Encryption/Decryption with Matrices

Mark McKelvy
CMPS352

Report

- Started with a remake of the crypto.m file.
  - Modified it so that a number p could be passed into the function, along with the string to encrypt.
  - Modified it so that a matrix A could be passed into the function, this is used for encrypting.
    - A is a 2x2 matrix.
- Checked to see if the m-file performed as claimed.
  - Pass a string *stringA* into the function, with original p = 97, A = [71 2; 2 26]
  - Result will be a string *stringB*.
  - Pass *stringB* into the function, with original p = 97, A = [71 2; 2 26]
  - Result should be *stringA*. Is it? Yes.
- Next checked to see if p = 96 would work.
  - Couldn't get original string back
- What about p = 95?
  - Couldn't get original string back
- What about p = 98?
  - Still couldn't get original string back.
- P = 97 is a prime number.
  - Try p = 91: no luck.
  - Try p = 103: still no luck.
- Let's observe the matrix A.
  - Main diagonal sums to the prime number p.
  - Matrix is currently [71 2; 2 26]
- Let's go back to p = 97, see if changing the values will matter (but leaving the sum equal to p)
  - Try changing the matrix to [67 2; 2 30] to see the effect.
  - Still cannot get the encrypted string back.

- Perhaps a second try at this, maybe the sum is important, but also one thing to note: there are 26 letters in the alphabet.
    - Try the next largest prime: p = 103
    - Let the sum of the main diagonal of A be p.
    - Let the 2,2 position of A remain 26.
    - Result: still unsuccessful
- Third time is a charm right?
    - Try p = 103 again.
    - Let the sum of the main diagonal of A be p.
    - Let the 1,1 position of A remain as 71.
    - Result: again unsuccessful.