Crypto Unit 3 Test Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Part 1: No Calculator**

**Find a unique solution, by hand**

1. Solve 7x = 3 (mod 24)
2. Solve 25x = 7 (mod 26)
3. Solve 9x = 24 (mod 31)

**Find all solutions, by hand**

1. Find all solutions to 10x = 14 (mod 26)
2. Find all solutions to 7x = 21 (mod 28)
3. Find the GCD of 610 and 987

**Find all solutions:**

1. Solve the system 2x + 4y = 14; 14x + 7y = 4 (mod 16)

**Part 2: Calculator**

Given the definitions below, evaluate the following mod 26.

A = ⎡6 1 ⎤

⎣17 13⎦

v = ⎡-12⎤

⎣ 18⎦

1. Find A\*v (mod 26)
2. Find A inverse (mod 26)
3. Solve Ax = v (mod 26) for x (x is a vector).

1. Solve the system 9x + 14y = 13; 13x + 27y = 11 (mod 41)
2. Solve 1330x = 1234 (mod 1346)

**In the following affine ciphers assume a 26 char alphabet, A=0, Z=25**

**also assume in y=ax+b that x is always the plaintext**

1. Affine encode the following using a = 5 and b = -14 y = ax+b mod 26

SNOWDAY

1. Affine decode the following using a = 9 and b = 17 y = ax+b mod 26

ULETMB

1. Find the encoding transformation if FKZMQUZWS decodes as FIREWORKS

**Part 3: Computer**

**You may use any Python code you developed in class or sympy libraries.**

1. Use a digraph encoding with a=375 and b= 114 to encrypt BOMBOGENESIS

**JIUVKYBXWAOA**

1. **Use a digraph encoding with a=343 and b= 31 to decrypt SSPXYOPX (y = ax+b)**

**CPVQVJVQ**

1. A digraph transformation has encoded EARLYDECISION as SWAPQNWQOUHGJF. Find the **decryption** coefficients and write the equation as x = ay + b.   
   **x = 12y + 22**
2. **Find the inverse of the equation y=13x-14 mod 41**

**y = 19x-20 mod 41**

You have intercepted the ciphertext

M4468NZ.F0SR6\*BD4GTOPKBV\*1D7?TYSKD

CXHG!EJ147SDL8SFFPG8O2R4NDJJXGG!.A66

NMJ947.AZH-2BXIZ.\*EM

which you know to have been encrypted with a linear 2x2 matrix encryption scheme.

Previous analysis has revealed the digraphs TO and ER are encrypted

as the ciphers AQ and 8J, respectively. Use this information to

determine the encryption matrix E and decipher the message.

Use the alphabet **ABCDEFGHIJKLMNOPQRSTUVWXYZ!.?0123456789-\***

1. Use this information to determine the encryption matrix E and decipher the message.

Encryption Matrix:

**I WANT AN OFFICIAL RED RYDER CARBINE ACTION 200- SHOT RANGE MODEL AIR RIFLE. NO. YOULL SHOOT YOUR EYE OUT KID.**

**10 14**

**40 6**

1. You have intercepted the ciphertext **K7EP?G0MJLYO?!D0GW6KMUBQ\*-.FJ-** and you know it was encrypted with the above alphabet, first as a 2x2 matrix cipher and THEN as a linear cipher using y = 3x, before being turned back into letters. Can you recover the original text? You know the first encryption matrix is [[7,24],[4,3]]  
     
   **NOBODY IS SAFE. RUN FOR YOUR LIVES**
2. Bonus: Using the above alphabet and matrix, find a pair of letters which encode to the same thing (so “EG” encodes to “EG” for example), or prove that none exists. You may do this mathematically or using the computer.