M 343 L 56115 Midterm

name:
ssn:
signature:

1. A user generates an RSA public key (n, e) but, due to a software fault, his modulus n is of the form $n = pq$ where p is prime but q is not prime. Not realising the error, he publishes his key.

(a) Show that if q is a Carmichael number then any messages relatively prime to n that this user receives will decrypt correctly.

(b) Give a small numerical example of this situation (that is, q is neither prime nor a Carmichael number) in which some messages relatively prime to n will not decrypt correctly.

Part (a) needs the additional hypothesis that $(p, q) = 1$. Under this hypothesis, the solution is as follows:

Since p is prime, we have $m^{p-1} \equiv 1 (\bmod p)$ if $(m, p) = 1$, by Fermat's little theorem. Since q is a Carmichael number, we have $m^{q-1} \equiv 1 (\bmod q)$ if $(m, q) = 1$, by definition. If d is such that $ed \equiv 1 (\bmod (p-1)(q-1))$, then $ed - 1 = k(p-1)(q-1)$ for some k. Suppose the user receives an encyphered message $c \equiv m^e (\bmod n)$, with $(m, n) = 1$. He computes

$$c^d \equiv m^{ed} \equiv m^{ed-1} m \equiv m^{k(p-1)(q-1)} m (\bmod n).$$

Now, $m^{k(p-1)(q-1)} = (m^{(p-1)})^{k(q-1)} \equiv 1 (\bmod p)$ and $m^{k(p-1)(q-1)} = (m^{(q-1)})^{k(p-1)} \equiv 1 (\bmod q)$ by the congruences above. Under the assumption that $(p, q) = 1$, we can conclude that $m^{k(p-1)(q-1)} \equiv 1 (\bmod n)$ and so $c^d \equiv m (\bmod n)$ as was to be shown.

For part (b) almost anything will work. An example is $p = 5, q = 21$ so $n = 105, (p-1)(q-1) = 80$ and we take $e = 3$. We have then that $d = 27$ so that $ed \equiv 1 (\bmod 80)$. The messge $m = 2$ encrypts as $2^3 = 8$ and 8 supposedly decrypts as $8^27 \equiv 92 (\bmod 105)$ which is not m. In fact, the only messages that will decrypt correctly are $1, 8, 13, 22, 29, 34, 41, 43, 62, 64, 71, 76, 83, 92, 97, 104$ out of a total of 48 possible $m, 1 \leq m \leq 105, (m, 105) = 1$.

2. Find all solutions $x, 1 \leq x \leq 54$ to the congruence $x^2 \equiv 1 (\bmod 55)$.

$x = 1, 21, 34, 54$

3. You are an attacker trying to decrypt a message encrypted as c using RSA with public key (n, e) (where n is the modulus and e is the encryption exponent). You notice that $c^{100} \equiv 1 (\bmod n)$. Show that, if the original message is m, then we must have $m^{100} \equiv 1 (\bmod n)$ also. Explain how to use this information to find m, if e and 100 have no common factors.

We know that there exists a decryption exponent d and that $m \equiv c^d (\bmod n)$. Therefore $m^{100} \equiv c^{100d} \equiv 1 (\bmod n)$.

If e and 100 have no common factors, there exists δ satisfying $e\delta \equiv 1 (\bmod 100)$. Then, $c^\delta \equiv m^{e\delta} \equiv m^{e\delta - 1} m (\bmod n)$. Since $e\delta \equiv 1 (\bmod 100)$ and $m^{100} \equiv 1 (\bmod n)$ we must have $m^{e\delta - 1} \equiv 1 (\bmod n)$ which then gives $c^\delta \equiv m (\bmod n)$, which decrypts the message.