**M 343 L 55540 Midterm**

name:
ssn:
signature:

Do three out of the four questions below and please indicate here which questions you chose:

1. Suppose Alice, Bill and Bob are communicating using the RSA cryptosystem. Suppose that Bill and Bob have public keys $(e_1, n)$ and $(e_2, n)$ respectively, with the same modulus $n$, and assume further that $e_2 = e_1 + 1$. Show that, if Alice sends both Bill and Bob the same message, an eavesdropper who obtains both encryptions can decipher the message without factoring $n$. What happens if $e_2 = 2e_1 + 1$ instead? Generalize.

If $m$ is the message, then Alice sends $m^{e_1} (\bmod n)$ to Bill and $m^{e_2} \equiv m^{e_1+1} \equiv m^{e_1} m (\bmod n)$ to Bob. An eavesdropper intercepting both communications obtains $m$ as $m^{e_2}(m^{e_1})^{-1} (\bmod n)$ unless $m^{e_1}$ is not invertible $\bmod n$, but the latter doesn't happen since this would imply that $m, n$ are not coprime, which is avoided in RSA since it allows an eavesdropper to factor $n$.

If $e_2 = 2e_1 + 1$, in the same way the eavesdropper gets $m$ as $m^{e_2}(m^{e_1})^{-2} (\bmod n)$. In general, if $e_1, e_2$ are coprime then there exists $u, v$ with $ue_1 + ve_2 = 1$ so $m$ can be recovered as $(m^{e_2})^v (m^{e_1})^u (\bmod n)$.

2. Estimate the probability that a hundred digit number $p$ is such that $p$ and $p+2$ are both prime and $p \equiv 1 \bmod 1234$.

The probability of a hundred digit number being prime is $1/(\log 10^1 00) = 1/230$ approximately. The probability of a **prime number** being $\equiv 1 \bmod 1234$ is $1/\phi(1234) = 1/616$ by the theorem on primes in arithmetic progressions (recall that if $p$ is prime then $(p, 1234) = 1$ except for $p = 2, 617$ of course). If these probabilities are independent, the answer to the question is $1/230^2$ times $1/616$ which is $3 \times 10^{-8}$ approximately. (in fact, these probabilities are not quite independent and the true answer is more like $4 \times 10^{-8}$).

3. Compute $\phi(p^2)$ where $p$ is prime. Show that $p^2$ is a pseudoprime to base $b$ if and only if $b^{p-1} \equiv 1 (\bmod p^2)$. Show that in this case $p^2$ is also a strong pseudoprime to base $b$.

$\phi(p^2) = p(p-1)$ because the numbers between 1 and $p^2$ coprime to $p^2$ are those numbers not divisible by $p$. Since there are $p$ numbers divisible by $p$ between 1 and $p^2$ we are left with $p^2 - p = p(p-1)$ numbers.

By definition $p^2$ is a pseudoprime to base $b$ if and only if $b^{p^2-1} \equiv 1 (\bmod p^2)$. On the other hand, by Euler's theorem $b^{p^2-p} \equiv 1 (\bmod p^2)$ for all $b$ with $(b, p^2) = 1$. So $p^2$ is a pseudoprime to base $b$ if and only if $1 \equiv b^{p^2-1} \equiv b^{p^2-1}(b^{p^2-p})^{-1} \equiv b^{p-1} (\bmod p^2)$.

Let $p^2 - 1 = 2^r m$, $m$ odd and let $j$ be the smallest integer with $b^{2^j m} \equiv 1 (\bmod p^2)$. If $j = 0$ then $p^2$ is a strong pseudoprime to base $b$ by definition. If $j > 0$ then $c = b^{2^{j-1} m}$ satisfies $c^2 \equiv 1 (\bmod p^2)$, so $p^2$ divides $(c-1)(c+1)$. If $p$ divides both $(c-1)$ and $(c+1)$ then $p$ divides $(c+1) - (c-1) = 2$, so $p = 2$ and the result is clear in this case. For $p > 2$ we must then have $p^2$ divides $(c-1)$ or $(c+1)$ and that implies that $p^2$ is a strong pseudoprime to base $b$.

4. Suppose a RSA public key pair $(e, n)$, where $e$ is the exponent and $n$ is the modulus is such that $e^r \equiv 1 (\bmod \phi(n))$ for some $r$. Show that reencrypting a message $r$ times will return the original message. Discuss how much of a security threat this can be. Find a lower bound for $r$ if $e = 3$. For which primes is this lower bound attained?

The encryption of a message $m$ is $m^e \bmod n$, and repeating the encryption we get $(m^e)^e = m^{e^2} \bmod n$. Likewise, reencrypting a message $r$ times will return $m^{e^r} \bmod n$. If $e^r \equiv 1 (\bmod \phi(n))$ then, by Euler's theorem $m^{e^r} \equiv m m^{e^r - 1} \equiv m (\bmod n)$, as desired.

This will be a security threat if the eavesdropper suspects that $e^r \equiv 1 (\bmod \phi(n))$ for a small $r$, in which case the eavesdropper will reencrypt the cyphertext a few times looking for something that resembles a message.

If $3^r \equiv 1 (\bmod \phi(n))$ then $3^r - 1$ is at least $\phi(n)$ so $r > \log_3(\phi(n) + 1)$. It seems like a tricky problem to determine which primes $p, q$ are such that $3^r - 1 = (p-1)(q-1)$. Enjoy.