

MATH 470 Homework 7

- [1] Use the index calculus approach to compute the discrete logarithm $L_7(29) \pmod{41}$, that is, the solution x of $29 \equiv 7^x \pmod{41}$. Note that the factor base of $p - 1 = 40$ can be taken to consist of only three elements.

The factors of $p - 1 = 40$ are just 2, 5 so we can use the factor base of 2, 3, 5. We compute successive powers of 7 $\pmod{41}$ and retain only those that contain 2, 3, 5 in the answer. From the the first 10 exponents: $7^2 \equiv 8 \equiv 2^3$, $7^3 \equiv 15 \equiv 3 \cdot 5$, $7^6 \equiv 20 \equiv 2^2 \cdot 5$, $7^{10} \equiv 9 \equiv 3^2 \cdot 5$ all $\pmod{41}$. This is sufficient to solve for the various values and means that we have $2 \equiv 3L(2)$, $3 \equiv L(3) + L(5)$, $6 \equiv 2L(2) + L(5)$, $10 \equiv 2L(3)$. On the other hand, if we run a few more exponents we get $7^{14} \equiv 2$, $7^{18} \equiv 5$, $7^{25} \equiv 3$. Thus either way, we get $L(2) \equiv 14$, $L(3) \equiv 25$, $L(5) \equiv 18$ all $\pmod{p - 1}$ and this finishes the precomputation.

We now have to choose exponents k such that $29 \cdot 7^k$ contains only factors of 2, 3, 5 when taken \pmod{p} . We just try low values of k and are rewarded by $29 \cdot 7^3 \equiv 25 \equiv 5^2 \pmod{p}$ so that $L(29) \equiv -3 + 2L(5) \equiv 33$. Thus $x = 33$.

- [2] Alice is about to send a message to Bill who is using an ElGamal cipher with published values $p = 123457$, $\beta = 94622$, $\alpha = 5$ when she notices her random number generator (to obtain k to compute the pair (r, t)) returns an unusually small value. "Must be okay", she says, and transmits $(125, 118586)$ to Bill. Eve is reading the traffic from Alice to Bill and also notices the unusually small value of r . What might Eve try to do about this - and if it works, what is Alice's message?

It seems obvious that a likely choice of k is $k = 3$ since $\alpha^k \equiv 125$ and α is a primitive root \pmod{p} . But if we know k then the codetext is just about broken; we know from the El Gamal implementation that $t \equiv \beta^k m \pmod{p}$ so that $m \equiv t\beta^{-k} \pmod{p}$. The message can then be read directly. Here we have to compute $118586 \cdot 94622^{-3} \pmod{p}$ which works out to be $m = 9999$.

- [3] Show that if $\gcd(e, 24) = 1$, then $e^2 \equiv 1 \pmod{24}$.

Show that if $n = 35$ is used as an RSA modulus then the decryption exponent d always equals the encryption exponent e .

If $\gcd(e, 24) = 1$ then e cannot be a multiple of 2 or 3. This leaves $e = 1, 5, 7, 11, 13, 17, 19, 23$. Also $(n - e)^2 \equiv n^2 - 2ne + e^2 \equiv e^2 \pmod{n}$, so we need only look at the first four entries (since, for example, $23 = n - 1$ with $n = 24$). But it is easily checked that $1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{24}$.

If $n = 35$ is used then $\phi(n) = 24$ and the condition on the exponent e is that $\gcd(e, \phi(n)) = 1$, or here $\gcd(e, 24) = 1$. d is chosen to be the unique number $ed \equiv 1 \pmod{n}$ and so from the above this means that $d = e$.

- [4] Alice wishes to speed up her RSA decryptions but is aware that a small value of d is insecure, so tries the following; As usual, she chooses a composite $n = pq$ and an exponent e such that $\gcd(e, \phi(n)) = 1$. She computes d in the usual way and then integers d_p and d_q such that $d_p \equiv d \pmod{p - 1}$ and $d_q \equiv d \pmod{q - 1}$. Since $d_p < p$ and $d_q < q$ these exponents are much shorter than d which is typically of length roughly $n = pq$. When she receives a codetext c , instead of computing $m \equiv c^d \pmod{n}$ which can be lengthy, she instead computes $m_p \equiv c^{d_p} \pmod{p}$ and $m_q \equiv c^{d_q} \pmod{q}$. She then uses the Chinese Remainder Theorem to combine these two equivalences into one \pmod{n} .

Show that the result of this computation is the original message m .

Use $n = 2501 = 41 \times 61$ and $e = 583$ to compute the values of d_p , d_q , and d . Then decrypt the codetext $c = 1417$ by both the usual RSA scheme and Alice's method. Do you see an advantage?

Is there a security problem here, that is, if Eve knows what Alice is doing can she exploit this? Of course, in an actual implementation, p and q are many orders of magnitude larger.

We have two congruences $x \equiv m_p \equiv c^{d_p} \equiv c^d \pmod{p}$ and $x \equiv m_q \equiv c^{d_q} \equiv c^d \pmod{q}$. Now there exists integers s, t with $ps + qt = \gcd(p, q) = 1$ by the Euclidean algorithm and so the solution to the pair of congruences is $x \equiv ps m_q + qt m_p \equiv c^d (ps + qt) \equiv c^d \equiv m \pmod{pq}$.

Use $n = 2501 = 41 \times 61$ and $e = 583$ to compute the values of d_p , d_q , and d . Then decrypt the codetext $c = 1417$ by both the usual RSA scheme and Alice's method. Do you see an advantage?

There is a considerable advantage here - in fact this is often the way RSA is implemented.

Is there a security problem here, that is, if Eve knows what Alice is doing can she exploit this? Of course, in an actual implementation, p and q are many orders of magnitude larger.

There is no reason to believe there is a security issue, but this has not been formally proven - it is in fact a well-researched open question!

- [5] Let $n = pq$ be the product of two primes. Suppose k is such $k \equiv 0 \pmod{\phi(n)}$ and a is a randomly chosen integer $1 < a < n - 1$.

Show that $k = 2^t r$ with r odd and $t \geq 1$ and that $a^k \equiv 1 \pmod{n}$.

From the above, it follows that $a^{k/2}$ is a square root of unity \pmod{n} and from the Chinese Remainder Theorem that $x = 1$ has four square roots \pmod{n} . It can be shown that with probability at least $\frac{1}{2}$ that one of the elements of the sequence $a^{k/2}, a^{k/4}, \dots, a^{k/2^t} \pmod{n}$ is a square root of unity different from ± 1 for any randomly chosen a .

Verify this last claim by taking $n = 642401$, $k = 10891968$ and $a = 2, 3, 5, 7, 11, 13$.

We know that $\phi(n) = (p - 1)(q - 1)$ and both these factors are even so that $\phi(n)$ is certainly divisible by 4. Thus if $k \equiv 0 \pmod{\phi(n)}$ then $k = s\phi(n)$ for some integer s and so k must be divisible by 4. Now if we just divide out all factors of 2 in k , we get $k = 2^t r$ with r odd - and we know that t is at least 2. Also, $a^k \equiv a^{s\phi(n)} \equiv (a^s)^{\phi(n)} \equiv 1 \pmod{n}$ by Euler's theorem.

For the second part, there is code available - see `boneh.mw` under the `maple` section of the web page. The utility of this idea is for the next problem.

- [6] Mallory works at a company that uses RSA for all e-mail traffic. The computer manager chooses large, safe primes p and q and forms the composite $n = pq$. Using these, he makes up a set of exponent pairs (e_j, d_j) in the usual way and distributes one pair to each employee and makes sure that no e_j or d_j is small. The common value of n and each user's e_j is made public. Each user is told to keep their decryption exponent d_j secret and no user is given the factorisation of n (in fact, the primes p and q are destroyed after the exponents are calculated). To read an encrypted message each user just computes $c^{d_j} \pmod{n}$ with their private d_j .

Mallory is able intercept messages between other employees. Is there any way he can read these? That is, if an $e - d$ pair is known can one reconstruct the primes p, q that make up the modulus n ?

It turns out that knowing n and an encrypt-decrypt pair e, d is enough information to factor n in a reasonably small amount of time. Thus Mallory can use his own (e, d) pair to do this. Once he has p and q , he has $\phi(n)$ and can compute anyone's d from their public e .

Mallory knows his d and the corresponding public e so he is able to compute the integer $k = ed - 1$. Now $ed \equiv 1 \pmod{\phi(n)}$ so that $k \equiv 0 \pmod{\phi(n)}$. Also, this means (by Euler's theorem) that for any a , $1 \leq a < \phi(n)$, $a^k \equiv 1 \pmod{n}$. So $a^{k/2}$ is a square root of unity \pmod{n} . We know there are four possible square roots \pmod{n} by the Chinese Remainder Theorem (two from each of the congruences $x^2 \equiv 1 \pmod{p}$, $x^2 \equiv 1 \pmod{q}$); two of these four solutions will be the trivial ones $x = \pm 1$, but there will also be two nontrivial ones). Of course, $a^{k/2}$ could just be the trivial solution ± 1 and we haven't gained anything. However, from problem 6 we know that if continue to take square roots (that is, form the sequence $a^{k/2}, a^{k/4}, \dots, a^{k/2^t} \pmod{n}$) then there is at least a probability half chance that we will come up with a nontrivial root. If not, then we change the value for a and repeat knowing that for m random choices our chances of failure are less than 2^{-m} . For each a , all of these computations take of order n^3 steps so this is quite feasible computationally. So, now we have a value x (actually $\pm x$) for a nontrivial root and also ± 1 . Now, $d = \gcd(x - 1, n)$ will reveal the factorisation of n .

[You will remember this last part from the Rabin cipher issue whereby if one could obtain the four solutions (actually, just a right pairing) to the decryption, then one could easily factor n].