Cryptography
Homework #2
Fall 2018

Due Monday, October 29

(1) Write a multiplication table for $(Z/10Z)^*$, note this is the group of units mod 10. Another notation for this is U(10).

(2) Compute the following values of Euler's function.
(a) $\phi(8712)$
(b) $\phi(4794327)$

(3) Compute the powers below in two ways: using the fast power algorithm and Euler's Theorem.
(a) $14^{225} \pmod{53}$
(b) $14^{3969} \pmod{101}$

(4) The following concerns the Diffie-Hellman key exchange. Alice and Bob use a prime $p = 31$ and base $g = 3$.
(a) Alice picks $a = 3$ as her secret key. What is her public key A?
(b) Bob picks $b = 7$ as his secret key. What is his public key B?
(c) What is their shared secret key?
(d) Alice and Bob use a symmetric cipher $c \equiv km \pmod{p}$ where k is their shared secret key. Alice codes the message HELPME by converting letters to the corresponding number in the range 1-26 and sends it to Bob.
(e) Show how Bob decodes the cipher.
(f) Explain why $g = 2$ would be a poor choice of base for this prime.

(5) Compute the following discrete logarithms if it exists (note there is no good method to do this)
(a) $\log_3 19 \pmod{29}$
(b) $\log_{10} 32 \pmod{53}$

(6) (a) Compute the order of 16 in U(199)
(b) Find 4 elements of order 47 in U(187)

(7) You are going to encode messages using the function $f(x) = x^{71} \pmod{2879}$

(a) Encode the following message two letters at a time (using the numbers 1-26). Don't worry about capitalization or punctuation.

"These are the times that try men's souls. The summer soldier and the sunshine patriot will, in this crisis, shrink from the service of their country"

(b) Compute the inverse decoding function **g(*x*)** (as discussed in class).

(c) Check that the decoding function recovers the original message.

(8) (a) Use the Chinese Remainder Theorem to find the smallest positive solution to the system of congruences: $x \equiv 34 \pmod{43}$, $x \equiv 2 \pmod{97}$, $x \equiv 20 \pmod{29}$

(b) Use Euler's Product Formula to compute $\phi(96)$, $\phi(245)$, $\phi(936)$