MATH 255: ELEMENTARY NUMBER THEORY
HOMEWORK #9

JOHN VOIGHT

8.1: Character Ciphers

Problem 8.1.1. Using the Caesar cipher, encrypt the message ATTACK AT DAWN.

Problem 8.1.6. Decrypt the message RTOLK TOIK, which was encrypted using the affine transformation $C = 3P + 24 \pmod{26}$.

Problem 8.1.8. The message KYVMR CLVFW KYVBV PZJJV MVEKV VE was encrypted using a shift transformation $C \equiv P + k \pmod{26}$. Use frequencies of letters to determine the value of k. What is the plaintext message?

Problem 8.1.10. If the two most common letters in a long ciphertext, encrypted by an affine transformation $C = aP + b \pmod{26}$, are X and Q, respectively, then what are the most likely values for a and b?

8.4: Public Key Cryptography

Problem 8.4.2. Find the primes p and q if $n = pq = 4386607$ and $\phi(n) = 4382136$.

Problem 8.4.3. Suppose a cryptanalyst discovers a message P that is not relatively prime to the encryption modulus $n = pq$ used in an RSA cipher. Show that the cryptanalyst can factor n.

Problem 8.4.4. Show that it is extremely unlikely that a message such as that described in Exercise 8.4.3 can be discovered. Do this by demonstrating that the probability that a message P is not relatively prime to n is $1/p + 1/q - 1/pq$, and if p and q are both larger than 10^{100}, this probability is less than 10^{-99}.

Problem 8.4.6. What is the ciphertext that is produced when RSA encryption with key $(e, n) = (7, 2627)$ is used to encrypt the message LIFE IS A DREAM? *[Hint: Break up the message into blocks.]*

Problem 8.4.13. Suppose that two parties share a common modulus n in the RSA cryptosystem, but have differing encrypting exponents. Show that the plaintext of a message sent to each of these two parties encrypted using each of their RSA keys can be recovered from the ciphertext messages.

Problem 8.4.A. Use the Fermat factorization method to find p, q if $n = pq = 7389187509467$.

Date: Due Wednesday, 1 April 2009.