EE-426 / CE-442: Cryptography and Network Security
ASSIGNMENT NO.1

Syed Ahad Ali
sa07753
L1

September 17, 2024

Fall 2024
Habib University
Dhanani School of Science & Engineering
TOTAL MARKS:100
OBTAINED MARKS:

Purpose

The purpose of this assignment is to help you apply the concepts of access control, security attacks, security services, and security mechanisms. In addition, concepts of modular arithmetic and concepts from number theory like extended Euclidean algorithm, linear Diophantine equation, residue matrices will be reinforced.

Instructions

1. This assignment should be done individually.
2. All questions should be answered in black ink only.
3. Scan your answer sheet and upload it on LMS before the due date.

Grading Criteria

1. Your assignments will be checked by the instructor.
2. You may be asked to give a viva where you will be judged on whether you understood the questions yourself. If you are unable to correctly answer the question you have attempted, you may lose your marks.
3. Zero will be given if the assignment is found to be plagiarized.
4. Untidy work will result in a reduction of your points.

Late Submission Penalty

- 1-day late submission - 20% deduction of the maximum allowable marks.
- 2-days late submission - 40% deduction of the maximum allowable marks.
- No submission will be accepted after one week of the original deadline.

CLO Assessments

Course Learning Outcomes		CLO Assessed
CLO 1	Apply the concepts from number theory and algebraic structures in understanding the design of cryptographic algorithms.	✓
CLO 2	Evaluate the suitability of message integrity, message authentication, and key management methods when applying in a given security scenario.	
CLO 3	Explain the setup, algorithms, and security issues in existing symmetric-key and asymmetric-key cryptosystems.	
CLO 4	Apply cryptography-based network security technologies in the design of networked information systems.	

1. ($5 \times 2 = 10$ points) For the DAC model discussed in Chapter 1, an alternative representation of the protection state is a directed graph. Each subject and each object in the protection state is represented by a node (a single node is used for an entity that is both subject and object). A directed line from a subject to an object indicates an access right, and the label on the link defines the access right.

   (a) Draw a directed graph that corresponds to the access matrix of the following Figure.

	File 1	File 2	File 3	File 4
User A	Own, Read, Write		Own, Read, Write	
User B	Read	Own, Read, Write	Write	Read
User C	Read, Write	Read		Own, Read, Write

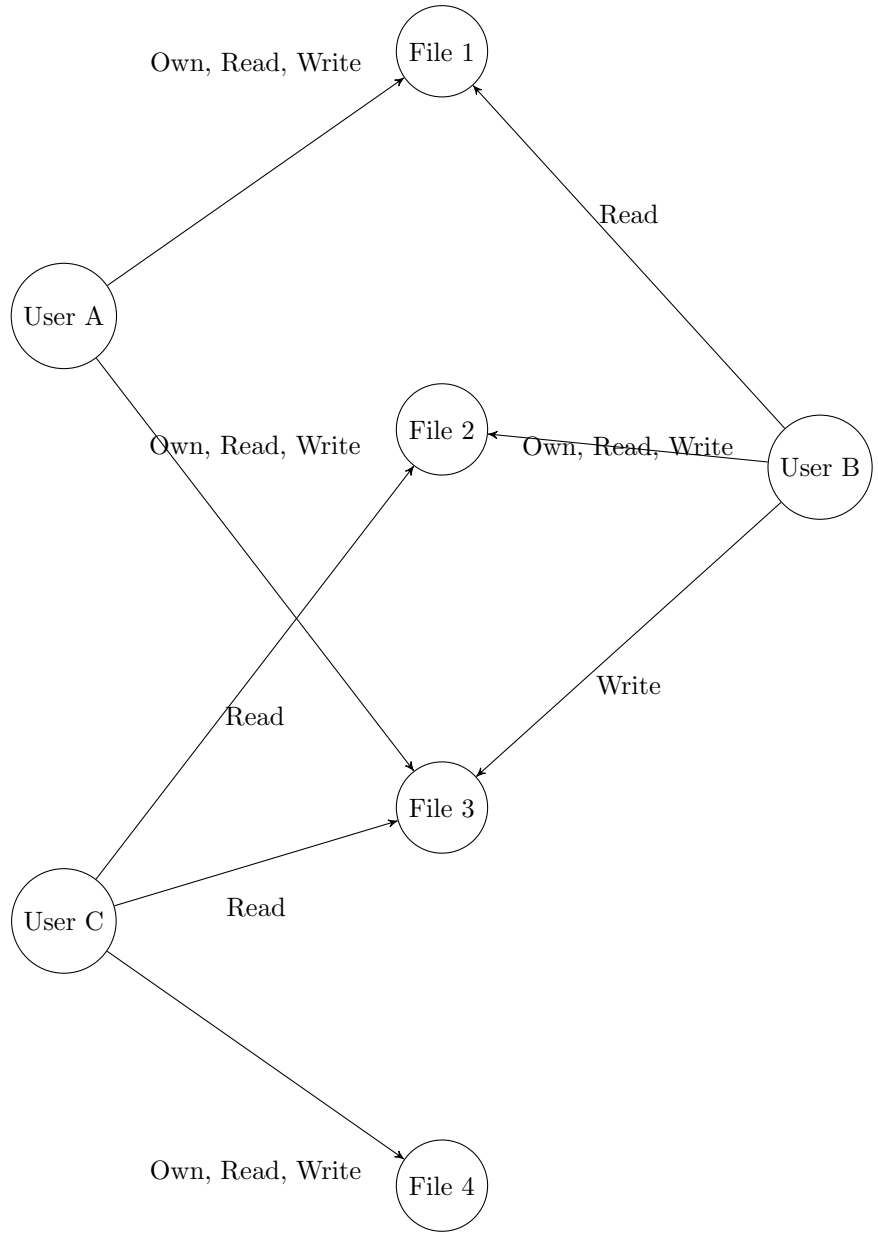
Figure 1: Access Matrix

(b) Draw a directed graph that corresponds to the extended access matrix of the following Figure.

		OBJECTS								
		Subjects			Files		Processes		Disk Drives	
		S1	S2	S3	F1	F2	P1	P2	D1	D2
SUBJECTS	S1	Control	Owner	Owner Control	Read*	Read Owner	Wakeup	Wakeup	Seek	Owner
	S2		Control		Write*	Execute			Owner	Seek*
	S2			Control		Write	Stop			

Figure 2: Extended Access Control Matrix

Solution:



(a)

Figure 3: Directed Graph for the Access Matrix

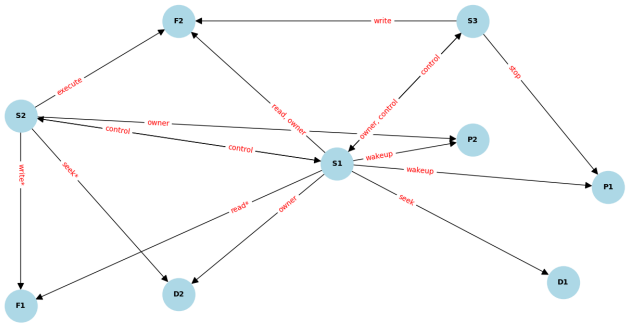


Figure 4: Directed Graph for the Extended Access Matrix (Note: There are directed edges from each subject node to themselves with the label of control)

(b)

2. (10 points) Using the Euclidean algorithm, find the greatest common divisor of the following pair of integers: 300 and 42.
Also, based on the result, comment whether the pair is relatively-prime or not relatively-prime.

Solution: The algorithm is as follows:

q	r_1	r_2	**r**
7	300	42	6
7	42	6	0
	6	0	

The greatest common divisor of 300 and 42 is 6. Since the GCD is not 1, the pair is not relatively-prime.

3. (10 points) Using the extended Euclidean algorithm, find the greatest common divisor of the following pair and the value of s and t: 400 and 60.

Solution:

q	r_1	r_2	**r**	s_1	s_2	**s**	t_1	t_2	**t**
6	400	60	40	1	0	1	0	1	-6
1	60	40	20	0	1	-1	1	-6	7
2	40	20	0	1	-1	3	-6	7	-20
	20	0		-1	3		7	-20	

The GCD of the pair 600 and 400 is 20. Value of s is -1 and t is 7.

4. ($2 \times 5 = 10$ points) Find the results of the following operations:
   (a) 22 mod 7
   (b) 140 mod 10
   (c) -78 mod 13
   (d) 0 mod 15
   (e) 144 mod 26

Solution:

(a) $22 \equiv 1 \pmod 7$

(b) $140 \equiv 0 \pmod{10}$

(c) $-78 \equiv 0 \pmod{13}$

(d) $0 \equiv 0 \pmod{15}$

(e) $144 \equiv 14 \pmod{26}$

5. (5 points) Perform the following operations using reduction first.
   (a) (4223 + 17372) mod 10
   (b) (424 × 32) mod 10

Solution:

(a)

$$(4223 + 17372) \bmod 10$$
$$(3 + 2) \bmod 10$$
$$5 \bmod 10 = 5$$

(b)

$$(424 \times 32) \bmod 10$$
$$(4 \times 2) \bmod 10$$
$$8 \bmod 10 = 8$$

6. (5 points) Let us assign numeric values to the uppercase alphabet (A = 0, B = 1, . . . , Z = 25). We can now do modular arithmetic on the system using modulo 26.
   (a) What is (M + N) mod 26 in this system?
   (b) What is (B + 6) mod 26 in this system?
   (c) What is (Z - 5) mod 26 in this system?
   (d) What is (A - 10) mod 26 in this system?
   (e) What is (D × 3) mod 26 in this system?

Solution:

(a)

$$(M + N) \bmod 26$$
$$(12 + 13) \bmod 26$$
$$25 \bmod 26 = 25$$

(b)

$$(B + 6) \bmod 26$$
$$(1 + 6) \bmod 26$$
$$7 \bmod 26 = 7$$

(c)

$$(Z - 5) \bmod 26$$
$$(25 - 5) \bmod 26$$
$$20 \bmod 26 = 20$$

(d)

$$(A - 10) \bmod 26$$
$$(0 - 10) \bmod 26$$
$$16 \bmod 26 = 16$$

(e)

$$(D \times 3) \bmod 26$$
$$(3 \times 3) \bmod 26$$
$$9 \bmod 26 = 9$$

7. (5 points) Suppose we are given a set of residues with modulus 26 (Z_{26}):
   (a) List all additive inverse pairs in modulus 26.
   (b) List all multiplicative inverse pairs in modulus 26.

Solution:

(a)
- (0, 0)
- (1, 25)
- (2, 24)
- (3, 23)
- (4, 22)
- (5, 21)
- (6, 20)
- (7, 19)
- (8, 18)
- (9, 17)
- (10, 16)
- (11, 15)
- (12, 14)
- (13, 13)

(b)
- (3, 9)
- (5, 21)
- (7, 15)
- (11, 19)
- (17, 23)
- (25, 25)

8. (5 points) Find the multiplicative inverse of the following integer in (Z_{180}) using the extended Euclidean algorithm: 11.

Solution:

q	r_1	r_2	**r**	t_1	t_2	**t**
16	180	11	4	0	1	-16
2	11	4	3	1	-16	33
1	4	3	1	-16	33	-49
3	3	1	0	33	-49	180
	1	0		-49	180	

The multiplicative inverse of 11 from the table is -49. Since the inverse is negative, the positive value is 131.

9. (10 points) A post office sells only 39-cent and 15-cent stamps. Find the number of stamps a customer needs to buy to put \$2.70 postage on a package. Find a few solutions.

Solution: Let x be the number of 39-cent stamps and y be the number of 15-cent stamps. The linear diophantine equation is:

$$39x + 15y = 270$$

By calculating the values of d, s, and t using the extended Euclidean algorithm;

q	r_1	r_2	**r**	s_1	s_2	**s**	t_1	t_2	**t**
2	39	15	9	1	0	1	0	1	-2
1	15	9	6	0	1	-1	1	-2	3
1	9	6	3	1	-1	2	-2	3	-5
2	6	3	0	-1	2	-5	3	-5	13
	3	0		2	-5		-5	13	

d = 3, s = 2, and t = -5.
Infinite solutions exist as 3—270.
Considering the solutions only where x and y both are positive integers, the equations are:

$$x = \frac{c \times s + k \times b}{d}$$

$$y = \frac{c \times t - k \times a}{d}$$

For k $\in$ [-36, -35] we will have positive values of x & y given as;

k	x	y
-36	0	18
-35	5	5

So the customer needs to buy 5 39-cent stamps and 5 15-cent stamps or just 18 15-cent stamps to put $2.70 postage on a package.

10. (10 points) Find all solutions to the following linear equation: 3x + 4 ≡ 6 (mod 13).

Solution:

$$3x + 4 \equiv 6 \pmod{13}$$

$$3x + 4 + 9 \equiv 6 + 9 \pmod{13}$$

$$3x \equiv 2 \pmod{13}$$

The equation is of the form $ax \equiv b$ (mod m). As d = 1 and 1—2, the equation has one solution:

$$x \equiv (3^{-1} \times 2) \pmod{13}$$

Finding the multiplicative inverse of 3 (mod 13):

q	r_1	r_2	r	t_1	t_2	t
4	13	3	1	0	1	-4
3	3	1	0	1	-4	13
	1	0		-4	13	

The multiplicative inverse of 3 in (Z_{13}) is -4 ≡ 9.

$$x \equiv 9 \times 2 \pmod{13}$$

$$x \equiv 18 \pmod{13}$$

$$x \equiv 5 \pmod{13}$$

So the solution to the equation is x = 5.

11. (10 points) Find the determinant and the multiplicative inverse of each residue matrix over (Z_{26}):

$$A = \begin{bmatrix} 1 & 5 \\ 3 & 4 \end{bmatrix}$$

$$B = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Solution:

(a) The inverse of a matrix A is given by:

$$A^{-1} = \frac{\text{Adj}(A)}{\det(A)} \pmod{26}$$

Since the matrix is 2x2, the determinant is calculated as:

$$\det(A) = 4 - 15 \pmod{26}$$

$$\det(A) = -11 \pmod{26}$$

$$\det(A) = 15 \pmod{26}$$

From Question 7, the multiplicative inverse of 15 in (Z_{26}) is 7. For the adjoint matrix:

$$\begin{bmatrix} 4 & -5 \\ -3 & 1 \end{bmatrix}$$

We take the modulo 26 of the negative values:

$$\begin{bmatrix} 4 & 21 \\ 23 & 1 \end{bmatrix}$$

Now the inverse of the matrix A can also be written as the following:

$$A^{-1} = \text{Adj}(A)\det(A)^{-1} \pmod{26}$$

Since the determinant is 15 and its inverse is 7, the inverse of the matrix A is:

$$A^{-1} = \begin{bmatrix} 4 & 21 \\ 23 & 1 \end{bmatrix} \times 7 \pmod{26}$$

$$A^{-1} = \begin{bmatrix} 28 & 147 \\ 161 & 7 \end{bmatrix} \pmod{26}$$

$$A^{-1} = \begin{bmatrix} 2 & 17 \\ 5 & 7 \end{bmatrix} \pmod{26}$$

(b) The determinant of the matrix B is calculated as:

$$B^{-1} = \text{Adj}(B)\det(B)^{-1} \pmod{26}$$

$$\det(B) = 17(18 \times 19 - 2 \times 21) - 17(21 \times 19 - 2 \times 21) + 5(21 \times 2 - 18 \times 2) \pmod{26}$$

$$\det(B) = -939 \pmod{26}$$

$$\det(B) = 23 \pmod{26}$$

From Question 7, the multiplicative inverse of 23 in (Z_{26}) is 17, So $\det(B)^{-1} = 17$. For the adjoint matrix:

$$\text{Adj}(B) = \begin{bmatrix} (18 \times 19 - 2 \times 21) & -(21 \times 19 - 21 \times 2) & (21 \times 2 - 18 \times 2) \\ -(17 \times 19 - 5 \times 2) & (17 \times 19 - 5 \times 2) & -(17 \times 2 - 17 \times 2) \\ (17 \times 21 - 5 \times 18) & -(17 \times 21 - 5 \times 21) & (17 \times 18 - 17 \times 21) \end{bmatrix}^{\text{T}} \pmod{26}$$

After simplifying the matrix:

$$\text{Adj}(B) = \begin{bmatrix} 300 & -357 & 6 \\ -313 & 313 & 0 \\ 267 & -252 & -51 \end{bmatrix}^{\text{T}} \pmod{26}$$

After taking the modulo 26 of the negative values:

$$\text{Adj}(B) = \begin{bmatrix} 14 & 7 & 6 \\ 25 & 1 & 0 \\ 7 & 8 & 1 \end{bmatrix}^{\text{T}} \pmod{26}$$

After taking the transpose of the matrix:

$$\text{Adj}(B) = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \pmod{26}$$

The inverse of the matrix B is:

$$B^{-1} = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \times 17 \pmod{26}$$

$$B^{-1} = \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{bmatrix} \pmod{26}$$

$$B^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \pmod{26}$$

12. (10 points) Find all solutions to the following sets of linear equations:

(a)

$$3x + 2y \equiv 5 \pmod{7}$$
$$4x + 6y \equiv 4 \pmod{7}$$

(b)

$$3x + 4y + 6z \equiv 9 \pmod{10}$$
$$x + y + 8z \equiv 7 \pmod{10}$$
$$5x + 8y + 3z \equiv 0 \pmod{10}$$

Solution:

(a) Given;

$$3x + 2y \equiv 5 \pmod{7}$$

$$4x + 6y \equiv 4 \pmod 7$$

We can rewrite the equations as;

$$\begin{bmatrix} 3 & 2 \\ 4 & 6 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 4 \end{bmatrix}$$

Where the matrix A_x, A_y, and A are:

$$A_x = \begin{bmatrix} 5 & 2 \\ 4 & 6 \end{bmatrix}$$

$$A_y = \begin{bmatrix} 3 & 5 \\ 4 & 4 \end{bmatrix}$$

$$A = \begin{bmatrix} 3 & 2 \\ 4 & 6 \end{bmatrix}$$

From Cramer's rule;

$$x = \frac{\det(A_x)}{\det(A)}$$

$$y = \frac{\det(A_y)}{\det(A)}$$

Or;

$$x = \det(A_x) \times \det(A)^{-1}$$

$$y = \det(A_y) \times \det(A)^{-1}$$

Calculating the determinants:

$$\det(A) = 18 - 8 \pmod 7$$

$$\det(A) = 10 \equiv 3 \pmod 7$$

$$\det(A_x) = 30 - 8 \pmod 7$$

$$\det(A_x) = 22 \equiv 1 \pmod 7$$

$$\det(A_y) = 12 - 20 \pmod 7$$

$$\det(A_y) = -8 \equiv 6 \pmod 7$$

Calculating the value of $\det(A)^{-1}$ in (Z_7) using the extended Euclidean algorithm:

q	r_1	r_2	**r**	t_1	t_2	**t**
2	7	3	1	0	1	-2
3	3	1	0	1	-2	7
	1	0		-2	7	

The multiplicative inverse of 3 in (Z_7) is -2 ≡ 5. Calculating the values of x and y:

$$x = 1 \times 5 \pmod 7$$

$$x = 5 \pmod 7$$
$$y = 6 \times 5 \pmod 7$$
$$y = 30 \pmod 7$$
$$y = 2 \pmod 7$$

So the solutions to the equations are x = 5 and y = 2.

(b) Given;

$$3x + 4y + 6z \equiv 9 \pmod{10}$$
$$x + y + 8z \equiv 7 \pmod{10}$$
$$5x + 8y + 3z \equiv 0 \pmod{10}$$

We can rewrite the equations as;

$$\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 7 \\ 0 \end{bmatrix}$$

Where the matrix A_x, A_y, A_z, and A are:

$$A_x = \begin{bmatrix} 9 & 4 & 6 \\ 7 & 1 & 8 \\ 0 & 8 & 3 \end{bmatrix}$$
$$A_y = \begin{bmatrix} 3 & 9 & 6 \\ 1 & 7 & 8 \\ 5 & 0 & 3 \end{bmatrix}$$
$$A_z = \begin{bmatrix} 3 & 4 & 9 \\ 1 & 1 & 7 \\ 5 & 8 & 0 \end{bmatrix}$$
$$A = \begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix}$$

From Cramer's rule;

$$x = \frac{\det(A_x)}{\det(A)}$$
$$y = \frac{\det(A_y)}{\det(A)}$$
$$z = \frac{\det(A_z)}{\det(A)}$$

Or;

$$x = \det(A_x) \times \det(A)^{-1}$$
$$y = \det(A_y) \times \det(A)^{-1}$$
$$z = \det(A_z) \times \det(A)^{-1}$$

Calculating the determinants:

$$\det(A) = 3\begin{vmatrix}1 & 8\\ 8 & 3\end{vmatrix} - 4\begin{vmatrix}1 & 8\\ 5 & 3\end{vmatrix} + 6\begin{vmatrix}1 & 1\\ 5 & 8\end{vmatrix}$$

$$= 3(1\cdot 3 - 8\cdot 8) - 4(1\cdot 3 - 5\cdot 8) + 6(1\cdot 8 - 1\cdot 5)$$

$$= 3(3-64) - 4(3-40) + 6(8-5)$$

$$= 3\cdot(-61) - 4\cdot(-37) + 6\cdot 3$$

$$= -183 + 148 + 18$$

$$= -17 \pmod{10}$$

$$= 3 \pmod{10}$$

$$\det(A_x) = 9\begin{vmatrix}1 & 8\\ 8 & 3\end{vmatrix} - 4\begin{vmatrix}7 & 8\\ 0 & 3\end{vmatrix} + 6\begin{vmatrix}7 & 1\\ 0 & 8\end{vmatrix}$$

$$= 9(1\cdot 3 - 8\cdot 8) - 4(7\cdot 3 - 8\cdot 0) + 6(7\cdot 8 - 1\cdot 0)$$

$$= 9(3-64) - 4(21) + 6(56)$$

$$= 9\cdot(-61) - 4\cdot 21 + 6\cdot 56$$

$$= -549 - 84 + 336$$

$$= -297 \pmod{10}$$

$$= 3 \pmod{10}$$

$$\det(A_y) = 3\begin{vmatrix}7 & 8\\ 0 & 3\end{vmatrix} - 9\begin{vmatrix}1 & 8\\ 5 & 3\end{vmatrix} + 6\begin{vmatrix}1 & 7\\ 5 & 0\end{vmatrix}$$

$$= 3(7\cdot 3 - 8\cdot 0) - 9(1\cdot 3 - 5\cdot 8) + 6(1\cdot 0 - 7\cdot 5)$$

$$= 3(21) - 9(3-40) + 6(0-35)$$

$$= 3\cdot 21 - 9\cdot(-37) + 6\cdot(-35)$$

$$= 63 + 333 - 210$$

$$= 186 \pmod{10}$$

$$= 6 \pmod{10}$$

$$\det(A_z) = 3\begin{vmatrix}1 & 7\\ 8 & 0\end{vmatrix} - 4\begin{vmatrix}1 & 7\\ 5 & 0\end{vmatrix} + 9\begin{vmatrix}1 & 1\\ 5 & 8\end{vmatrix}$$

$$= 3(1\cdot 0 - 7\cdot 8) - 4(1\cdot 0 - 7\cdot 5) + 9(1\cdot 8 - 1\cdot 5)$$

$$= 3(0-56) - 4(0-35) + 9(8-5)$$

$$= 3\cdot(-56) - 4\cdot 35 + 9\cdot 3$$

$$= -168 - 140 + 27$$

$$= -281 \pmod{10}$$
$$= -1 \pmod{10}$$
$$= 9 \pmod{10}$$

Calculating the value of $\det(A)^{-1}$ in (Z_{10}) using the extended Euclidean algorithm:

q	r_1	r_2	**r**	t_1	t_2	**t**
3	10	3	1	0	1	-3
3	3	1	0	1	-3	10
	1	0		-3	10	

The multiplicative inverse of 3 in (Z_{10}) is -3 $\equiv$ 7. Calculating the values of x, y, and z:

$$x = 3 \times 7 \pmod{10}$$
$$x = 21 \pmod{10}$$
$$x = 1 \pmod{10}$$
$$y = 6 \times 7 \pmod{10}$$
$$y = 42 \pmod{10}$$
$$y = 2 \pmod{10}$$
$$z = 9 \times 7 \pmod{10}$$
$$z = 63 \pmod{10}$$
$$z = 3 \pmod{10}$$

So the solutions to the equations are x = 1, y = 2, and z = 3.