Technische Universität München (I7)
Dr. M. Luttenberger / S. Jaax

Winter term 2017/2018
2019/01/10

Solution

Cryptography – Homework 5

Discussed on Tuesday, 8th January, 2018.

Exercise 5.1 Warm-up II

(a) $\mathbb{Z}_{54}^*$ is a cyclic group. What is its order? Determine a generator g of $\mathbb{Z}_{54}^*$ and solve $7^x \equiv 19 \bmod 54$ for x (i.e. compute the discrete logarithm of 19 to the base 7).

(b) Let $\pi = [23154] \in S_5$. Determine π^{842}.

(c) Compute the greatest common divisor d of 234, 762, and 139. Furthermore determine $r, s, t \in \mathbb{Z}$ such that $r \cdot 234 + s \cdot 762 + t \cdot 139 = d$.

(d) Solve for X: $X \equiv 2 \bmod 5 \wedge X \equiv 5 \bmod 11 \wedge X \equiv 1 \bmod 21$.

(e) We have seen that it is fairly easy to compute square roots modulo certain primes. Let $p = 47$. Solve for X: $X^2 \equiv 6 \bmod 47$ (*Hint*: $p \equiv 3 \bmod 4$ since p is a safe prime).

Solution:

(a) $|\mathbb{Z}_{54}^*| = \varphi(54) = \varphi(2 \cdot 3^3) = \varphi(2) \cdot \varphi(3^3) = 1 \cdot (3^3 - 3^2) = 18$. A possible generator is 5 because $5^9 \equiv_{54} 53 \neq 1$ and $5^6 \equiv_{54} 19 \neq 1$. A possible solution to $7^x \equiv_{54} 19$ is $x = 3$ (brute-force).

(b) $|S_5| = 5! = 120$, therefore $\pi^{842} = \pi^2 = [31245]$. Note that we can always reduce exponents modulo the order of the group we compute in!

(c) $\mathsf{gcd}(234, 762, 139) = \mathsf{gcd}(234, \mathsf{gcd}(762, 139)) = \mathsf{gcd}(234, 1) = 1$ (or shortcut: 139 is a prime therefore it must be 1)

(d) This is the CRT "backwards". We have $1 = 1 \cdot 11 - 2 \cdot 5$ and therefore the three equations reduce to two: $X = 2 \cdot 11 - 2 \cdot 5 \cdot 5 \bmod 55 \wedge X = 1 \bmod 21$. Which gives us $X = 27 \bmod 55 \wedge X = 1 \bmod 21$. By using the extended euclidean algorithm we get $1 = 21 \cdot 21 - 8 \cdot 55$ and thus the final solution is: $X = 27 \cdot 21 \cdot 21 - 1 \cdot 8 \cdot 55 \bmod 55 \cdot 21$ which is $X = 1072 \bmod 1155$. One can easily check that 1072 satisfies all three equations—so we have not made a mistake :).

(e) Modulo primes with $p \equiv 3 \bmod 4$ we can compute square-roots easily: $6^{\frac{p+1}{4}} = 6^{12} = 37 \bmod 47$. (Check: $37^2 = 6 \bmod 47$)

Exercise 5.2 Applications of the CRT

The Chinese remainder theorem states that $\mathbb{Z}_{NM}^* \simeq Z_N^* \times Z_M^*$ for $\mathsf{gcd}(M, N) = 1$. An important practical consequence of the CRT is the possibility to do computations with smaller numbers and thus to reduce the running time of algorithms in certain situations (e.g. when decrypting an RSA encrypted message).

(a) Compute all solutions to the quadratic equation $X^2 \equiv 118 \bmod 221$

(b) Find all solutions to $X^2 \equiv 1 \bmod 175$

(c) For $p = 13$ and $q = 19$ set $n = pq$. Let $e = 127$ and $d = e^{-1} \bmod \varphi(n)$. Given $c := 197 = m^e \bmod n$. Determine d and then m via $m = c^d \bmod n$. (this is Textbook-RSA with very small primes :))

Solution:

(a) As $221 = 13 \cdot 17$ we can compute in $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$ instead of solving the equation in $\mathbb{Z}_{221}$. By the Chinese remainder theorem we obtain a pair of equations: $X^2 \equiv 118 \bmod 13$ and $X^2 \equiv 118 \bmod 17$ which are equivalent to $X^2 \equiv 1 \bmod 13$ and $X^2 \equiv 16 \bmod 17$. The first equation has solutions $x_1 = 1$ and $x_2 = -1 = 12$. while the second equation has solutions $y_1 = 4$ and $y_2 = -4 = 13$. The pair of equations in $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$ therefore has four solutions: $\{(1, 4), (1, 13), (12, 4), (12, 13)\}$ which can be mapped back to $\mathbb{Z}_{221}$ via the transformation $(x, y) \mapsto x \cdot (-3) \cdot 17 + y \cdot (4 \cdot 13)$.

(b) We apply the CRT and note that $175 = 7 \cdot 5^2$. We get two equations: $X^2 = 1 \bmod 7$ (with solutions $x'_1 = 1$ and $x'_2 = 6$) and $X^2 = 1 \bmod 5^2$ with solutions $x'_3 = 1$ and $x'_4 = 24$). We recombine these solutions (4 possibilities) to get the solutions to the original equation: $x_1 = h^{-1}(1,1) = 1$, $x_2 = 76$, $x_3 = 99$ and $x_4 = 174$.

(c) d can be determined by the extended euclidean algorithm: $\mathsf{gcd}(e, \varphi(n)) = 1$ and we find $1 = (-17) \cdot e + 10 \cdot \varphi(n)$ thus $d = -17 = 199 \bmod \varphi(n)$. Retrieving m can be done by computing $197^d \bmod n$ but the numbers are rather large and therefore we rather apply the CRT to compute in $\mathbb{Z}_p \times \mathbb{Z}_q$ instead of $\mathbb{Z}_n$.

We have $c = 197 \equiv_{19} 7$ and $d = 199 =\equiv_{18} 1$ (reducing the exponent), thus $197^d = 7 \bmod 19$. Moreover $c = 197 \equiv_{13} 2$ and $d = 199 \equiv_{12} 7$, thus $197^d = 2^7 = 128 = 11 \bmod 13$. Putting it all together again by moving back to $\mathbb{Z}_{13 \cdot 19}$ (note that $3 \cdot 13 - 2 \cdot 19 = 1$) we get: $197^d = 7 \cdot (3 \cdot 13) - 11 \cdot (2 \cdot 19) = -145 = 102 = m$.

Exercise 5.3 φ vs. λ

Let $p = 7$, $q = 11$, and $N = pq$. Furthermore set $e = 7$.

(a) Compute $\varphi(N)$ and $\lambda(N)$.

(b) Compute $e^{-1} \bmod \varphi(N)$ and $e^{-1} \bmod \lambda(N)$.

(c) Compute $\mathbb{Z}^*_{\varphi(N)}$ and $\mathbb{Z}^*_{\lambda(N)}$. How are both set related?

(d) Prove that for $N = pq$ with $p \neq q$ prime and for any $e \in \mathbb{N}$, $\mathsf{gcd}(e, \varphi(N)) = 1$ if and only if $\mathsf{gcd}(e, \lambda(N)) = 1$.

Solution:

(a) $\varphi(N) = 6 \cdot 10 = 60$ and $\lambda(N) = lcm(6, 10) = 30$.

(b) $e^{-1} = 13 \bmod 30$ and $e^{-1} = 43 \bmod 60$.

(c) $\mathbb{Z}^*_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}$ and $\mathbb{Z}^*_{60} = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}$. Hence, $\mathbb{Z}^*_{\lambda(N)} \subseteq \mathbb{Z}^*_{\varphi(N)}$. This also holds in general: Cauchy's theorem states that for every finite group G, and every prime factor p of $|G|$, there exists a group element $a \in G$ satisfying $\mathrm{ord}(a) = p$. Hence $\lambda(N) = \mathsf{lcm}\{\mathrm{ord}(a) \mid a \in \mathbb{Z}^*_N\}$ and $\varphi(N) = |\mathbb{Z}^*_N|$ share the same set of unique prime factors for every N. Thus for every N and every $x < \lambda(N)$ we have: If x is co-prime to $\lambda(N)$, then x is also co-prime to $\varphi(N)$.

(d) Recall that for natural numbers a, b we have $lcm(a, b) = \frac{ab}{\mathsf{gcd}(a,b)}$. Since $\lambda(N) = lcm(p-1, q-1)$ and $\varphi(N) = (p-1)(q-1)$, we have $\varphi(N) = \mathsf{gcd}(p-1, q-1) \cdot \lambda(N)$. Thus, if $\mathsf{gcd}(e, \varphi(N)) = 1$ then for sure $\mathsf{gcd}(e, \lambda(N)) = 1$.

On the other hand, by the last exercise we have $\mathbb{Z}^*_{\lambda(N)} \subseteq \mathbb{Z}^*_{\varphi(N)}$. Hence $e \in \mathbb{Z}^*_{\lambda(N)} \Rightarrow e \in \mathbb{Z}^*_{\varphi(N)}$.

Exercise 5.4

(a) Let $\langle \mathbb{G}, \cdot, 1 \rangle$ be a finite cyclic group with generator g. Denote by $q := |\mathbb{G}|$ the order of $\mathbb{G}$.

Assume $q = d \cdot m$ is a composite and let d be a non-trivial factor of q. Let $y \in \mathbb{G}$.

Show:

If $k \in \mathbb{N}$ satisfies $g^k = y$ in $\mathbb{G}$, then $(k \bmod d)$ is the unique solution of the following problem:

$$\text{Determine } x \in \mathbb{Z}_d \text{ such that } (g^m)^x = y^m \text{ in } \mathbb{G}.$$

(b) Given are the prime 89 and the generator 3 of $\langle \mathbb{Z}^*_{89}, \cdot, 1 \rangle$.

Your task is to determine $k \in \mathbb{Z}$ such that $3^k \equiv 86 \pmod{89}$. Proceed as follows:

i) Using the preceding exercise, first determine k modulo 11.

ii) Someone tells you that $k \equiv 5 \pmod 8$. Determine k.

Solution:

(a) Let $k \in \mathbb{N}$ satisfy $g^k = y$ in $\mathbb{G}$.

Set $k_d := (k \bmod d)$. Then for a suitable $l \in \mathbb{Z}$ we have $k_d = k - l \cdot d$. Hence:

$$(g^m)^{k_d} = g^{m \cdot k_d} = g^{m \cdot k - l \cdot d \cdot m} = (g^k)^m \cdot (g^{md})^l = y^m \cdot (g^q)^l = y^m \cdot 1^l = y^m$$

Hence, k_d is a solution of $(g^m)^x = y^m$.

Let $x \in \mathbb{Z}_d$ be any other solution of $(g^m)^x = y^m$. Then:

$$1 = (g^m)^{x-k_d}$$

Wlog. assume $k_d \leq x$ (else swap x and k_d). As both $x, k_d \in \mathbb{Z}_d$, we also have $x - k_d \in \mathbb{Z}_d$. Trivially, g^m has order $q/m = d$. So, $1 = (g^m)^{x-k_d}$ implies that $(x - k_d)$ is a multiple of d, hence $x - k_d = 0$ (as 0 is the only multiple of d in $\mathbb{Z}_d$) resp. $x = k_d$.

(b) We have $q = |\mathbb{Z}_{89}^*| = 88 = 11 \cdot 8$.

In order to determine $k_{11} := (k \bmod 11)$, we need to solve

$$(3^8)^x \equiv_{89} 86^8 \equiv_{89} (-3)^8 \equiv_{89} 3^8$$

for which the only solution in $\mathbb{Z}_{11}$ is $k_{11} = 1$.

We also have $k_5 := (k \bmod 8) = 5$.

By the CRT $\mathbb{Z}_{88} \cong \mathbb{Z}_8 \times \mathbb{Z}_{11}$ (the additive group, as $\mathbb{Z}_{89}^* \cong \mathbb{Z}_{88}$).

Either by using the extended Euclidean algorithm or by educated guessing: $1 = \mathsf{gcd}(8, 11) = -4 \cdot 8 + 3 \cdot 11$.

Hence, the isomorphism form $\mathbb{Z}_8 \times \mathbb{Z}_{11}$ to $\mathbb{Z}_{88}$ is given by

$$h(x_8, x_{11}) = (33 \cdot k_8 - 32 \cdot k_{11}) \bmod 88.$$

Thus: $k = h(5, 1) = 45$ and $3^{45} \equiv_{89} 86$.

Exercise 5.5 Computing Discrete Logarithms

Let p be prime. Assume there is a generator $g \in \mathbb{Z}_p^*$ such that computing the discrete logarithm in $\mathbb{Z}_p^*$ with respect to g can be done efficiently. Show that then the discrete logarithm with respect to any other generator g' of $\mathbb{Z}_p^*$ can also be computed efficiently.

Solution: Let $g \neq g'$ and $y \in \mathbb{Z}_p^*$. We show: Computing x with $(g')^x = y$ in $\mathbb{Z}_p^*$ can be reduced to computing discrete logarithms using g as base.

- Since g is a generator of $\mathbb{Z}_p^*$, we know that there exists a $k \in \{1, \ldots, p-1\}$ such that $g^k = g'$ in $\mathbb{Z}_p^*$. Now we can restate the problem as $(g')^x = y \Leftrightarrow g^{kx} = y$.
- Recall now that for every $s \in \mathbb{N}$, since p is prime,

  $$g^s = g^{s \bmod (p-1)} \text{ holds in } \mathbb{Z}_p^*.$$

  The idea is to exponentiate g^{kx} by a suitable l to "get rid" of the k in the computation. For this we show that $\mathsf{gcd}(k, p-1) = 1$. Assume that $\mathsf{gcd}(k, p-1) = d \geq 1$. Then there are $\alpha, \beta \in \mathbb{N}$ such that $k = d \cdot \alpha$ and $(p-1) = d \cdot \beta$. Hence $\beta \leq p-1$. Now we compute in $\mathbb{Z}_p^*$:

  $$(g')^\beta = \left(g^k\right)^\beta = g^{d\alpha\beta} = g^{\alpha(p-1)} = 1,$$

  since $(p-1)$ is the order of $\mathbb{Z}_p^*$. Hence g' can generate at most β elements in $\mathbb{Z}_p^*$: $p-1 = o_{g'} \leq \beta \leq p-1$. Hence $\beta = p-1$ and $d = 1$. With this we can compute $l \in \mathbb{Z}_{p-1}^*$ such that $l \cdot k = 1$ in $\mathbb{Z}_{p-1}^*$ (using e.g. the extended Euclidean algorithm).
- Now we calculate in $\mathbb{Z}_p^*$:

  $$\begin{aligned} & g^{kx} = y \\ \Leftrightarrow\ & g^{kxl} = y^l && (\text{ Exponentiate with } l) \\ \Leftrightarrow\ & g^{klx \bmod (p-1)} = y^l && (\phi(p) = p-1) \\ \Leftrightarrow\ & g^x = y^l && (k \cdot l \equiv 1 \bmod (p-1)) \end{aligned}$$

In summary, the following steps are needed for computing x such that $g^x = y$:

1. Compute $k \in \{1, \ldots, p-1\}$ such that $g^k = g'$ in $\mathbb{Z}_p^*$.
2. Compute $l \in \{1, \ldots, p-2\}$ such that $k \cdot l = 1$ in $\mathbb{Z}_{p-1}^*$.
3. Compute $x \in \{1, \ldots, p-1\}$ such that $g^x = y^l$ in $\mathbb{Z}_p^*$.