St. Vincent Pallotti College of Engineering & Technology, Nagpur
Department of Computer Engineering
Session 2024-25
CNS Practical Details

Practical 3:

Aim: To implement algorithms for real world applications to ensure confidentiality, integrity and authenticity of data.

1A.

Implement Euclid & Extended Euclid Algorithm (EEA) to compute the GCD of two integers. EEA algorithm not only computes the GCD of two integers but also finds the coefficients of Bezout's identity as integers.

Working:

Euclid Algorithm:

The Euclidean Algorithm for finding GCD (A, B) is as follows: If A = 0 then GCD (A, B) =B, since the GCD (0, B) = B, and we can stop. If B = 0 then GCD (A, B) =A, since the GCD(A,0) =A, and we can stop. Write A in quotient remainder form (A = B·Q + R).

Working:

Extended Euclidean Algorithm:

Given two integers *a* and *b*, we often need to find other two integers, *s* and *t*, such that

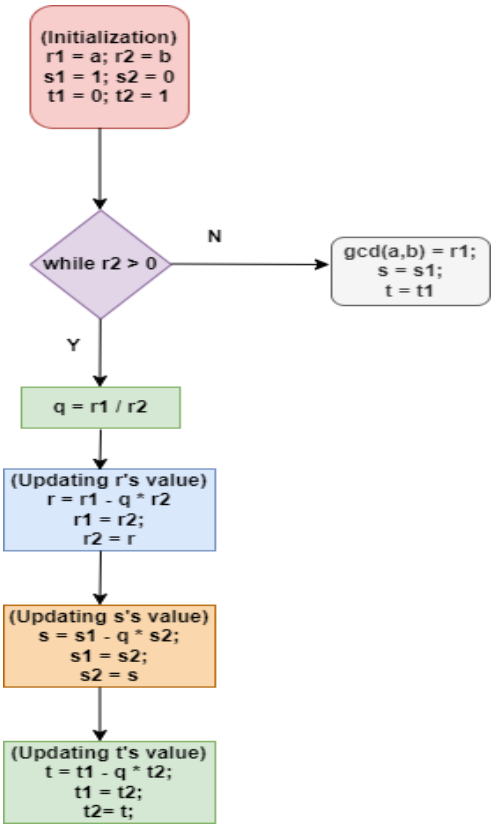
$s * a + t * b = \gcd(a, b)$

***Example*: $\mathbf{gcd(161, 28) = 7, s = -1}$ *and* $\boldsymbol{t = 6}$.**

$(-1) * 161 + 6 * 28 = 7$

The extended Euclidean algorithm can calculate the *gcd (a, b)* and at the same time calculate the values of *s* and *t*.

Following is the flow of Extended Euclidean algorithm:



Given a = 161 and b = 28, find *gcd (a,b)* and the values of *s* and *t*

q	r1	r2	r	s1	s2	s	t1	t2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

i	ri	qi	si	ti
0	161		1	0
1	28	5	0	1
2	21	1	1	-5
3	7	3	-1	6
4	0			

we get gcd (161, 28) = 7 , s = -1, t = 6 .

s *a + t * b = gcd (a,b)

NOTE: Students can execute either in JAVA or C/C++ environment.

1B

Implement Multiplicative & Affine Cipher method to show the encryption and decryption process.

1C

Case Study:

A financial institution, "Secure Bank", needs to transmit sensitive financial data between its headquarters and its branch offices. The data includes account numbers, transaction amounts, and customer information. The institution requires a secure encryption method to protect this data from unauthorized access.

Objective:

Implement Hill Cipher Method to encrypt and decrypt the financial data during the transmission. The technique should be able to handle large amount of data efficiently and should be resistant to cryptanalysis and interception by unauthorized users.

Requirement & Working:

Step 1: Key Generation

The headquarters generates a random 2x2 matrix, known as the Hill Cipher key. This key is shared with the branch offices through a secure channel.

Step 2: Encryption

When the headquarters needs to send financial data to a branch office, it breaks the data into blocks of two numbers each (e.g., account number and transaction amount). Each block is then encrypted using the Hill Cipher key. The encryption process involves multiplying the block by the Hill Cipher key modulo 26 (the number of letters in the alphabet).

Step 3: Decryption

The branch office receives the encrypted data and uses the same Hill Cipher key to decrypt it. The decryption process involves multiplying the encrypted block by the inverse of the Hill Cipher key modulo 26.