CS-463/563 Crytography for Cyber Security
Fall 2023
Homework Assignment #2

August 9, 2023

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. $150 * 92 \bmod 14$ (Hint: $a * b \bmod c = ((a \bmod c) * (b \bmod c)) \bmod c$)

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

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

iv. $4^8 * 5^{12} \bmod 14$ (Hint: Try to compute the exponent in stages, each time simplifying it using the mod function. For example, to compute $4^8 \bmod 14$, express $4^8 \bmod 14 \equiv (4^2 \bmod 14)^4 \bmod 14$, compute the one in the parenthesis, and repeat this process.

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

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

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

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

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

iv. Find (if it exists) the multiplicative inverse of $5 \in \mathbb{Z}_{13}$ (integer ring) (Hint: For $a \in \mathbb{Z}n$, its multiplicative inverse, if it exists, is defined as a^{-1} such that $a.a^{-1} \equiv 1 \bmod n$.)

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

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