Introduction to Cryptography, Spring 2024

Homework 1

Due: 3/5/2024 (Tuesday)

Notes:

(1) **Show necessary steps of your computation in your homework. I don't want just the answers.**

(2) **Submit a "hardcopy" right after the class on the due day. If you are not able to attend the class, submit it to EC238 before the due day. I don't accept late submission.**

1. Compute the values of $75 \bmod 47$ and $-115 \bmod 47$
2. Use the extended Euclidean algorithm to solve the equation $235\mathrm{x} + 53\mathrm{y} = 1$ for integers x and y
3. Use Euler's theorem to compute $23^{1562} \bmod 31$ and $23^{1562} \bmod 35$
4. Use the Rabin-Miller method to determine whether 133 and 137 are prime with confidence at least 98%?
5. Use CRT to solve the system of equations: $x \bmod 4 = 2, x \bmod 9 = 7, x \bmod 11 = 5$, for integer x , $0 \leq x \leq 395$
6. Find all roots of $1 = x^{\phi(22)} \bmod 22$ and compute their orders.
7. Use the baby-step-giant step algorithm to solve all possible values for $x = \mathrm{dlog}_{5,23}(17)$