Dr. A. Betten Fall 2009

MATH 360 Mathematics of Information Security

Assignment # 2

Problem # 5
Compute $\gcd(4883, 4369)$ and express it in the form $s \cdot 4883 + t \cdot 4369$

Problem # 6
a) Express 9776 in binary.
b) Express $(10010101)_2$ in decimal.
c) Express $(5416)_7$ in base 11

Problem # 7
You intercept the ciphertext "OFJDFOHFXOL", which was enciphered using an affine transformation of single-letter plaintext units in the 27-letter alphabet (with blank=26). You know that the first word is "I" ("I" followed by blank). Determine the enciphering key, and read the message.

Problem # 8
Divide 2^{9439} by 107. What is the remainder?

Problem # 9
Find the last 2 digits of 123^{62}. *Hint:* You may use the Chinese Remainder Theorem.

Problem # 10
(a) Solve $7d \equiv 1 \bmod 30$
(b) Suppose you write a message as a number m mod 31. Encrypt m as m^7 md 31. How would you decrypt? *Hint:* Decryption is done by raising the ciphertext to a power mod 31. Fermat's theorem will be useful.

Problem # 11
Let p be a prime and a an integer not divisible by p. Explain in your own words why the sets

$$\{1, 2, 3, \ldots, p-1\}$$

and

$$\{1a, 2a, 3a, \ldots, (p-1)a\}$$

are the same (when considered mod p).