Assignment 2 from Number Theory

Deadline : One week from Today

1. Find the GCD of 2740 and 1760, using Euclidean algorithm**.**
2. Find the gcd of 42823 and 6409
3. Find the multiplicative inverse of
    a. 50 mod 71
    b. 43 mod 64
    c. Find the modular multiplicative inverse of 11 in $\mathbb{Z}_{26}$.
4. Define Finite Fields of Order *p.*
5. Define the term Irreducible polynomial and write the Irreducible polynomial used by AES in GF(8)
6. Find arithmetic multiplication in GF(2^8) for the following:
    a. {02} • {87} mod {11B}
    b. {03} •{6E} mod {11B}
    c. Compute $x^{12}+x^9+x^7+x^5+x^2$ mod $x^8+x^4+x^3+x+1$
7. For given f(x) = $x^3 + x^2$ and g(x) = $x^9 + x + 1$, find f(x) . g(x), f(x) × g(x) in GF(8).
8. Find the GCD of x2 + 7x + 6 and $x^2 - 5x - 6$ using Euclidean algorithm
9. Encrypt plaintext 'ABRA KA DABRA' with Caesar cipher with key=8 and Rail fence Cipher with rails =3 .
10. what is Hill cipher? Encrypt the message 'paymoremoney' with key given below

    17 17 5
    21 18 21
    2 2 9

11. Encrypt the text ‘welcometocryptoclass’ using the key ‘diamond’ with Playfair cipher and decrypt the resulting cipher.

12. For given 3rd round key as A2 D4 FA 22 45 657089 02 47 EA F4 64 11 44 B8, find the 4th Round key. use necessary data structures of AES.

13Find the Euler's totient function of 24.