Grading Rubric: Each problem is worth 10 points. Points are evenly distributed among the sub-questions for each problem.

1.1 The system must keep personal identification numbers confidential, both in the host system and during transmission for a transaction. It must protect the integrity of account records and of individual transactions. Availability of the host system is important to the economic well-being of the bank, but not to its fiduciary responsibility. The availability of individual teller machines is of less concern.

1.3 a. The system will have to assure confidentiality if it is being used to publish corporate proprietary material.
b. The system will have to assure integrity if it is being used to laws or regulations.
c. The system will have to assure availability if it is being used to publish a daily paper.

1.4
a. An organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability.

b. A law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate.

c. A financial organization managing routine administrative information (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

d. The management within the contracting organization determines that:
(i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

e. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact

from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. Examples from FIPS 199.

2.3： a. 2 b. 3 c. 4 There are other correct answers

2.10: $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$

2.12
a. gcd(24140, 16762) = gcd(16762, 7378) = gcd(7378, 2006) = gcd(2006, 1360) = gcd(1360, 646) = gcd (646, 68) = gcd(68, 34) = gcd(34, 0) = 34
b. 35

2.13 a. We want to show that m > 2r. This is equivalent to qn + r > 2r, which is equivalent to qn > r. Since n > r, we must have qn > r.

b. If you study the pseudocode for Euclid's algorithm in the text, you can see that the relationship defined by Euclid's algorithm can be expressed as

$$A_i = q_i A_{i+1} + A_{i+2}$$

The relationship $A_{i+2} < A_i/2$ follows immediately from (a).

c. From (b), we see that $A_3 < 2^{-1}A_1$, that $A_5 < 2^{-1}A_3 < 2^{-2}A_5$, and in general that $A_{2j+1} < 2^{-j}A_1$ for all integers j such that $1 < 2j + 1 \leq k + 2$, where k is the number of steps in the algorithm. If k is odd, we take j = (k + 1)/2 to obtain N > (k + 1)/2, and if k is even, we take j = k/2 to obtain N > k/2. In either case k < 2N.

2.16
a. 3239
c. 550

2.26 Only multiples of p have a factor in common with p^n, when p is prime. There are just p^{n-1} of these $\leq p^n$, so $\varphi(p_n) = p^n - p^{n-1}$.

2.27 a. $\varphi(41) = 40$, because 41 is prime
b. $\varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$
c. $\varphi(231) = \varphi(3) * \varphi(7) * \varphi(11) = 2 * 6 * 10 = 120$
d. $\varphi(440) = \varphi(2^3) * \varphi(5) * \varphi(11) = (2^3 - 2^2) * 4 * 10 = 160$

Problem 3.3: Assume that the most frequent plaintext letter is e and the second most frequent letter is t. Note that the numerical values are e = 4; B = 1; t =19; U = 20. Then we have the following equations:

$1 = (4a + b) \bmod 26$
$20 = (19a + b) \bmod 26$

Thus, 19 = 15*a* mod 26. By trial and error, we solve: *a* = 3.
Then 1 = (12 + *b*) mod 26. By observation, *b* = 15.

Problem 3.5: a. The first letter t corresponds to A, the second letter h corresponds to B, e is C, s is D, and so on. Second and subsequent occurrences of a letter in the key sentence are ignored. The result

```
ciphertext: SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA
plaintext: basilisk to leviathan blake is contact
```

b. It is a monoalphabetic cipher and so easily breakable.

c. The last sentence may not contain all the letters of the alphabet. If the first sentence is used, the second and subsequent sentences may also be used until all 26 letters are encountered.

Problem 3.14:
a. We need an even number of letters, so append a "q" to the end of the message (any other letter is also fine). Then convert the letters into the corresponding alphabetic positions:

M	e	e	t	m	e	a	t	t	h	e	u	s	u	a	l
13	5	5	20	13	5	1	20	20	8	5	21	19	21	1	12
P	l	a	c	e	a	t	t	e	n	r	a	t	h	e	r
16	12	1	3	5	1	20	20	5	14	18	1	20	8	5	18
T	h	a	n	e	i	g	h	t	o	c	l	o	c	k	q
20	8	1	14	5	9	7	8	20	15	3	12	15	3	11	17

The calculations proceed two letters at a time. The first pair:

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 13 \\ 5 \end{pmatrix} \bmod 26 = \begin{pmatrix} 137 \\ 100 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 22 \end{pmatrix}$$

The first two ciphertext characters are alphabetic positions 7 and 22, which correspond to GV.
The complete ciphertext:

GVUIGVKODZYPUHEKJHUZWFZFWSJSDZMUDZMYCJQMFWWUQRKR

(Note: an alternative method is to use Y=xK where y and x are both row vectors. If you use this way, use the transpose of the K given above so that ciphertext will be the same)

b. We first perform a matrix inversion. Note that the determinant of the encryption matrix is (9 × 7) – (4 × 5) = 43. Using the matrix inversion formula from the book:

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = \frac{1}{43}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \bmod 26 = 23\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \bmod 26 = \begin{pmatrix} 161 & -92 \\ -115 & 9 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$$

Here we used the fact that $(43)^{-1} = 23$ in Z_{26}. Once the inverse matrix has been determined, decryption can proceed.

Problem 3.15: Consider the matrix **K** with elements k_{ij} to consist of the set of column vectors K_j, where:

$$\mathbf{K} = \begin{pmatrix} k_{11} & \cdots & k_{1n} \\ \vdots & \vdots & \vdots \\ k_{n1} & \cdots & k_{nn} \end{pmatrix} \quad \text{and} \quad \mathbf{K}_j = \begin{pmatrix} k_{1j} \\ \vdots \\ k_{nj} \end{pmatrix}$$

The ciphertext of the following chosen plaintext *n*-grams reveals the columns of **K**:
(B, A, A, …, A, A) ↔ K1
(A, B, A, …, A, A) ↔ K2
:
(A, A, A, …, A, B) ↔ K*n*

Problem 3.19:

key: legleglegle
plaintext: explanation
ciphertext: PBVWETLXOZR

Problem 3.20:

(a).

s	e	n	d	m	o	r	e	m	o	n	e	y
18	4	13	3	12	14	17	4	12	14	13	4	24
9	0	1	7	23	15	21	14	11	11	2	8	9
1	4	14	10	9	3	12	18	23	25	15	12	7
B	E	C	K	J	D	M	S	X	Z	P	M	H

(b)

c	a	s	h	n	o	t	n	e	e	d	e	d
2	0	18	7	13	14	19	13	4	4	3	4	3
25	4	22	3	22	15	19	5	19	21	12	8	4
1	4	14	10	9	3	12	18	23	25	15	12	7
B	E	C	K	J	D	M	S	X	Z	P	M	H