APRIL/MAY 2019

MMA45A — NUMBER THEORY AND CRYPTOGRAPHY

Time : Three hours

Maximum : 75 marks

SECTION A — ($5 \times 6 = 30$ marks)

Answer ALL questions.

1. (a) Divide $(11001001)_2$ by $(100111)_2$ and divide $(HAPPY)_{26}$ by $(SAD)_{26}$.

Or

(b) Find an upper bound for the number of bit operations it takes to compute the binomial coefficient $\left(\dfrac{n}{m}\right)$.

2. (a) Write down the digraph transformation.

Or

(b) Working in the 26-letter alphabet, use matrix $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(Z/26Z)$. Find encipher the message unit "NO".

3. (a) Let

$f(X) = X^4 + X^3 + X^2 + 1$, $g = X^3 + 1 \in F_2[X]$, g.c.d. (f, g) using the Euclidean algorithm for polynomials and express the g.c.d. in the form $u(X)f(X) + v(X)g(X)$.

Or

(b) Prove that $(a+b)^p = a^p + b^p$ in any field of characteristic p.

4. (a) Write a short notes on Key Exchange.

Or

(b) Explain the Knapsack problem.

5. (a) Prove that If $n \equiv 3 \mod 4$, prove that n is a strong pseudo prime to the base b in and only if it is an Euler pseudo prime to the base b.

Or

(b) Prove that a Carmichael number must be the product of at least three distinct primes.

SECTION B — (3 × 15 = 45 marks)

Answer any THREE questions.

6. State and prove Chinese Remainder Theorem.

7. An enciphering matrix A in the 26-letter alphabet. We intercept the cipher text "WKNCCHSSJH". We know that the first word is "GIVE". Find the deciphering matrix A^{-1} and read the message.

8. Prove that there exists a sequence of prime p such that the probability that a random $g \in F_p^*$ is generator approaches zero.

9. Write down the algorithm for finding discrete logs in finite fields.

10. Find factor 4087 using $f(x) = x^2 + x + 1$ and $x_0 = 2$.
