PUBLIC KEY CRYPTOGRAPHY - Mathematics

Project 2 (Weeks 3-4)

Topics: ciphers, congruences, (pseudo)primality.

- You will prepare and explain a written homework on one of the following questions, which will be assigned to you during the seminars:

  1. Explain Kasiski's test for determining the key length for the Belaso cipher, and apply it in an example.
  2. Determine the formula for the number of keys for the Hill cipher, and apply it in an example.
  3. Prove the Chinese Remainder Theorem.
  4. Prove the properties of Euler's function.
  5. Let $n \in \mathbb{N}$ be odd composite. Prove that:
     (i) If n is divisible by a perfect square greater than 1, then n is not a Carmichael number.
     (ii) If n is not divisible by a perfect square greater than 1, then n is a Carmichael number if and only if $p-1|n-1$ for every prime $p|n$.
  6. Let $n \in \mathbb{N}$ be odd composite, and b, b_1, b_2 integers which are relatively prime to n. Prove that:
     (i) n is pseudoprime to the base b if and only if the order of b in $(\mathbb{Z}_n^*, \cdot)$ (that is, the smallest positive power of b which is equal to 1 modulo n) divides $n-1$.
     (ii) If n is pseudoprime to the bases b_1 and b_2, then n is pseudoprime to the base $b_1 b_2^{-1}$, where b_2^{-1} is an integer which is inverse to b_2 modulo n.
  7. Let $n = pq$ be a product of two distinct primes, $d = gcd(p-1, q-1)$ and b an integer. Prove that n is pseudoprime to the base b if and only if $b^d \equiv 1 \bmod n$. In terms of d how many bases are there to which n is a pseudoprime?
  8. Let b be an integer. Construct an infinite number of pseudoprimes to the base b, and give some examples.
  9. Let $n \in \mathbb{N}$ be odd composite, and b an integer with $gcd(b, n) = 1$. Prove that if n is strong pseudoprime to the base b, then n is pseudoprime to the base b. Give examples of n and b such that n is pseudoprime to the base b, but not strong pseudoprime to the base b.
  10. Prove a criterion which describes all generators of the cyclic group $(\mathbb{Z}_n, +)$, where $n \geq 2$ is a natural number. A *generator* of $(\mathbb{Z}_n, +)$ is an element $\hat{g} \in \mathbb{Z}_n$ such that for every $\hat{x} \in \mathbb{Z}_n$ there exists $k \in \{0, 1, \ldots, n-1\}$ such that $\hat{x} = k\hat{g}$.

Points

- **1 point** if handed in by Week 5 or Week 6.
- **0.5 points** if handed in by Week 7 or Week 8.