Name: _____

Section: _____

United States Air Force Academy
Department of Computer Science
CS431 – Fall 2014
Graded Review 1
(125 PTS)

TEXTBOOK, LAPTOP AND ANY MATERIALS OR PROGRAMS PRODUCED BY YOU ARE PERMITTED

NETWORK ACCESS IS NOT ALLOWED, DISABLE YOUR WIRELESS CARD

You MUST show some form of work for full credit

Test Time: 50 Minutes

ACADEMIC SECURITY: This examination is not released from academic security until 1623 on Fri 26 Sep. Until this time, you may not discuss the examination contents or the course material with anyone other than your instructor.

INTEGRITY: Your honor is extremely important. This academic security policy is designed to help you succeed in meeting academic requirements while practicing the honorable behavior our country rightfully demands of its military. Do not compromise your integrity by violating academic security or by taking unfair advantage of your classmates.

AUTHORIZED RESOURCES: *Any except the internet. Disable your wireless card.*

ACADEMIC TESTING MATERIAL

SAFEGUARD IT BEFORE IT IS ADMINISTERED.

NOTE: **You must use the given method to solve where specified.** Otherwise, you can solve using any desired method. Brute force, spreadsheet, calculator, trial and error, any of these approaches can yield full credit answers-**but you must show some form of work.**

1. [5 pts] Find the inverse of 17 mod 25.

2. [10 pts] Solve using the Extended Euclidean algorithm: $x \equiv 22^{-1} \pmod{25}$

3. [10 pts] Find ***all*** solutions in the appropriate range, or indicate when no solution exists. Any method for solving is acceptable, but show some work:

   $8x \equiv 20 \pmod{100}$

   $6x \equiv 5 \pmod{27}$

4. [15 pts] List ***all*** solutions to the equations below, or state that no solutions exist.

$x^2 \equiv 3 \pmod{11}$

$x^2 \equiv 2 \pmod{43}$

$x^2 \equiv 29 \pmod{35}$

5. [15 pts] We want to use an affine cipher for encryption and decryption but we are limited to the first 18 letters of the alphabet for all plaintext and ciphertext. How many keys are there for this affine cipher? Why?

6. [10 pts] You run an experiment where you flip a coin (giving outcome E_1) and roll a die (giving outcome E_2). You think about it and notice:

$$H(E_1, E_2) = H(E_1) + H(E_2)$$

Now describe an experiment **different** from any discussed in class or in the readings or in the problem sets for which:

$$H(E_1, E_2) \neq H(E_1) + H(E_2)$$

What must be true about the relationship between E_1 and E_2 to cause this?

7. [30 pts] Let the plaintext, key, and ciphertext for a cipher be ***P***={*a, b*}, ***K***={*k*1, *k*2 } and ***C***={A, B} where the keys are equally likely. The following tables give the ciphertext resulting from each key/plaintext pair, and the plaintext probabilities:

	a	*b*
*k*1	A	B
*k*2	B	A

p(Plaintext = '*a*') = 0.70
p(Plaintext = '*b*') = 0.30

Find the following:

a. p(**Ciphertext** = 'A')

b. p(**Plaintext** = '*a*', **Ciphertext** = 'A')

c. H(**P**)

d. H(**K**)

e. H(**P|C**).

8. [10 pts] Mark each of the following as ***True*** or ***False***.

   _____ a) Two integers x and y are both relatively prime to m. Therefore, they must be relatively prime to each other.

   _____ b) Conditioning can only increase entropy.

   _____ c) If $a \mid b$ and $a \mid c$, then it is also true that $a \mid (ax + by)$ for any values of x and y.

   _____ d) A system has perfect secrecy if and only if, for all possible plaintexts P and possible ciphertexts C, $H(P \mid C) < H(P)$.

   _____ e) The Vigenere Cipher could not be broken using the technique we learned if all plaintext letters were equally likely.

9. [15 pts] Five cadets are fighting over a tray of extra Choco-Tacos at lunch. When the cadets tried to distribute the ice cream treats as equally as possible, four were left over. When they fought over who should get the extras, one of the cadets was ordered to sit down. When the remaining cadets again tried to divide the Choco-Tacos equally, three of the treats were left over. When the cadets fought again over who should get the extras, another cadet had to leave. When the remaining cadets divided the treats one last time, only one was left over. So they gave the extra to the Mitchell Hall worker clearing the table and all skipped away happily.

   How many Choco-Tacos were on the tray at the start?

10. [5 pts] For the last problem, what is another number of Choco-Tacos that would meet the constraints?