Homework 9, solutions

Solution to Problem 7. We have $m = 2623$ and $e = 11$. This is the public key. For part b) we will need also the private key, so we start by finding it. This is quivalent to factoring m. We may try the method discussed in class: add small squres to m and check if you get a sqaure. We quickly find that $2623 + 9^2 = 52^2$. Thus

$$2623 = 52^2 - 9^2 = (52 - 9)(52 + 9) = 43 \cdot 61.$$

It follows that $\phi(2623) = 42 \cdot 60 = 2520$. Now, using the Euclidean Algorithm we find d such that $11d \equiv 1(\mod 2520)$. We get $d = 2291$. Thus $d = 2291$, $m = 2623$ is the secret key.

Before we proceed let us explain one more technical issue. We will need to compute $a^b(\mod m)$ for rather large numbers a, b. To do it using just a calculator we use the method of succesive squares. We illustarte it by finding $284^{2291}(\mod 2623)$. We write 2291 in the binary system:

$$2291 = 2^{11} + 2^7 + 2^6 + 2^5 + 2^4 + 2 + 1.$$

This implies that for any a we have

$$a^{2291} = a \cdot a^2 \cdot a^{16} \cdot a^{32} \cdot a^{32} \cdot a^{64} \cdot a^{128} \cdot a^{2048}.$$

We find the factors on the right side modulo 2623 by succesive squaring. We start with $a = 284$. Thus

$$a^2 \equiv 284^2 \equiv 1966(\mod 2623)$$

$$a^4 \equiv 1966^2 \equiv 1477(\mod 2623)$$

$$a^8 \equiv 1477^2 \equiv 1816(\mod 2623)$$

$$a^{16} \equiv 1816^2 \equiv 745(\mod 2623)$$

$$a^{32} \equiv 745^2 \equiv 1572(\mod 2623)$$

$$a^{64} \equiv 1572^2 \equiv 318(\mod 2623)$$

$$a^{128} \equiv 318^2 \equiv 1450(\mod 2623)$$

$$a^{256} \equiv 1450^2 \equiv 1477(\mod 2623)$$

$$a^{512} \equiv 1477^2 \equiv 1816(\mod 2623)$$

$$a^{1024} \equiv 1816^2 \equiv 745(\mod 2623)$$

$$a^{2048} \equiv 745^2 \equiv 1572(\mod 2623)$$

Now $284 \cdot 1966 \equiv 2268(\mod 2623)$, $1966 \cdot 745 \equiv 448(\mod 2623)$,
$448 \cdot 1572 \equiv 1292(\mod 2623)$, $1292 \cdot 318 \equiv 1668(\mod 2623)$,
$1668 \cdot 1450 \equiv 194(\mod 2623)$, $194 \cdot 1572 \equiv 700(\mod 2623)$.
Thus $284^{2291} \equiv 700(\mod 2623)$.

a) We format the text: PA TI EN CE IS AV IR TU AX and change it into numbers

$$1500\ 1908\ 0413\ 0204\ 0818\ 0021\ 0817\ 1920\ 0023.$$

Now, using the method of succesive squares with $e = 11 = 8 + 2 + 1$, we find $b^e(\mod 2623)$ for every block b.

$$1500^{11} \equiv 2546(\mod 2623)$$

$$1908^{11} \equiv 2068(\mod 2623)$$

$$413^{11} \equiv 1782(\mod 2623)$$

$$204^{11} \equiv 581(\mod 2623)$$

$$818^{11} \equiv 2151(\mod 2623)$$

$$21^{11} \equiv 2228(\mod 2623)$$

$$817^{11} \equiv 1806(\mod 2623)$$

$$1920^{11} \equiv 528(\mod 2623)$$

$$23^{11} \equiv 1014(\mod 2623)$$

Thus the encoded meassage is 2546 2068 1782 581 2151 2228 1806 528 1014.

b) We need to compute $b^{2291}(\mod 2623)$ for every block b of the encoded message. We have already done it for the first block 284 above in the example. We use the same method for other blocks and get the decoded meassage:

$$700\ 1819\ 412\ 10\ 418\ 2200\ 1819\ 423$$

which translates into letters as follows: HA ST EM AK ES WA ST EX. Thus the massage is HASTE MAKES WASTE.

Solution to Problem 8. The method is the same as for problem 7. We find that $2419 = 50^2 - 9^2 = 41 \cdot 59$, $\phi(2419) = 2320$, $d = 357 = 256 + 64 + 32 + 4 + 1$.

a) Our message is PL EA SE RE PL YS OO NX whih is

$$1511\ 0400\ 1804\ 1704\ 1511\ 2418\ 1414\ 1323.$$

After encoding we get 1124 558 1517 1589 1124 2418 1307 253.

b) Decoded message is 214 1306 1700 1920 1100 1908 1413 1823, which translates into letters as CO NG RA TU LA TI ON SX. The massage is CONGRATULATIONS.

Solution to Problem 12. Let us first explain what the problem asks. We are given odd primes $p < q$ and $1 \leq e < \phi(pq)$. The number d' is such that $ed' \equiv 1(\mod [p-1, q-1])$. We are asked to show that $a^{ed'} \equiv a(\mod pq)$ for every integer a. This is the same as to prove that $a^{ed'} \equiv a(\mod p)$ and $a^{ed'} \equiv a(\mod q)$. We will just justify the first congruence, the second is proved the same way. Note that our assumption yields $p-1|ed'-1$ (since $p-1|[p-1, q-1]$). Thus, if $p \nmid a$, then $a^{ed'-1} \equiv 1(\mod p)$ by Fermat's Little Theorem. Multiplying both sides by a we get $a^{ed'} \equiv a(\mod p)$. If $p|a$, the last congruence is clear. This proves the result.

Remark. This result simplifies the computations of d since the number $[p-1, q-1]$ is usually smaller than $\phi(pq)$, so inverting e modulo $[p-1, q-1]$ is simpler than modulo $\phi(pq)$.

Solution to Problem 14a). Suppose that $3^{(F_n-1)/2} \equiv -1(\mod F_n)$. Then $3^{F_n-1} \equiv 1(\mod F_n)$. This means that the order of 3 modulo F_n difides $F_n - 1 = 2^{2^n}$, but it does not divide $(F_n - 1)/2 = 2^{2^n-1}$. It follows that the order of 3 modulo F_n is equal to $F_n - 1$. As the order must divide $\phi(F_n)$, we get

$$F_n - 1 \leq \phi(F_n) < F_n.$$

This implies that $\phi(F_n) = F_n - 1$. It is easy to see that $\phi(n) = n - 1$ if and only if n is a prime number. Thus F_n is prime.