(*b*) Intercept the message "! IWGVIEX! ZRADRYD", which was sent using a linear enciphering transformation of diagraph-vector in a 29-letter alphabet, in which *A*-*Z* have numerical equivalent 0-25, blank = 26, ? = 27, ! = 28. The last five letters of plain text are the sender's signature "MARIA".

(*i*) Find the deciphering matrix, and read the message.

(*ii*) Find the enciphering matrix.

6. (*a*) Let n be any square free integer. Let d and e be positive integers such that $de-1$ is divisible by $p-1$ for every prime divisor p of n. Prove that $a^{de} \equiv a \bmod n$ for any integer a.

OR

(*b*) Write short notes on the following :

(*i*) Classical versus Public Key

(*ii*) Authentication

(*iii*) Key exchange

———

2016

NUMBER THEORETIC CRYPTOGRAPHY - I

Time : Three Hours] [*Maximum Marks* : 80

The figures in the right hand margin indicate marks. Answer from both the Sections as directed.

SECTION-A

1. Answer any **four** of the following : 4×4

(*a*) Find an upper bound for the number of bit operations required to multiply a polynomial $\Sigma a_i x^i$ of degree $\leq n_1$ and a polynomial $\Sigma b_j x^j$ of degree $\leq n_2$ whose coefficients are positive integers $\leq m$. $(n_2 \leq n_1)$

(*b*) If g.c.d. $(a,m) = 1$, then show that $a^{\varphi(m)} \equiv 1 \bmod m$.

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

(*d*) Prove that 3 is a quadratic nonresidue modulo any Mersenne prime greater than 3.

(*e*) Find the inverse of $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2$ $(Z/26Z)$.

(*f*) Explain how RSA works.

OR

2. Answer all questions from the following : 2×8

(*a*) Find g.c.d (1547, 640).

(*b*) If a is not divisible by p and if $n \equiv m \bmod (p-1)$, then show that $a^n \equiv a^m \bmod p$.

(*c*) Find the value of $\left(\frac{91}{167}\right)$ using quadratic reciprocity.

(*d*) Define the Jacobi symbol.

(*e*) Find a condition on the last decimal digit of p which is equivalent to s being a square in F_p.

(*f*) Define Cryptosystem.

(*g*) How many different shift transformations are there with N-letter alphabet ?

(*h*) Define deciphering key.

SECTION-B

Answer all questions : 16×4

3. (*a*) State and prove that Fermat's little theorem.

OR

(*b*) (*i*) Define Euler phi-function and show that it is multiplicative.

(*ii*) If g.c.d. $(a,m) = 1$, then $a^{\varphi(m)} \equiv 1 \bmod m$. Justify.

4. (*a*) If F_q is a field of $q = p^f$ elements, then every element satisfies the equation $x^q - x = 0$, and Fq is precisely the set of roots of that equation. Conversely, for every prime power $q = p^f$ the splitting field over F_p of the polynomial $x^q - x$ is a field of q elements. Justify.

OR

(*b*) State and prove that the law of quadratic reciprocity.

5. (*a*) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Z/NZ)$ and set $D = ad - bc$. Then prove that the following are equivalent :

(*i*) g.c.d $(D, N) = 1$

(*ii*) A has an inverse matrix

(*iii*) If x and y are both not 0 in Z/NZ, then $A\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

(*iv*) A gives a 1 to 1 correspondence of $(Z/NZ)^2$ with itself.

OR