USN | | | | | | | | | | |

CMRIT
CMR INSTITUTE OF TECHNOLOGY, BENGALURU.
ACCREDITED WITH A+ GRADE BY NAAC

## INTERNAL ASSESSMENT TEST – I

| Sub: | CRYPTOGRAPHY | | | | | | | Code: | 21EC643 |
|---|---|---|---|---|---|---|---|---|---|
| Date: | 06/ 06 / 2024 | Duration: | 90 mins | Max Marks: | 50 | Sem: | VI | Branch: | ECE |

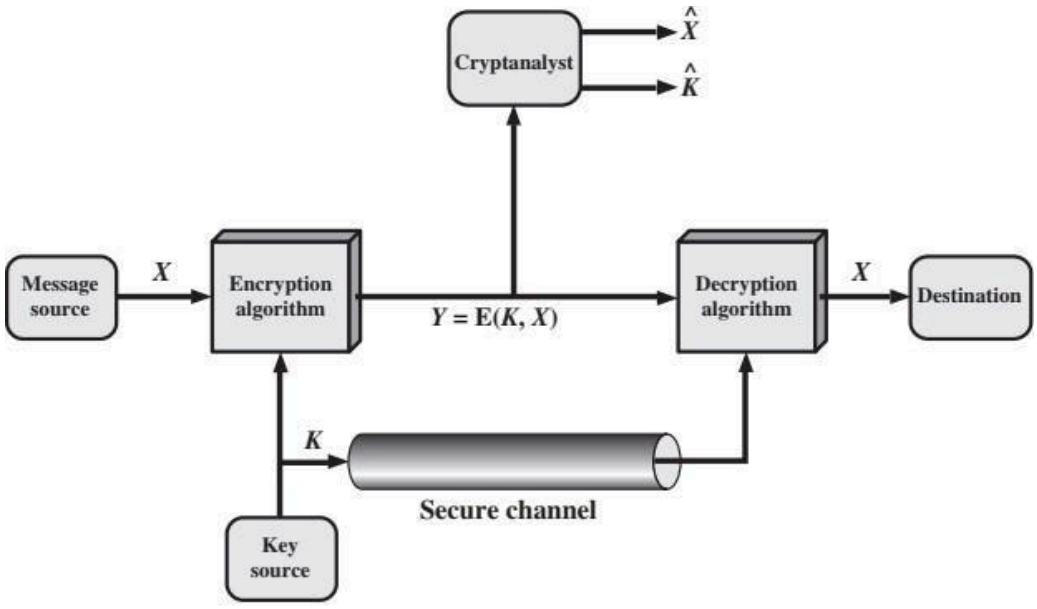
**Answer any 5 full questions**

| | | Marks | CO | RBT |
|---|---|---|---|---|
| 1 | Draw the model of symmetric cryptosystem and explain in detail. | [10] | CO1 | L1 |
| 2 | Encrypt the message "EXAMPOSTPONED" using, play fair cipher with the keyword "BANGLORE" and decrypt the cipher text "QBZKREDJEBCX" to recover the original message. Give the rules for encryption and decryption. | [10] | CO1 | L2 |
| 3 | Use extended Euclidean algorithm and express GCD(1771,528) = $x \cdot 1771 + y \cdot 528$ | [10] | CO3 | L3 |
| 4 | Find the solutions to each of the following linear equations<br>a) $8x \equiv 7 (mod 19)$ b) $3x \equiv 4 (mod 5)$ c) $8x \equiv 6 (mod 5)$ d) $2x \equiv 7 (mod 23)$ | [10] | CO3 | L2 |
| 5 | a) Using the Euclidean Algorithm find the greatest common divisor of 24140 and 16762.<br>b) Write a short note on transposition cipher and one time pad, also explain them with examples. | [5]<br>[5] | CO3<br>CO1 | L3<br>L1 |
| 6 | a) Write a note on finite field of form GF(P)<br>b) Prove that if $a \times c \bmod n \equiv b \times c \bmod n$ then $(a \bmod n) \equiv b \pmod n$. | [5]<br>[5] | CO4<br>CO3 | L2<br>L3 |
| 7 | a) Develop a set of additive and multiplicative tables for modulo-9.<br>b) Find multiplicative inverse of 557 in (mod1759). | [10] | CO3 | L3 |
| 8 | a) Prove the congruence property $w \times x \pmod n \equiv y \times x \pmod n$ provided '$x$' is relatively prime to 'n'.<br>b) What are groups? With an example explain the group axioms. Define Abelian group and cyclic group. | [5]<br>[5] | CO3<br>CO1 | L3<br>L1 |

# IAT-1 Solutions

## 1. Draw the model of the symmetric cryptosystem and explain in detail.

**Marks Distribution: Model of Symmetric System [4 marks] + Explanation [6 marks]**




Model of Symmetric Cryptosystem

A symmetric encryption scheme has five ingredients:

- Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

- Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

- Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

• Decryption algorithm: This is essentially the encryption algorithm run in

reverse. It takes the ciphertext and the secret key and produces the original plaintext.
There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even

if he or she is in possession of a number of ciphertexts together with the plain- text that produced each ciphertext.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

We assume that it is impractical to decrypt a message on the basis of the ciphertext plus knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we need to keep only the key secret. This feature of symmetric encryption is what makes it feasible for widespread use. The fact that the algorithm need not be kept secret means that manufacturers can and have developed low-cost chip implementations of data encryption algorithms. These chips are widely available and incorporated into a number of products. With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.

Let us take a closer look at the essential elements of a symmetric encryption scheme. A source produces a message in plaintext, $X = [X_1, X_2, \ldots, X_M]$. The $M$ elements of $X$ are letters in some finite alphabet. Traditionally, the alphabet usually consisted of the 26 capital letters. Nowadays, the binary alphabet {0, 1} is typically used. For encryption, a key of the form $K = [K_1, K_2, \ldots, K_J]$ is generated. If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination.

With the message $X$ and the encryption key $K$ as input, the encryption algorithm forms the ciphertext $Y = [Y_1, Y_2, \ldots, Y_N]$. We can write this as

$$Y = \mathrm{E}(K, X)$$

This notation indicates that $Y$ is produced by using encryption algorithm E as a function of the plaintext $X$, with the specific function determined by the value of the key $K$.

The intended receiver, in possession of the key, is able to invert the transformation:

$$X = \mathrm{D}(K, Y)$$

An opponent, observing $Y$ but not having access to $K$ or $X$, may attempt to recover $X$ or $K$ or both $X$ and $K$. It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms. If the opponent is interested in only this particular message, then the focus of the effort is to recover $X$ by generating a plaintext estimate $\hat{X}$. Often, however, the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover $K$ by generating an estimate $\hat{K}$.

Cryptographic systems are characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to ciphertext.** All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (i.e., that all operations are reversible). Most systems, referred to as *product systems*, involve multiple stages of substitutions and transpositions.
2. **The number of keys used.** If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
3. **The way in which the plaintext is processed.** A *block cipher* processes the input one block of elements at a time, producing an output block for each input block. A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.

### Cryptanalysis and Brute-Force Attack

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

2. **Encrypt the message "EXAMPOSTPONED" using, play fair cipher with the keyword "BANGLORE"and decrypt the ciphertext "QBZKREDJEBCX" to recover the original message. Give the rules for encryption and decryption.**

**Marks Distribution: Playfair matrix [2 marks] + Encryption rule [2 marks] + Decryption rule [2 marks] + Encryption [2 marks] + Decryption [2 marks]**

| | | | | |
|---|---|---|---|---|
| B | A | N | G | L |
| O | R | E | C | D |
| F | H | I/J | K | M |
| P | Q | S | T | U |
| V | W | X | Y | Z |

**Plaintext is encrypted two letters at a time.**

**If a pair is a repeated letter, insert filler like 'X'. Encryption Rule of Play-Fair Cipher:**

(1) If both letters fall in the same row, replace each with the letter to its right (circularly).

(2) If both letters fall in the same column, replace each with the letter below it (circularly).

(3) Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair.

**Ciphertext is decrypted two letters at a time. Decryption Rules of Play-Fair Cipher:**

(1) Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the left, with the first element of the row circularly following the last.

(2) Two plaintext letters that fall in the same column are each replaced by the letter above, with the top element of the column circularly following the last.

(3) Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

**Plain Text: EX, AM, PO, ST, PO, NE, DX**

**Cipher Text: IN, LH, VF,TU,VF,EI,EZ**

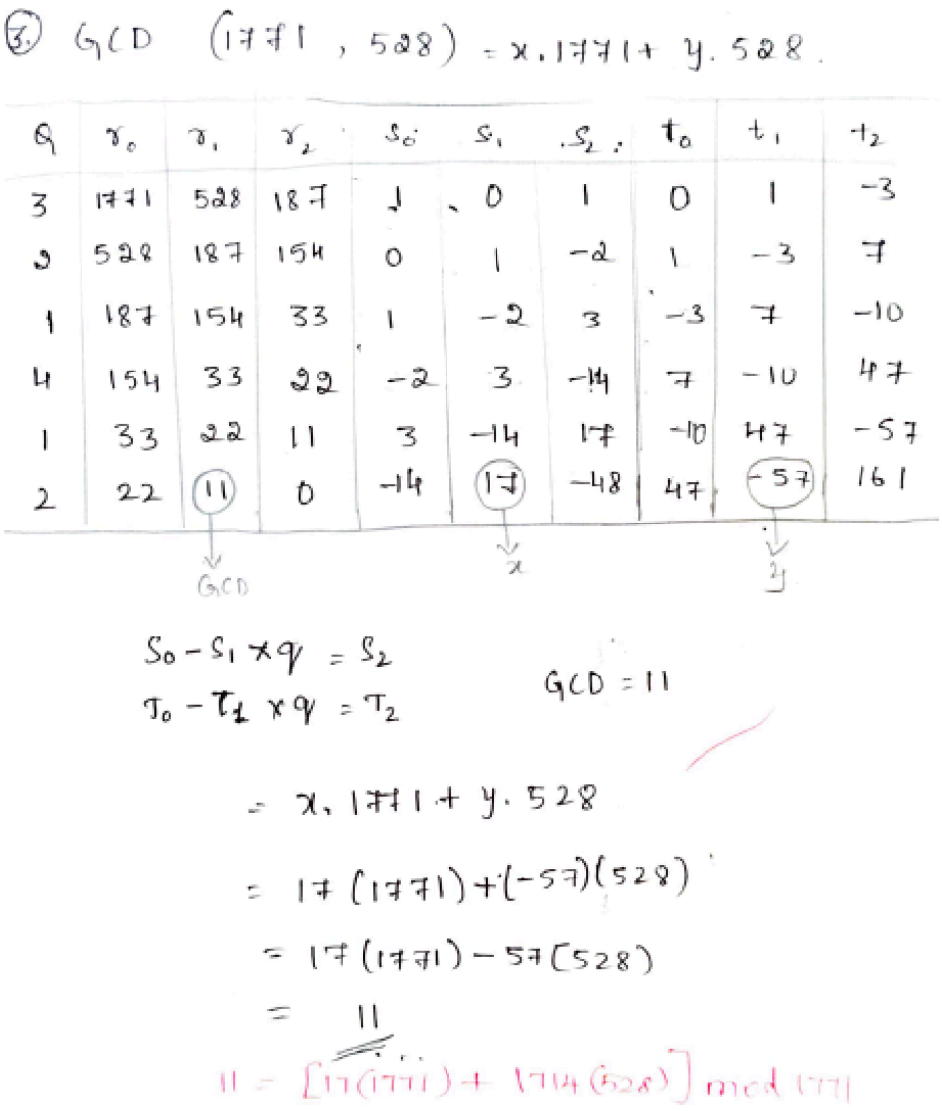
**(JN, LH, VF,TU,VF,EJ,EZ)**

**Cipher text:QB, ZK, RE, DJ, EB, CX**

**Plain text: PA,YM,OR, EM,ON,EY**

**3) Use extended Euclidean algorithm and express**

**GCD (1771, 528) = $x \cdot 1771 + y \cdot 528$**



| q | $r_0$ | $r_1$ | $r_2$ | $s_0$ | $s_1$ | $s_2$ | $t_0$ | $t_1$ | $t_2$ |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 1771 | 528 | 187 | 1 | 0 | 1 | 0 | 1 | -3 |
| 2 | 528 | 187 | 154 | 0 | 1 | -2 | 1 | -3 | 7 |
| 1 | 187 | 154 | 33 | 1 | -2 | 3 | -3 | 7 | -10 |
| 4 | 154 | 33 | 22 | -2 | 3 | -11 | 7 | -10 | 47 |
| 1 | 33 | 22 | 11 | 3 | -11 | 17 | -10 | 47 | -57 |
| 2 | 22 | 11 | 0 | -11 | 17 | -48 | 47 | -57 | 161 |

GCD = 11

$s_0 - s_1 \times q = s_2$

$t_0 - t_1 \times q = t_2$

$= x \cdot 1771 + y \cdot 528$

$= 17(1771) + (-57)(528)$

$= 17(1771) - 57(528)$

$= 11$

$11 = [17(1771) + (-57)(528)] \bmod 1771$

**4) Find the solutions to each of the following linear equations**

**a)8x≡7(mod19)**

**x=[inv(8) mod 19* 7 mod 19]= (12 * 7) mod 19 = 8**

**b) 3x≡4(mod5)**

**x=inv(3) mod 5 * 4 mod5 = (2 *4)mod 5=3**

**c) 8x≡6(mod5) — x=2**

**d) 2x≡7(mod23)** **x=15**

**5a) Using the Euclidean Algorithm, find the greatest common divisor of 24140 and 16762.**

| Dividend | Divisor | Remainder | Quotient |
|---|---|---|---|
| 24140 | 16762 | 7378 | 1 |
| 16762 | 7378 | 2006 | 2 |
| 7378 | 2006 | 1360 | 3 |
| 2006 | 1360 | 646 | 1 |
| 1360 | 646 | 68 | 2 |
| 646 | 68 | 34 (GCD) | 9 |
| 68 | 34 | 0 | 2 |

We know, gcd(a, b) = gcd(b, a mod b) gcd(24140,16762) =gcd(16762,7378) gcd(7378,2006) =gcd(2006,1360) gcd(1360,646) =gcd(646,68) gcd(68,34) = 34 gcd(24140,16762) = 34.

**5b) Write a short note on transposition cipher and one time pad, also explain them with examples.**

- now consider classical transposition or permutation ciphers
- these hide the message by rearranging the letter order
- without altering the actual letters used
- Rail fence technique : “MEETMEAFTERTOGAPARTY”
- M E M E F E T G P R Y
- E T M A T R O A A T

- Cipher text “MEMEFETGPRYETMATROAAT”
- More complex scheme is to write the message in a rectangle
- Plaintext “ATTACKPOSTPONEDUNTILTWOAMXYZ”
-

| 4 | 3 | 1 | 2 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| A | T | T | A | C | K | P |
| O | S | T | P | O | N | E |
| D | U | N | T | I | L | T |
| W | O | A | M | X | Y | Z |

- Ciphertext: “TTNAAPTMTSUOAODWCOIXKNLYPETZ”

| 4 | 3 | 1 | 2 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| T | T | N | A | A | P | T |
| M | T | S | U | O | A | O |
| D | W | C | O | I | X | K |
| N | L | Y | P | E | T | Z |

Ciphertext2: “NSCYAUOPTTWLTMDNAOIEPAXTTOKZ”

**One-Time Pad**

**C:** ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

**Key:** PXLMVMSYDOFUYRVZWC TNLEBNECVGDUPAHFZZLMNYIH

**P:** MR MUSTARD WITH THE CANDLESTICK IN THE HALL

**C:** ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

**Key:** PFTGPMIYDGAXGOUFHKLLLMHSQDQOGTEWBQFGYOVUHWT

**P:** MISS SCARLET WITH THE KNIFE IN THE LIBRARY

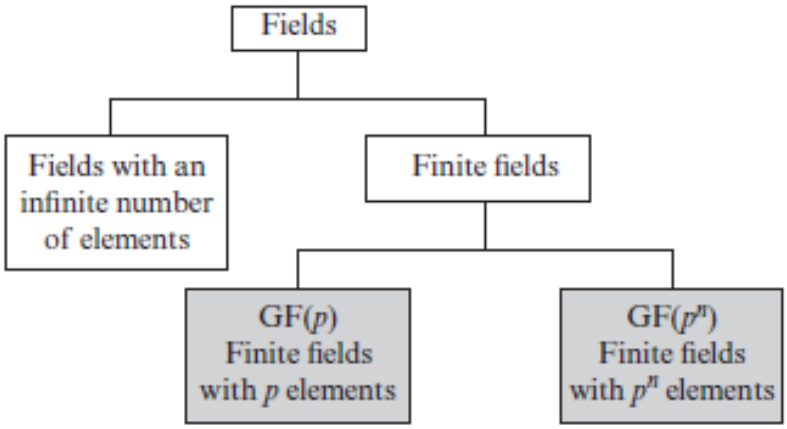
Two fundamental difficulties:

1. There is the practical problem of making large quantities of random keys.
2. And the problem of key distribution and protection, where for every message to be sent, a key of equal length is needed by both sender and receiver.

## 6a) Write a note on finite field of form GF(P)

**Finite (Galois) Fields**

- finite fields play a key role in cryptography
- can show number of elements in a finite field **must** be a power of a prime $p^n$ known as Galois fields.(GF)
- **GF** stands for Galois field, in honor of the mathematician who first studied finite fields.
- Denoted by GF($p^n$)
- in particular often use the fields:
  - GF(p)
  - GF($2^n$)
- Where P is prime Number.




- GF(p) is the set of integers {0,1, … , p-1} with arithmetic operations modulo prime p
- these form a finite field
  - since have multiplicative inverses
  - find inverse with Extended Euclidean algorithm
- hence arithmetic is "well-behaved" and can do addition, subtraction, multiplication, and division without leaving the field GF(p)

Multiplicative inverse ($w^{-1}$): For each $w \in Zp$, $w \neq 0$, *there exists a* $z \in Zp$ such that $w \times z \equiv 1 \pmod p$

## 6b) Prove that if a×c mod n ≡b×c mod n then (a mod n) ≡b (mod n).

To Prove if $(a \times b) \equiv (a \times c) \pmod p$ then $b \equiv c \pmod p$

- If a,b,c are all belongs to the set $Z_n$={0,1,2,…….p-1} and a is relatively prime to p.
- Then there exist a number $a^{-1}$ such that $a \times a^{-1} \equiv 1 \pmod p$
- Now to prove $(a \times b) \equiv (a \times c) \pmod p$ will apply multiplicative inverse to both sides.

- $a^{-1} \times (a \times b) \equiv a^{-1} \times (a \times c) \pmod{p}$ since $a \times a^{-1} \equiv 1 \pmod{p}$
- $\therefore b \equiv c \pmod{p}$
- Point to note that if a is not relatively prime to p then
- $(a \times b) \equiv (a \times c) \pmod{p}$
- e.g. $(6 \times 3) \equiv (6 \times 7) \pmod{8}$
- Here $(6 \times 3) \equiv 2 \pmod{8}$ and $(6 \times 7) \equiv 2 \pmod{8}$ but $3 \equiv 7 \pmod{8}$
- As 6 has no multiplicative inverse over modulo 8.

## 7a) Develop a set of additive and multiplicative tables for modulo-9.

### Additive Table for Modulo 9

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

### Multiplicative Table for Modulo 9

| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **2** | **0** | **2** | **4** | **6** | **8** | **1** | **3** | **5** | **7** |
| **3** | **0** | **3** | **6** | **0** | **3** | **6** | **0** | **2** | **5** |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **4** | 0 | 4 | 8 | 3 | 7 | 0 | 5 | 2 | 5 |
| **5** | 0 | 5 | 1 | 6 | 0 | 6 | 2 | 8 | 4 |
| **6** | 0 | 6 | 3 | 0 | 5 | 3 | 0 | 6 | 3 |
| **7** | 0 | 7 | 5 | 2 | 1 | 8 | 4 | 4 | 2 |
| **8** | 0 | 8 | 7 | 5 | 5 | 4 | 3 | 2 | 1 |

**7b. Find multiplicative inverse of 557 in (mod 1759).**

Xi=X(i-2) - Qi X(i-1), Yi=Y(i-2) - Qi Y(i-1)

| Dividend | Divisor | Ri | Qi | Xi | Yi |
|---|---|---|---|---|---|
| 1759 | 557 | - | - | 1 | 0 |
| 1759 | 557 | - | - | 0 | 1 |
| 1759 | 557 | 88 | 3 | 1 | -3 |
| 557 | 88 | 29 | 6 | -6 | 19 |
| 88 | 29 | 1 | 3 | 19 | -60 |

**Inverse of 557 in mod 1759≡ -60 mod 1759 ≡ 1699 mod 1759**

**Verify: (557*1699) mod 1759≡1 mod 1759**

**8. a)** Prove the congruence property w × *x* (mod n) ≡ y × *x* (mod n) provided '*x*' is relatively prime to 'n'.

w × x (mod n) ≡ y × x (mod n) Provided x is relatively prime to n
6 × 3 (mod 8) = 18(mod 8) = 2 (mod8)
6 × 7 (mod 8) = 42(mod 8) = 2 (mod8)
6 × 3 (mod 8) ≡ 6 × 7 (mod 8) But 3 is not congruent to 7 (mod 8)

b) What are groups? With an example explain the group axioms. Define Abelian group and cyclic group.

- a set G of elements or "numbers" may be finite or infinite
- with some binary operation ' · ' so denoted as {G, · }
- Obeys CAIN:

- Closure: a,b in G, then $a \cdot b$ in G
- Associative law: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- has Identity e: $e \cdot a = a \cdot e = a$
- has inverses $a^{-1}$: $a \cdot a^{-1} = e$

- If also commutative $a \cdot b = b \cdot a$ then forms an **Abelian group**

**Cyclic Group**

- define **exponentiation** as repeated application of operator
  - example: $a^3 = a.a.a$
- and let identity be: $e=a^0$
- a group is cyclic if every element is a power of some fixed element a
  - i.e., $b = a^k$ for some a and every b in group
- a is said to be a generator of the group