Unit 2 Practice Test

**Part 1: No Calculator**

**Find all solutions, by hand, or state that there are none:**

1. 7x = 3 (mod 24)
2. 25x = 7 (mod 26)
3. 9x = 24 (mod 27)
4. 10x = 14 (mod 26)
5. 7x = 21 (mod 28)

**Use the Euclidean Algorithm and/or Extended Algorithm to solve by hand:**

1. Find the GCD of 621 and 987
2. Find the inverse of 354 mod 673

**Find all solutions as (x, y) pairs in mod 16:**

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

Given the definitions below, evaluate the following mod 26.

A = ⎡6 1 ⎤ v = ⎡-12⎤

⎣17 13⎦ ⎣ 18⎦

1. Find A\*v (mod 26)
2. Find A inverse (mod 26)

**Part 2: Calculator**

Continue with A and v as defined above.

1. Solve Ax = v (mod 26) for x (x is a 2x1 matrix like v).
2. Solve the system 9x + 14y = 13; 13x + 27y = 11 (mod 41)
3. Solve 1330x = 1234 (mod 1346)

**In the following affine ciphers assume a 26 char alphabet, A=0, Z=25, and assume in y=ax+b that x is always the plaintext.**

1. Affine encode the following using a = 5 and b = 12 y = ax+b mod 26: SNOWDAY
2. Affine decode the following using a = 9 and b = 17 y = ax+b mod 26: ULETMB
3. Find the encoding transformation if FKZMQUZWS decodes as FIREWORKS

**Part 3: Computer**

**You may use any Python code you developed in class or any additional methods you wish to write. You may not use websites or additional programs you haven’t written.**

1. Use a digraph encoding with a=375 and b= 114 to encrypt BOMBOGENESIS
2. Use a digraph encoding with a=343 and b= 31 to decrypt PVAIUJKSYRSR (y = ax+b)
3. A digraph transformation has encoded EARLYDECISION as SWAPQNWQOUHGJF. Find the original transformation coefficients and write the equation as y = ax + b
4. Find the inverse of the equation y=13x-14 mod 41
5. Using the matrix [[6, 1], [17, 3]], encrypt “INFINITYWAR” and decrypt “SKCVSCKLURRZWWYBWX”.
6. 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 decryption matrix D and decipher the message.

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

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]].
2. Decode the ciphertext “IISUMSWIFDBWTKBNYDVKWFLCMOYWZHYVUYFFBHUMDBEHMEPGTO”. It was encoded using a Vigenere cipher with keyword “STEPONE”, then a keyword columnar transposition cipher (no junk characters) with the keyword “STEPTWO”, then a Hill cipher using the matrix from #21. The standard 26-letter alphabet was used.