Homework #8, Revisited

Out : November 11, 2:30 pm 1997
Due : November 18, 12:30 pm 1997

IMPORTANT:

We goofed. The copy of Homework 8 we handed out last week contained some highly misleading instructions. Namely, the directions we gave for problems 2 and 3 said to calculate s as the mod m multiplicative inverse of k. In fact, this *should* have directed you to calculate s as the mod $\phi(m)$ multiplicative inverse of k. The accompanying example contained an error as well. This, combined with the fact that we accidentally provided you with tables of mod m inverses (as opposed to mod $\phi(m)$) for problem 1 amount to a rather confusing assignment.

Our solution to this is to re-issue a corrected version of Homework 8 instead of Homework 9 this week. You will thus have an additional week. Note that problems 4 and 5 are not affected, and only one of the actual questions has changed (the modulus for problem 3 is now 571). If you saw through our mistakes and answered the questions accordingly, your answers are still valid. However, it is nevertheless recommended that you carefully read this corrected version to be sure.

For the first three problems, you will consider different exponentiation cyphers corresponding to different moduli. For each, you will consider several different keys. Remember that for a modulus m and key k, the encryption function is

$$f(clear) = clear^k \pmod{m}$$

Remember also that the rule for the decryption function has the form

$$g(cyph) = cyph^s \pmod{m}$$

1. For the following values of *modulus* and *key*, give the decrypting exponent s (i.e., the number to which the cyphertext should be raised to get the plaintext). If no such exponent exists, explain why.

   You may find the following tables of modular inverses useful. We write the multiplicative inverse of a number x as x^{-1}.

x	$x^{-1} \bmod 16$
0	–
1	1
2	–
3	11
4	–
5	13
6	–
7	7
8	–
9	9
10	–
11	3
12	–
13	5
14	–
15	15

x	$x^{-1} \bmod 18$
0	–
1	1
2	–
3	–
4	–
5	11
6	–
7	13
8	–
9	–
10	–
11	5
12	–
13	7
14	–
15	–
16	–
17	17

x	$x^{-1} \bmod 22$
0	–
1	1
2	–
3	15
4	–
5	9
6	–
7	19
8	–
9	5
10	–
11	–
12	–
13	17
14	–
15	3
16	–
17	13
18	–
19	7
20	–
21	21

(a) $key = 5$ and $modulus = 17$

(b) $key = 15$ and $modulus = 17$

(c) $key = 2$ and $modulus = 19$

(d) $key = 12$ and $modulus = 19$

(e) $key = 0$ and $modulus = 23$

(f) $key = 13$ and $modulus = 23$

In the next two problems, you will use Euclid's algorithm to find the value of s (the mod $\phi(m)$ multiplicative inverse of k).

For part A, *determine the value of s using the provided EuclidCards^{TM}. Please cut out and tape together the cards as appropriate and staple the resulting records of your Euclid-algorithm calculations to the rest of your homework. If the given key k does not have a mod $\phi(m)$ multiplicative inverse, you should say so, and tell us a number bigger than 1 that divides both k and $\phi(m)$.*

For part B, *if you successfully found an s in part A, demonstrate by algebra and arithmetic and Euler's Theorem that the decryption function you found does indeed reverse the action of the encryption function.*

Example: Modulus $m = 1091$, key $k = 533$

Part a:

See attached figure.

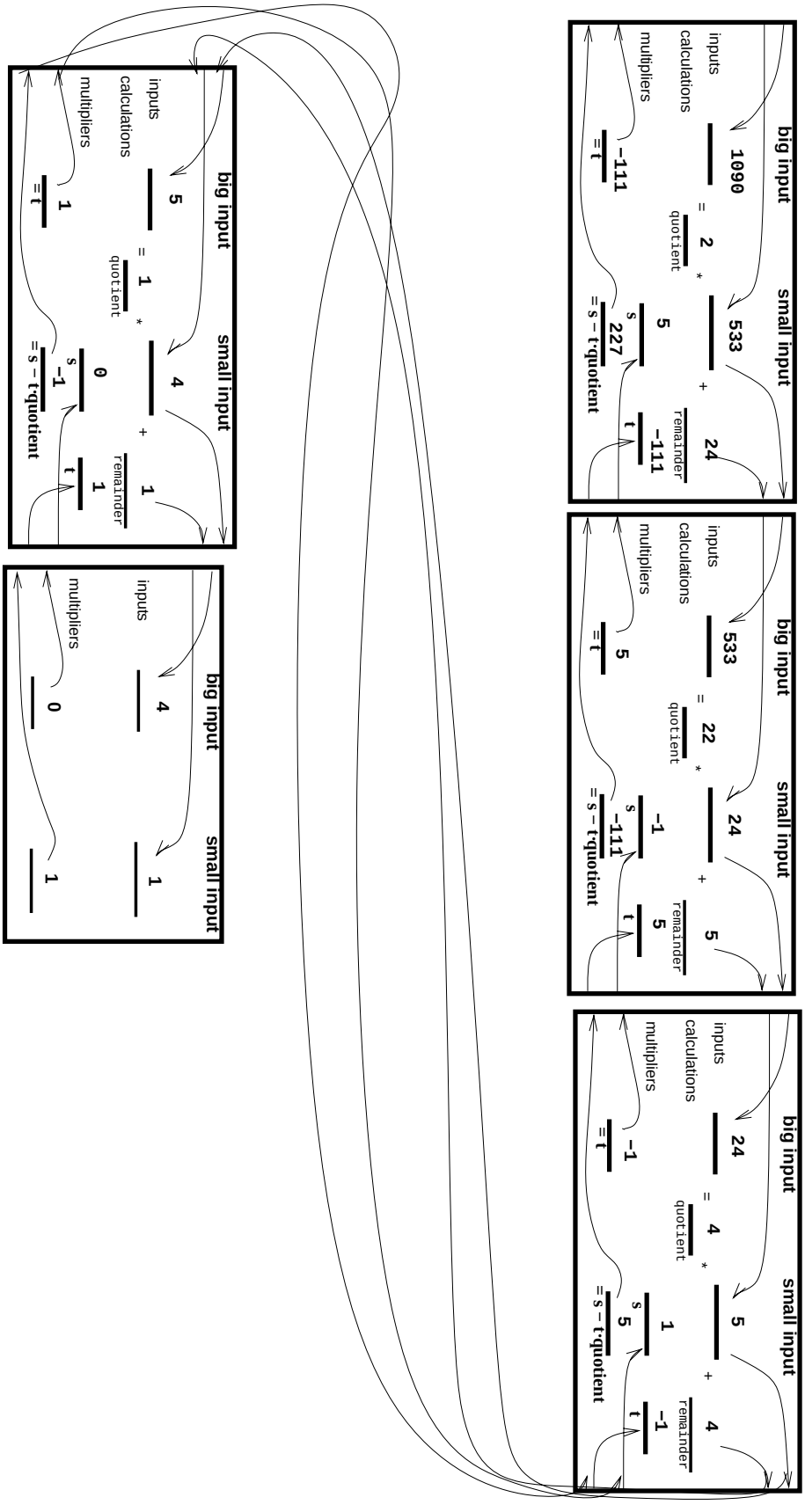
Part b:

Let c denote the cleartext.

$$\begin{aligned} (c^{533})^{227} &= c^{120991} \\ &= c^{1090 \cdot 111 + 1} \\ &= (c^{1090})^{111} c^1 \\ &\equiv (1)^{111} c^1 \pmod{1091} \\ &= c \end{aligned}$$

2. For the next few problems, the modulus is $m = 503$, a prime.
   (a) key is $k = 37$
   (b) key is $k = 241$
   (c) key is $k = 24$
3. For the next few problems, the modulus is $m = 571$, also a prime.
   (a) key is $k = 133$
   (b) key is $k = 77$
4. (a) Give a good (over)estimate of the number of EuclidCards^{TM} needed when the big input is a 60-digit number.
   (b) What if the small input is a 25 digit number?
5. Simplify the following expression:

$$10^{(\log_{10}(10^{(\log_{10} 10)}))}$$


big input
small input
inputs
calculations
multipliers
1090
533
2
quotient
*
+
24
remainder
−111
5
227
s
= s − t·quotient
−111
t
= t
big input
small input
inputs
calculations
multipliers
533
24
22
quotient
*
+
5
remainder
5
−1
−111
s
= s − t·quotient
5
t
= t
big input
small input
inputs
calculations
multipliers
24
5
4
quotient
*
+
4
remainder
1
5
s
= s − t·quotient
−1
−1
t
= t
big input
small input
inputs
calculations
multipliers
5
4
1
quotient
*
+
1
remainder
1
0
s
= s − t·quotient
−1
1
t
= t
big input
small input
inputs
multipliers
4
0
1
1