WRITTEN HW #6 SOLUTIONS

(1) (10 points) Show that $\phi(n) = 26$ has no solutions.

Solution. Case 1: n is prime. This clearly doesn't work, since $\phi(p) = p - 1$, and 27 is not prime.
Case 2: $n = pq$, where $p \neq q$ are prime. Then $phi(n) = (p-1)(q-1)$, which does not work since $26 = 2 \cdot 13$, and this cannot be expressed as $(p-1)(q-1)$.
Case 3: $n = p^2$, so $\phi(n) = p(p-1)$. This clearly doesn't work.
Case 4: $n = 4p$, so $\phi(n) = 2(p-1)$. Since 14 is not prime, this doesn't work.
26 has only 2 nontrivial factors, so if $\phi(n) = 26$, n has at most three factors (if 2 is one of them; if not, it can only have two factors). If $\phi(2n) = 26$ for n odd, $\phi(n) = 26$ as well, so we can deal only with the odd cases or with multiples of 4. We have covered those cases above, showing that 26 is not in the image of ϕ. □

(2) (10 points) Suppose Julius Caesar decides to encode his messages by using a linear transformation $x \bmod 26 \mapsto ax+b \bmod 26$ instead of just the linear shift $x \bmod 26 \mapsto x + b \bmod 26$, where a, b are integers. What conditions (if any) must a, b satisfy to ensure that distinct encrypted messages are decrypted to distinct unencrypted messages? For these a, b, what is the decrypting transformation? Your answer will be in terms of a, b. (For instance, in the case where $x \bmod 26 \mapsto x + b \bmod 26$ is the encrypting transformation, the decrypting transformation is $x \bmod 26 \mapsto x - b \bmod 26$.)

Solution. For $x \mod 26 \mapsto ax + b \mod 26$ to be one-to-one (a necessary condition for the message to be decryptable), we need a to be invertible mod 26, i.e. $\gcd(a, 26) = 1$. It is not hard to see that if this does not hold, that $x \bmod 26 \mapsto ax \mod 26$ maps multiple letters to the same one, and the shift induced by b does nothing to fix this. There are no restrictions on b.

To invert this map for decryption, we use the map $x \mod 26 \mapsto a^{-1}x - a^{-1}b \mod 26$; plugging in the original formula shows this is indeed an inverse function. □

(3) (10 points) The message at the end of the assignment was encrypted using a Caesar cipher of form described in the problem above: that is, of the form $x \bmod 26 \mapsto ax+b \bmod 26$ for suitably chosen a, b. Decrypt the message, and explain how you did it. You do not need to rewrite the original message (it is rather long), but you should be able to identify its source.

Solution. We will decrypt this using frequency analysis. The single "h" in the text is likely an "a", since it is not capitalized. "hqq" is likely "all". "Fm fj" is likely "it is". By doing these sorts of tricks and plugging in the letters

we've figured out, we can piece together than this is the Gettysburg Address. □

(4) (10 points) For this problem, you can use a computer to do basic computations for you, including calculating powers mod N and computing the multiplicative inverse of a number mod N. However, you should still write out your work and explain when you had a computer do calculations for you.

- (5 points) Suppose you want to be able to decrypt messages sent to you via the RSA cryptosystem. You choose $p = 20857, q = 29453$, and compute $N = 614301221$. You also choose $e = 23$ as your encryption exponent. Someone sends you the message 485195366. Decrypt the message.
- (5 points) Now suppose Alice has published the RSA public key $(N, e) = (735047, 41)$, and you intercept the message 184520. Decrypt the message. (If your factor/divisor program from the last programming assignment works, this is a good place to use it!) Would you have been able to decrypt the message if N had been 50 digits long, instead of 6 digits long?

Solution. We have that $p = 20857, q = 29453, N = 614301221, e = 23$. Calculating $\phi(N) = (p-1)(q-1) = 614250912$, we find that $d = e^{-1} \mod \phi(N) = 133532807$. Taking $M = 485195366$, we take $M^d \mod N$ and find that the message is 314.

For the second part, we start by factoring $N = 735047 = 757 \cdot 971$. We find $\phi(N) = 733320$. Since our given exponent is $e = 41$, we find $d = e^{-1} \mod \phi(N) = 125201$. Finally, we raise our message $M = 184520$ to the dth power, take it mod N, and extract the original message 2718.

If N were 50 digits rather than 6, performing the first step of factoring N would have taken an enormous amount of time, making this problem much harder to solve (at least, in a reasonable amount of time). □

(5) (10 points) Let $N = pq$ be the product of two distinct odd primes, and let $a \equiv 1 \mod \phi(N)$, where a is a positive integer. Show that $x^a \equiv x \mod N$, regardless of whether $\gcd(x, N) = 1$ or not. (This shows that when encoding and decoding a message x using the RSA cryptosystem, we don't need to worry about whether x is relatively prime to any particular number or not. Contrast this to the fact that we do need to worry about whether e is relatively prime to $\phi(N)$.)

Solution. We have several cases here. If $\gcd(x, N) = 1$, then by Fermat-Euler $x^a \equiv x \mod N$. If $\gcd(x, N) = N$, then both sides of the congruence are 0 mod N, so the congruence again holds. The tricky case is when $\gcd(x, N) = p$ (or q, but the problem is symmetric – if we can show the congruence holds for p, it will also hold for q).

We will assume that $x = kp^e$, where $\gcd(k, p) = 1$, and that $a = 1 + f\phi(N) = 1 + f(p-1)(q-1)$.

Consider $x^a \mod p$. Since $p \mid x$, both $x^a, x \equiv 0 \mod p$ so the congruence holds in this case.

Now consider $x^a \mod q$:

$$x^a = x \cdot x^{f\phi(n)} = x \cdot (x^{f(p-1)})^{q-1} \equiv x \cdot 1 \mod q,$$

by Fermat's Little Theorem (since $\gcd(x, N) = p, q \nmid x$). Hence the congruence $x^a \equiv x \mod q$ holds. By the Chinese Remainder Theorem, since $x^a \equiv x \mod p, \mod q$, the congruence also holds mod pq.

While it doesn't matter whether the message we send is relatively prime to our modulus N in RSA, it does matter whether our exponent e is relatively prime to $\phi(N)$ because we need the inverse of e to decrypt the message, which only exists as long as $\gcd(e, \phi(N)) = 1$. □

(6) (10 points) In contrast to the above problem, show that if N is an arbitrary integer, and $a \equiv 1 \mod \phi(N)$, it might not be the case that $x^a \equiv x \mod N$, for some choice of x. (Probably the easiest way to do this problem is to actually write down N, a, x, such that $a \equiv 1 \mod \phi(N)$ but $x^a \not\equiv x \mod N$.

Solution. If we let $N = 12$, so $\phi(N) = 4$, we can allow $a = 5 \equiv 1 \mod 4$, and let $x = 2$. In this case, $2^5 = 32 \equiv 8 \mod 12$, showing that the Fermat-Euler theorem does require $\gcd(x, N) = 1$ for it to always be true. □

Message for problem #2: "Wxpg jnxgt huq jtstu bthgj hzx xpg whmctgj kgxpzcm wxgmc xu mcfj nxumfutum h utv uhmfxu, nxuntfstq fu ofktgmb, huq qtqfnhmtq mxmct agxaxjfmfxu mchm hoo rtu hgt ngthmtq tdpho. Uxv vt hgt tuzhztq fu h zgthm nfsfo vhg, mtjmfuz vctmctg mchm uhmfxu, xg hub uhmfxu, jx nxuntfstq huq jx qtqfnhmtq, nhu oxuz tuqpgt. Vt hgt rtm xu h zgthm khmmot-wftoq xw mchm vhg. Vt chst nxrt mx qtqfnhmt h axgmfxu xw mchm wftoq, hj h wfuho gtjmfuz aohnt wxg mcxjt vcx ctgt zhst mctfg ofstj mchm mchm uhmfxu rfzcm ofst. Fm fj homxztmctg wfmmfuz huq agxatg mchm vt jcxpoq qx mcfj. Kpm, fu h ohgztg jtujt, vt nhu uxm qtqfnhmt, vt nhu uxm nxujtnghmt, vt nhu uxm chooxv mcfj zgxpuq. Mct kghst rtu, ofsfuz huq qthq, vcx jmgpzzotq ctgt, chst nxujtnghmtq fm, whg hkxst xpg axxg axvtg mx hqq xg qtmghnm. Mct vxgoq vfoo ofmmot uxmt, uxg oxuz gtrtrktg vchm vt jhb ctgt, kpm fm nhuutstg wxgztm vchm mctb qfq ctgt. Fm fj wxg pj mct ofsfuz, ghmctg, mx kt qtqfnhmtq ctgt mx mct puwfufjctq vxgl vcfnc mctb vcx wxpzcm ctgt chst mcpj whg jx uxkob hqshuntq. Fm fj ghmctg wxg pj mx kt ctgt qtqfnhmtq mx mct zgthm mhjl gtrhfufuz ktwxgt pj-mchm wgxr mctjt cxuxgtq qthq vt mhlt fungthjtq qtsxmfxu mx mchm nhpjt wxg vcfnc mctb zhst mct ohjm wpoo rthjpgt xw qtsxmfxu-mchm vt ctgt cfzcob gtjxost mchm mctjt qthq jchoo uxm chst qftq fu shfu-mchm mcfj uhmfxu, puqtg Zxq, jchoo chst h utv kfgmc xw wgttqxr-huq mchm zxstgurtum xw mct atxaot, kb mct atxaot, wxg mct atxaot, jchoo uxm atgfjc wgxr mct thgmc."