Άσκηση 6 Dai16067 Κρυπτογραφία

A)

1) Ο κανόνας είναι ότι $\Phi((n)) = (p-1)(q-1)$ και $\gcd(e_i, \Phi(n)) = 1$. Το μόνο ei που ικανοποιεί και τη δεύτερη συνθήκη (του e) είναι το $e_2=49$ $\Phi(n)= (p-1)(q-1) = 40 \cdot 16 = 640 = 2\text{^}7 \cdot 5$. Επί πλέον $\gcd(e_i, \Phi(n)) = 1$ πρέπει να ικανοποιείται (που δεν ικανοποιείται σε αυτή τη περίπτωση) . Επομένως, μόνο το $e_2 = 49$ μπορεί να χρησιμοποιηθεί μόνο ως εκθέτης για το δημόσιο κλειδί καθώς ικανοποιείται κάθε συνθήκη ($\gcd(e_i, \Phi(n))=1$.Ενώ το e1=32 δεν ικανοποιεί την $2^η$ σχέση.

2) N=p*q=41*17=697

   $K_{pub} =\varphi (n, e) = (697,49)$

   Οπότε το $d=e^{-1} \bmod \varphi(n)=49^{-1} \bmod 640$.

   Με τον διευρυμένο ευκλείδειο αλγόριθμο βρίσκω το εξής:

   640=13*49+3

   49=16*3 +1 ⇔
   1=49-16*3=49-16(640-13*49)=209*49-16*640 => 49^{-1} mod 640= 209. Οπότε το ιδιωτικό κλειδί είναι $K_{pr}(p,q,d)=(41,17,209)$

B) O Bob έχει στην διάθεση του το ιδιωτικό κλειδί $K_{pr}=d$, Kpub=(e,n) δημόσιο κλειδί το οποίο είναι ευρέως γνωστό. Η Alice από την άλλη διαλέγει τυχαία κλειδί kses $y=e_{Kpub}(Kses)=K^e_{ses} \bmod n$.

$Kses=d_{Kpr}(y)=y^d \bmod n$

Η Alice καθορίζει πλήρως την επιλογή του κλειδιού Kses. Στη πράξη το kses μπορεί να είναι πολύ μεγαλύτερο από όσο χρειάζεται για ένα συμμετρικό-κλειδί αλγόριθμο.