm}$ such that $(R_n(x), R_m(x)) = (a, b)$. To show that $x \in \mathbb{Z}_{nm}^*$, assume towards a contradiction that $d = \gcd(x, nm) > 1$. Let p be an arbitrary prime in the decomposition of d. Since $p \mid mn$, by Lemma 4.7, $p \mid n$ or $p \mid m$. In the first case, since also $p \mid x$, we get $p \mid \gcd(x, n)$. But $\gcd(x, n) = \gcd(R_n(x), n) = \gcd(a, n) = 1$ (because $a \in \mathbb{Z}_n^*$), so this is a contradiction. Analogously, in the second case we get $p \mid \gcd(b, m)$.

f **is injective.** By CRT, the x defined above is unique in $\mathbb{Z}_{nm}$, hence, it is also unique in $\mathbb{Z}_{nm}^*$.

f **is a homomorphism.** For any $a, b \in \mathbb{Z}_{nm}^*$,

$$\begin{aligned}
f(a \odot_{nm} b) &= (R_n(a \odot_{nm} b), R_m(a \odot_{nm} b)) \\
&= (R_n(R_{nm}(ab)), R_m(R_{nm}(ab))) \\
&= (R_n(ab),\ R_m(ab)) \\
&= (R_n(R_n(a) \cdot R_n(b)),\ R_m(R_m(a) \cdot R_m(b))) \\
&= (R_n(a) \odot_n R_n(b),\ R_m(a) \odot_m R_m(b)) \\
&= (R_n(a), R_m(a)) \star (R_n(b), R_m(b)) \ ^1 \\
&= f(a) \star f(b).
\end{aligned}$$

9.3 An RSA Attack

First, consider the case when n_1, n_2 and n_3 are not relatively prime. Without loss of generality, assume that $\gcd(n_1, n_2) > 1$. We can now use the Extended GCD algorithm to compute $p = \gcd(n_1, n_2)$ and this way efficiently factorize n_1. This allows us to compute the secret key of Alice and decrypt c_1.

[1] The operation $\star$ on $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$ is defined as $(a_1, b_1) \star (a_2, b_2) := (a_1 \odot_n a_2,\ b_1 \odot_m b_2)$.

Secondly, assume that n_1, n_2 and n_3 are relatively prime. Consider the following system of congruence equations:

$$\begin{aligned} x &\equiv c_1 \pmod{n_1} \\ x &\equiv c_2 \pmod{n_2} \\ x &\equiv c_3 \pmod{n_3} \end{aligned}$$

Let $N = n_1 n_2 n_3$. Using the Chinese Remainder Theorem, we can efficiently find the solution x_0 to the above system of equations, such that $0 \leq x_0 < N$.
Notice now that m^3 is also a solution to the system of equations, because $c_i \equiv m^3 \pmod{n_i}$ for $i \in \{1, 2, 3\}$. Moreover, since $0 \leq m < n_i$ for $i \in \{1, 2, 3\}$, we have $0 \leq m^3 < n_1 \cdot n_2 \cdot n_3 = N$. Since by the Chinese Remainder Theorem x_0 is unique in $\{0, \ldots, N-1\}$, it follows that $x_0 = m^3$.
What is left is to compute the cube root of x_0 over $\mathbb{Z}$, which can be done efficiently.

Note. This attack is also possible for $e > 3$. However, for given e one needs e ciphertexts, each encrypted for a different recipient.

9.4 Non Minimality of Ring Axioms

We only need to show that the operation $+$ is commutative. Let $a, b \in R$.
We have

$$\begin{aligned} (1+1)(a+b) &= (1+1)a + (1+1)b && \text{(Axiom iii), distributivity)} \\ &= (1a+1a) + (1b+1b) && \text{(Axiom iii), distributivity, twice)} \\ &= (a+a) + (b+b) && \text{(Axiom ii), neutral element)} \\ &= a+a+b+b && \text{(Axiom i), associativity)} \end{aligned}$$

But also

$$\begin{aligned} (1+1)(a+b) &= 1(a+b) + 1(a+b) && \text{(Axiom iii), distributivity)} \\ &= (1a+1b) + (1a+1b) && \text{(Axiom iii), distributivity, twice)} \\ &= (a+b) + (a+b) && \text{(Axiom ii), neutral element)} \\ &= a+b+a+b && \text{(Axiom i), associativity)} \end{aligned}$$

Therefore

$$\begin{aligned} & a+b+a+b = a+a+b+b \\ \stackrel{\cdot}{\iff}\ & a+b+a+b+(-b) = a+a+b+b+(-b) && \text{(Add } -b \text{ on the right)} \\ \stackrel{\cdot}{\iff}\ & a+b+a = a+a+b && \text{(Axiom i), associativity and inverse)} \\ \stackrel{\cdot}{\iff}\ & (-a)+a+b+a = (-a)+a+a+b && \text{(Add } -a \text{ on the right)} \\ \stackrel{\cdot}{\iff}\ & b+a = a+b && \text{(Axiom i), associativity and inverse)} \end{aligned}$$

9.5 Elementary Properties of Rings

a) We have

$$(-a)b + ab \overset{\text{distrib.}}{=} (-a+a)b \overset{\text{def. inverse}}{=} 0b \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

Therefore, $(-a)b$ is the additive inverse of ab, which means that $(-a)b = -ab$.

b) We have

$$\begin{aligned}(-a)(-b) + (-(ab)) &\overset{\text{a)}}{=} (-a)(-b) + (-a)b \overset{\text{distrib.}}{=} (-a)(-b+b)\\ &\overset{\text{def. inverse}}{=} (-a)0 \overset{\text{Lemma 5.17 (i)}}{=} 0.\end{aligned}$$

Therefore, $(-a)(-b)$ is the additive inverse of $-(ab)$, which means that $(-a)(-b) = -(-(ab)) = ab$.

9.6 Properties of Commutative Rings

a) From $a|b$ it follows that $\exists d\ b = ad$ and, thus, $bc = (ad)c = a(dc)$. Hence, $a|bc$.

b) From $a|b$ it follows that $\exists d\ b = ad$ and from $a|c$ it follows that $\exists e\ c = ae$. By the distributive law, we have $b + c = ad + ae = a(d + e)$. Hence, $a|(b + c)$.

9.7 Ideals in Rings

a) We have $0 = x0 \in (x)$. Let $a, b \in (x)$. Than $a = xk_1$ and $b = xk_2$ for $k_1, k_2 \in \mathbb{Z}$, so that $a + b = x(k_1 + k_2) \in (x)$. This shows that (x) is an additive subgroup of R. Let $a \in (x)$ and $z \in \mathbb{Z}$. We have $az = (xk)z = x(kz) \in (x)$ for some $k \in \mathbb{Z}$. This shows that (x) is closed under multiplication by elements of $\mathbb{Z}$.

b) Let I be an ideal of $\mathbb{Z}$. If $I = \{0\}$ then $I = (0)$. Let d be the smallest positive element of I. Suppose $d \neq 1$. Let $x \in I$. We can write $x = qd + r$ with $0 \leq |r| < d$. We can also rewrite this as $r = x - qd$, and since both x and qd are elements of I, then $r \in I$. We can assume $r \geq 0$ (otherwise, $-r \in I$ is positive). But then r is positive and smaller than d which means $r = 0$ by assumption on d. This shows $I = (d)$.

c) First of all $0 = 0x+0y \in (x, y)$. Also, if $a, b \in (x, y)$ then $a = xk_1+y\ell_1$ and $b = xk_2+y\ell_2$ for some $k_1, k_2, \ell_1, \ell_2 \in R$. Therefore $a + b = x(k_1 + k_2) + b(\ell_1 + \ell_2) \in (x, y)$. This shows that (x, y) is an additive subgroup of R. Let $a \in (x, y)$ and $r \in \mathbb{R}$. Then $ar = (xk + y\ell) = x(kr) + y(\ell r) \in (x, y)$. This shows that (x, y) is closed under multiplication by elements of R.

d) Suppose that there exists $p(x) \in \mathbb{Z}[x]$ such that $(p(x)) = (2, x)$. If $\deg p(x) \geq 1$, then the product of $\deg p(x)f(x) \geq 1$ for all $0 \neq f \in \mathbb{Z}[x]$, so that $2 \notin (p(x))$. Suppose then that $\deg p(x) = 0$. Since $p(x) \in I$, then $p(x) = 2k$ for some $k \in \mathbb{Z}$. But then $p(x)f(x) \iff (2k)(f(x)) = x$. If a is the coefficient of the first degree term of $f(x)$, we would have $(2k)a = 2(ka) = 1$, but 2 does not have an inverse in $\mathbb{Z}$. This concludes the proof.

The proof of subtask b) does not go through here because we cannot perform division with remainder in $\mathbb{Z}[x]$.