Cryptography
Homework #2 Solutions
Fall 2018

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

U(10) = {1,3,7,9} The multiplication table is:

	1	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

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

(a) $8712 = 2^3 3^2 11^2 \Rightarrow \phi(8712) = 8712\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{11}\right) = 2640$

(b)

$$4794327 = 3^2 * 19 * 23^2 * 53 \Rightarrow \phi(4794327) = 4794327 * \left(1-\frac{1}{3}\right)\left(1-\frac{1}{19}\right)\left(1-\frac{1}{23}\right)\left(1-\frac{1}{53}\right) = 2841696$$

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

(a) Fast power
225 = 128 + 64 + 32 + 1

$14^1 \equiv 14 \pmod{53}$

$14^2 \equiv 196 \equiv 37 \pmod{53}$

$14^4 \equiv 37^2 \equiv 1369 \equiv 44 \pmod{53}$

$14^8 \equiv 44^2 \equiv 1936 \equiv 28 \pmod{53}$

$14^{16} \equiv 28^2 \equiv 784 \equiv 42 \pmod{53}$

$14^{32} \equiv 42^2 \equiv 1764 \equiv 15 \pmod{53}$

$14^{64} \equiv 15^2 \equiv 225 \equiv 13 \pmod{53}$

$14^{128} \equiv 13^2 \equiv 169 \equiv 10 \pmod{53}$

$14^{225} \equiv 10 * 13 * 15 * 14 \equiv 5 \pmod{53}$

Euler's Theorem

$\phi(53) = 52$

$14^{225} \equiv 14^{17} \equiv 14^{16} * 14 \equiv 42 * 14 \equiv 5 \pmod{53}$

(b) Fast Power

3969 = 2048 + 1024 + 512 + 256 +128 + 1

All the powers below are done mod 101

$14^1 \equiv 14,\ 14^2 \equiv 95,\ 14^4 \equiv 36,\ 14^8 \equiv 84,\ 14^{16} \equiv 87,\ 14^{32} \equiv 95,\ 14^{64} \equiv 36, 14^{128} \equiv 84,\ 14^{256} \equiv 87$

$14^{512} \equiv 95,\ 14^{1024} \equiv 36,\ 14^{2048} \equiv 84$

$14^{3969} \equiv 84 * 36 * 95 * 87 * 84 * 14 \equiv 65 \pmod{101}$

Euler's Theorem

$\phi(101) = 100$

$14^{3969} \equiv 14^{69} \equiv 14^{64} * 14^4 * 14 \equiv 36 * 36 * 14 \equiv 65 \pmod{101}$

(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.

(a) $A \equiv g^a \pmod{p} \equiv 3^3 \pmod{31} \equiv 27 \pmod{31}$

(b) $B \equiv g^b \pmod{p} \equiv 3^7 \pmod{31} \equiv 17 \pmod{31}$

(c) Shared key: $B^a \equiv A^b \equiv 17^3 \equiv 4913 \equiv 15 \pmod{31}$

(d) H = 8, E = 5, L = 12, P = 16, M = 13, E = 5

We use $c = 15m \pmod{31}$ to encode the message (letter by letter). We get:
27 13 25 23 9 13

(e) First Bob computes the inverse $15^{-1} \bmod 31 = 29$. Then Bob decodes using the formula $m = k^{-1} * c \pmod{p}$ to recover the original message.

$29 * 27 \pmod{31} = 8 = H$, $29 * 13 \pmod{13} = 5 = E$, $29 * 25 \pmod{31} = 12 = L$
$29 * 23 \pmod{31} = 16 = P$, $29 * 9 \pmod{31} = 13 = M$, $29 * 13 \pmod{13} = 5 = E$

(f) Since $2^5 = 32$, 2 has order 5 mod 31. This is a small order.

(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) $\log_{10} 32 \pmod{53}$

(a) I used the Sage command [x for x in range(0,29) if 3^x % 29 == 19] and got the answer 13.
So $\log_3 19 \pmod{29} = 13$
(b) I used the Sage command [x for x in range(0,53) if 10^x % 53 == 32] and got no solutions (the reason is that 10 is not a primitive root mod 53).

(6) Compute the order of 16 in U(199)

Divisors of 198 = {1,2,3,6,9,11,18,22,33,66,99,198}

For each divisor i, compute $16^i \bmod 199$. The smallest power that gives an answer of 1 is $16^{99} \equiv 1 \pmod{199}$. Hence the order of 16 is 99 in U(199).

(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.

(a) First of all, there are 119 characters (not counting spaces and punctuation). To make it even I repeated the final y. We get the following encoding of the message two letters at a time..

```
2008 519 501 1805 2008 520 913 519 2008 120 2018 2513 514 1919 1521 1219 2008
519 2113 1305 1819 1512 409 518 114 420 805 1921 1419 809 1405 1601 2018 915
2023 912 1209 1420 809 1903 1809 1909 1919 818 914 1106 1815 1320 805 1905
1822 903 515 620 805 918 315 2114 2018
```

The coded message using the function $f(x) = x^{71} \pmod{2879}$ is

```
1232 2773 2850 1495 1232 2768 708 2773 1232 1687 1267 1611 1096 1703 2102 482
1232 2773 2423 2012 2443 2378 2242 2321 2567 1995 123 1891 479 1452 167 1161
1267 79 1347 559 853 1843 1452 2843 2512 1633 1703 548 499 2639 1849 922 123
205 2402 2236 749 938 123 556 2455 132 1267
```

(b) Note $\phi(2879) = 2878$. First we find the inverse $d = 71^{-1} \equiv 1135 \pmod{2878}$. When we decode the message we get

```
2008 519 501 1805 2008 520 913 519 2008 120 2018 2513 514 1919 1521 1219 2008
519 2113 1305 1819 1512 409 518 114 420 805 1921 1419 809 1405 1601 2018 915
2023 912 1209 1420 809 1903 1809 1909 1919 818 914 1106 1815 1320 805 1905
1822 903 515 620 805 918 315 2114 2018
```

Which is the same as the original message (taken two letters at a time).

Note: I did this all in Sage (including putting the decoded message back into characters) as follows.

```
L = list('thesearethetimes...')

M = [ord(i)- ord('a') + 1 for i in L]

A = [ M[2*i]*100 + M[2*i+1] for i in range(0, len(M)/2)]

B = [i^71 % 2879 for i in A]

C = [i^1135 % 2879 for i in B]

D = [(i//100, i % 100) for i in C]

E = flatten(D)

F = [chr(i + ord('a') - 1) for i in E]

print F
```

```
The output is: ['t', 'h', 'e', 's', 'e', 'a', 'r', 'e', 't', 'h', 'e', 't',
'i', 'm', 'e', 's',…
```

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

$x \equiv 34 \pmod{43},\ x \equiv 2 \pmod{97},\ x \equiv 20 \pmod{29}$

$x \equiv 34 \pmod{43} \Rightarrow x = 34 + 43y$

$34 + 43y \equiv 2 \pmod{97}$

$43y \equiv -32 \equiv 65 \pmod{97}$

$43^{-1} \equiv 88 \pmod{97}$

$88 * 43y \equiv 88 * 65 \equiv 94 \pmod{97}$

$y \equiv 94 \pmod{97}$

$x = 34 + 43 * 94 = 4076$

General solution to first two equations

$x \equiv 4076 \pmod{43 * 97} \equiv 4076 \pmod{4171} \Rightarrow x = 4076 + 4171z$

$4076 + 4171z \equiv 20 \pmod{29}$

$4171z \equiv -4056 \equiv 4 \pmod{29}$

$4171^{-1} \equiv 23 \pmod{29}$

$23 * 4171z \equiv 23 * 4 \equiv 92 \equiv 5 \pmod{29}$

$z \equiv 5 \pmod{29}$

$x = 4076 + 4171 * 5 = 24931$

General Solution to all equations

$x = 24931 \pmod{43 * 97 * 29} \equiv 24931 \pmod{120959}$

$x = 24931 + 120959k$

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

$96 = 2^5 * 3,\ \phi(96) = 96 * \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 32$

$245 = 5 * 7^2,\ \phi(245) = 245 * \left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 168$

$936 = 2^3 * 3^2 * 13,\ \phi(936) = 936 * \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{13}\right) = 288$