CS 463/563: Cryptography for Cybersecurity

Spring 2024

Homework #2 (Module 2)

Points: 20

Note: Modular arithmetic is fundamental to cryptography. In this system, you can only have integers. For example, in mod 14 system, the answer MUST be 0,1,2,3,…9,11,12,13. Non-integer values have no place in this arithmetic. If you have an answer which is a floating point, such as 12.5, then you are doing something wrong.

Question 1: [10 points]. Modular Arithmetic: Compute the following without a calculator. SHOW YOUR WORK.

i. **150 * 92 mod 14** (Hint: a*b mod c = ((a mod c) * (b mod c)) mod c)

ii. **6 * (4/11) mod 14** (Hint: In mod 14 system, a, a+14, a+28, a+42, a+56, etc. are all equivalent)

iii. **24/17 mod 14** (Hint: First, simplify the numerator and denominator separately by applying the mod function independently, and then solve as in (ii) above)

iv. $\mathbf{4^8 * 5^{12}}$ **mod 14** (Hint: Try to compute the exponent in stages, each time simplifying it using the mod function. For example, to compute 48 mod 14, express 48 mod 14 = (42 mod 14)4 mod 14, compute the one in the parenthesis, and repeat this process)

v. $\mathbf{5^{10} * 6^8}$ **mod 14** (same as above)

Question 2: [10 points]. SHOW YOUR WORK. You may use EXCEL or a calculator.

i. Show the elements of groups $\mathbf{Z_{13}}$ and Z^*_{13} (Note that 13 is a prime number)

ii. Show the elements of groups $\mathbf{Z_{18}}$ and Z^*_{18} (Note that 18 is NOT a prime number)

iii. Find the order of **5** in $\mathbf{Z^*_{13}}$ (Hint: Order of an element in a finite group G is the smallest positive integer k such that ak =1 where 1 is the identity element of G)

iv. Find (if it exists) the multiplicative inverse of $\mathbf{5} \in \mathbf{Z_{13}}$ (integer ring) (Hint: For a ∈ Zn, its multiplicative inverse, if it exists, is defined as a-1 such that a.a-1 ≡ 1 mod n)

v. Is $\mathbf{Z^*_{13}}$ a cyclic group? If so, what is its order and the generator element? (Hint: group G which contains some element α with maximum order ord(α) = |G| is said to be cyclic. Elements with maximum order are called generators)

What to submit? Submit a single pdf file with your answers on Canvas. Show your work.