Cryptography Assignment

6)The polynomial x^3+x+1 is irreducible over $GF(2)(\cong F_2)$, since it is a polynomial of degree 3 so it is sufficient of check whether the roots are in $GF(2)(\cong F_2)$ by simple calculations shows that elements of $GF(2)(\cong F_2)$ i.e $0, 1$ are not the roots. Let α be the root of $x^3 + x + 1$ in some field extension K (say). Now K is a vector space over $GF(2)(\cong F_2)$ with $1, \alpha, \alpha^2$ as the basis contaning 2^3 elements.[A vector space K of dimension n over a field F containing p elements, contains p^n element, p is prime]
So, $|K| = 2^3$, therefore $K \cong GF(2^3)$ (two fields with p^n elements, p is prime are isomorphic see $Artin, Finite\ Fields\ Pg.509$ for more details)

$GF(2^3) = (0, 1, \alpha, 1 + \alpha, \alpha^2, \alpha^2 + 1, \alpha + \alpha^2, 1 + \alpha + \alpha^2)$

(Elements of $GF(2^3)$ are obtained by the linear combination of $(1, \alpha, \alpha^2)$ with coefficients from $GF(2)(\cong F_2)$ and computation is done using the relation $1 + \alpha + \alpha^2 = 0$ i.e., $modulo\ 1 + \alpha + \alpha^2$ and $1 + 1 = 0$ base field is F_2).....(i)

Ciphertext for the given plaintexts (α, α^2) is

$(\alpha, \alpha^2) \begin{pmatrix} \alpha^2 & \alpha+1 \\ \alpha^2+1 & 1 \end{pmatrix} = (\alpha^4 + \alpha^3 + \alpha^2, 2\alpha^2 + \alpha) = (1, \alpha)$[using (i)] Cipher

text is $(1, \alpha)$ corresponding to the key $\begin{pmatrix} \alpha^2 & \alpha+1 \\ \alpha^2+1 & 1 \end{pmatrix}$

$KcannotcontainallmatricesoverGF(2^3)$ (it will only contain 2X2 invertible matrices over $GF(2^3)$ this will also helps in finding the number of keys) since if we encrypt the plaintext then to get back the plaintext from the ciphertext we have to find the inverse of the given key(a 2X2 matrix over $GF(2^3)$ which is possible only if it is a invertible matrix.

All the matrix over $GF(2^3)$ are not invertible therefore the keyspace does not contain all the matrices.

7) a) For the given RSA system e has to be relatively prime with $\phi(n)$
i.e $(e, \phi(n)) = 1$,where $n = pq$ p, q are distinct large primes.
$\phi(n) = \phi(pq) = (p-1)(q-1) \Rightarrow \phi(n)$ is even so if we take the value of e to be 1004 then 2 will be a common factor of $\phi(n)$ and e thus $(e, \phi) > 2$ which is not the choice of e otherwise there would be difficulty recovering the plaintext back [note $\phi(n)$ is even for $n > 2$]

b) We know that the exponent e should be chosen with $(e, \phi(pq)) = 1$—(1) one good way of choosing e is any prime greater than p, q since it obviously satisfies (1) By whichever method we find e it must be true that $2^e > n = pq$, so that it is impossible to recover the plaintext block P, $P \neq 1, 0$ just by taking the eth root of the cipher text C with $C \equiv P^e$ $(mod$n$)$,$0 < C < n$. So if we choose e to be 3 then by taking the $3rd$ root of the cipher text we can get back the plain text without knowing the private key (d, p, q) In the given example $C = 4921675101, e = 3, n = 34968844844341$ as above we have to find the $3rd$ root of $4921675101 (= C)$ to get P which is 1701 so we get the plaintext $P = 1701$ without factorisation of $n = 34968844844341$ which is bit diffcult to do but since e was choosen small we did not required to do the factorisation to attack the given RSA with public key $(3, 34968844844341)$ and private key (p, q, d), exact value of p, q, d can be obtained only by factorisation of n to attack the RSA but in this case sice e was small we have decipher the cipher text. So we conclude that small value of e is not a good choice even if we choose large p and q primes.