WRITTEN HW #6, DUE NOV 7 2011

Remember to write clearly and to justify all your claims in your solutions. Please staple your assignment before turning it in.

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

(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 $x \bmod 26 \mapsto x - b \bmod 26$.)

(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.

(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?

(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 $\phi(N)$.)

(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 $x^a \not\equiv x \mod N$.

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."