Que 1: Construct a playfair cipher for

Plaintext: semester7 and

key: technology.

Que 2: In one of his cases, Sherlock Holmes was confronted with the following message.

534 C2 13 127 36 31 4 17 21 41
DOUGLAS 109 293 5 37 BIRLSTONE
26 BIRLSTONE 9 127 171

Although Watson was puzzled, Holmes was able immediately to deduce the type of cipher. Can you?

Q3

The purpose of this problem is to set an upper bound on the number of iterations of the Euclidean algorithm.

a. Suppose that $m = qn + r$ with $q > 0$ and $0 \leq r < n$. Show that $m/2 > r$.

b. Let A_i be the value of A in the Euclidean algorithm after the ith iteration. Show that

$$A_{i+2} < \frac{A_i}{2}$$

c. Show that if m, n, and N are integers with $(1 \leq m, n, \leq 2^N)$, then the Euclidean algorithm takes at most $2N$ steps to find $\gcd(m, n)$.

Q4

Determine the gcd of the following pairs of polynomials.

a. $x^3 + x + 1$ and $x^2 + x + 1$ over GF(2)

b. $x^3 - x + 1$ and $x^2 + 1$ over GF(3)

c. $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over GF(3)

d. $x^5 + 88x^4 + 73x^3 + 83x^2 + 51x + 67$ and $x^3 + 97x^2 + 40x + 38$ over GF(101)