Modern Cryptology (236506) – Exercise no. 2

Submission in singles until 29/04/2019

The exercise must be typed and printed.

1. Prove that the following ciphers are not perfect when used on long plaintexts, using as few blocks as you can. There is no need to prove that the number of blocks is indeed minimal.
   
   (a) DES.
   (b) AES-128 (AES with 128-bit keys).
   (c) AES-256 (AES with 256-bit keys).

2. Prove the complementation property of DES.

3. During the school’s sports day, the gym teacher tried to hold a ball game tournament. First, he tried to split the students into soccer teams (11 players), but 4 students were left out. He then tried handball teams (7 players), but again, 4 students were left out. Finally, he decided on playing basketball (5 players in each team), in which case all students were split into teams.

   At the end of the day, the teacher recalled he did not count the exact number of participants, though he estimated their number to be around 1000. Help the teacher find the accurate number, using the methods taught in class. Write your calculations explicitly.

4. Let $\varphi$ be Euler’s function. Prove the following:
   
   (a) For any $a, b \in \mathbb{N}$ such that $\gcd(a, b) = 1$, $\varphi(a)\varphi(b) = \varphi(ab)$.
   (b) For any prime $p$ and $e \geq 1$, $\varphi(p^e) = (p - 1)p^{e-1} = p^e - p^{e-1}$.
   (c) For any $n \in \mathbb{N}$, where $n = p_1^{e_1} \ldots p_k^{e_k}$ and $p_1, \ldots, p_k$ are distinct primes: $\varphi(n) = n \cdot \prod_{i=1}^{k} (1 - \frac{1}{p_i})$.
   (d) For any $n \in \mathbb{N}$, $\sum_{d|n} \varphi(d) = n$. 

1
5. In this question we discuss a variant of Wilson’s theorem. For an integer \( m > 2 \), let \( P \) be the product of the elements in \( \mathbb{Z}_m^\times \).

(a) Show that \( P = \pm 1 \pmod{m} \), without using Wilson’s theorem.

Hint: split \( \mathbb{Z}_m^\times \) into two subsets, \( x : x^2 = 1 \pmod{m} \) and \( x : x^2 \neq 1 \pmod{m} \), and calculate the product of each set separately.

(b) Give an example for an \( m \) such that there are more than 2 solutions to the equation \( x^2 = 1 \pmod{m} \).

(c) In the special case where \( m \) is a prime, what are all the solutions to the congruence \( x^2 = 1 \pmod{m} \)?

(d) Deduce Wilson’s theorem from the above claims.