

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.
- [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?
- [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 .
- [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.
- [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 $a = 2, 3, 5, 7, 11, 13$.
- [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 ?