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

**Winter term 2017/2018**
**2019/01/05**

# 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 $\pi^{842}$.

(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).

## 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 :))

## Exercise 5.3 $\varphi$ vs. $\lambda$

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 groups related to each other?

(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 $\mathsf{gcd}(e, \lambda(N)) = 1$.

## 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 $k$.

**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.