OPEN BOOK ASSIGNMENT - 01

1. Using play fair cipher, find the encrypted message for “FIREWALL” with “OCCURENCES” as key.
2. Find the ciphertext for the plaintext=” WELCOME TO PES UNIVERSITY” and consider shift index by 7 as key using shift cipher.
3. Using Rail fence cipher encrypt the message “HELLO AND WELCOME TO THE WORLD OF CRYPTOGRAPHY” and key is 5.
4. Find ciphertext for cipher system double transposition cipher using key1 “BRIDGE” key2=”OVER” for the plaintext=”THIS IS ASSIGNMENT ONE”. Decipher the cipher text back to plain text.
5. What is the difference between Known plaint text and chosen cipher text attacks.
6. Perform the encryption and decryption using hill cipher, given:

   $$\text{Key} = \begin{matrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 2 & 12 & 15 \end{matrix}$$

   Plain text: “APT”

7. The Euclidean algorithm has been known for over 2000 years and has always been a favourite among number theorists. After these many years, there is now a potential competitor, invented by J. Stein in 1961. Stein’s algorithms is as follows: Determine gcd(A, B) with A, B Ú 1.

   STEP 1 Set $A_1 = A$, $B_1 = B$, $C_1 = 1$

   STEP 2 For n > 1, (1) If $A_n = B_n$, stop. gcd(A, B) = A_nC_n

   (2) If A_n and B_n are both even, set $A_{n+1} = A_n/2$, $B_{n+1} = B_n/2$, $C_{n+1} = 2C_n$

   (3) If A_n is even and B_n is odd, set $A_{n+1} = A_n/2$, $B_{n+1} = B_n$, $C_{n+1} = C_n$

   (4) If A_n is odd and B_n is even, set $A_{n+1} = A_n$, $B_{n+1} = B_n/2$, $C_{n+1} = C_n$

   (5) If A_n and B_n are both odd, set $A_{n+1} = A_n - B_n$, $B_{n+1} = \min(B_n, A_n)$, $C_{n+1} = C_n$

   Continue to step n + 1.

   a. To get a feel for the two algorithms, compute gcd(6150, 704) using both the Euclidean and Stein’s algorithm.

   b. What is the apparent advantage of Stein’s algorithm over the Euclidean algorithm?

8. For each of the following equations, find an integer x that satisfies the equation using Chinese remainder theorem.

   a. $4x \equiv 2 \pmod{3}$

   b. $7x \equiv 4 \pmod{9}$

   c. $5x \equiv 3 \pmod{11}$