CS 355, Fall, 2019, Homework 3

1. Does the congruence $15275x \equiv 70 \pmod{27965}$ have a solution? Explain your answer. If it does have a solution, find all of its solutions.

2. Does the congruence $91x \equiv 85 \pmod{107}$ have a solution? Explain your answer. If it does have a solution, find all of its solutions.

3. Let X' denote the bit-by-bit complement of a bit string X.

a. Show that if $C = DES_K(M)$, then $C' = DES_{K'}(M')$. (Go through each step of DES and tell which intermediate values are complemented and which are not. For example, is the input to the third S-box in Round 5 complemented when M and K are replaced by their complements? Explain why your answers are correct.)

b. Explain how this property can be exploited in a chosen-plaintext attack to reduce the search effort by roughly 50%. Part of your answer should be an algorithm which tells exactly what to do. (Hint: Begin by obtaining the ciphertext for a plaintext M and for its complement M'.)

4. Suppose that a plaintext of length 640 bits is enciphered using DES with one of the encryption modes, yielding a ciphertext of length 640 bits. The ciphertext is then sent by radio to a receiver, who will decipher it. Now suppose that during transmission, bit 249 is complemented by radio interference. How many bits deciphered MAY be incorrect if the encryption mode is:

a. ECB?

b. CBC?

c. OFB?

d. CTR?

e. CFB?

Explain how you got each answer.