# Ο αλγόριθμος RSA.

Ο αλγόριθμος RSA ανακαλύφθηκε το 1978 από τους Ron Rivest, Adi Shamir και Leonard Adlerman.

Ξεκινάμε με δύο μεγάλους πρώτους αριθμούς $p, q$. Διαλέγουμε $1 < e < pq$ τέτοιο ώστε $(e, (p-1)(q-1)) = 1$. Δηλαδή ένα αντιστρέψιμο στοιχείο στην πολ/κή ομάδα $\mathbb{Z}^*_{(p-1)(q-1)}$. Υπολογίζουμε τον αντίστροφο του $e \mod (p-1)(q-1)$, δηλαδή την λύση της ισοδυναμίας

$$ed \equiv 1 \mod (p-1)(q-1) = \phi(pq).$$

Η συνάρτηση απόκρυψης είναι $c(t) := t^e \mod pq$, δηλαδή κάθε ακέραιος $t$ κρυπτογραφείται στον $c(t)$. Η συνάρτηση αποκρυπτογράφησης είναι $t^d \mod pq$, δηλαδή προκειμένου να αποκρυπτογραφήσουμε το κρυπτογραφημένο μήνυμα υψώνουμε στην $d$.

Το δημόσιο κλειδί είναι το ζευγάρι $\{pq, e\}$. Το ιδιωτικό κλειδί είναι ο αριθμός $d$ το οποίο το κρατάμε μυστικό.

Το δημόσιο κλειδί το δίνουμε σε όλους, που θέλουμε να μας στείλουν ένα μήνυμα Μόλις λάβουμε ένα κρυπτογραφημένο μήνυμα το αποκρυπτογραφούμε με χρήση το κλειδιού $d$.

Η ουσία του αλγορίθμου είναι ότι ο κακόβουλος παραβιαστής του κρυπτογραφημένου μηνύματος θα πρέπει να παραγοντοποιήσει τον αριθμό $pq$ κάτι που είναι απελπιστικά χρονοβόρο.

Στην εργαστηριακή αυτή άσκηση θα πρέπει να γράψετε ένα πρόγραμμα το οποίο θα χρησιμοποιεί το μέθοδο rsa προκειμένου να κρυπτογραφηθεί ένα μήνυμα

Χρειαζόμαστε ένα τρόπο να μετατρέπουμε μια φράση κειμένου σε μια ακολουθία αριθμών. Αυτό στο pari μπορεί να υλοποιηθεί ως εξής:

Ορίζουμε μία λίστα που να περιέχει χαρακτήρες με την εντολή:

```
{alphabet=[" ","A","B","C","D","E","F","G","H","I","J","K","L","M",
           "N","O","P","Q","R","S","T","U","V","W","X","Y","Z"];
}
```

Στα στοιχεία της λίστας έχουμε πρόσβαση ως εξής:

```
alphabet[4]
%2 = "C"
```

Δηλαδή η εντολή alphabet[4] επιστρέφει το τέταρτο στοιχείο της λίστας που είναι το "C".

Γράφοντας τις εντολές

```
{lettertonumber(l,n)=
     for(n=1,27,if(alphabet[n]==l,return(n)));
     error("invalid input.")
}
```

Ορίζεται μία νέα εντολή του pari η lettertonumber. Αυτή είναι η αντίστροφη συνάρτηση του alphabet[n] και επιστρέφει τον αριθμό που αντιστοιχεί σε ένα γράμμα. Δοκιμάστε να την τεστάρετε δίνοντας

```
lettertonumber("G")
%4 = 8
```

Δηλαδή το γράμμα G βρίσκετε στην έβδομη θέση της λίστας που δημιουργήσαμε προηγουμένως. Θεωρήστε το μήνυμα προς κρυπτογράφηση: EPITHESH AYRIO TO PRWI. Το μήνυμα αυτό θα το αποθηκεύσουμε σε μία μεταβλητή

```
message=["E","P","I","T","H","E","S","H"," ","A",
"Y","R","I","O"," ","T","O"," ","P","R","W","I"]
```

Εσείς θα πρέπει να βρείτε δύο μεγάλους πρώτους $p, q$ (Η συνάρτηση prime(n) του pari, η οποία επιστρέφει τον $n$-οστό πρώτο είναι χρήσιμη για αυτό τον σκοπό). Στην συνέχεια να υπολογίσετε το δημόσιο και το ιδιωτικό κλειδί. Τέλος να φτιάξετε μια επαναληπτική διαδικασία που να διαβάζει ένα ένα τα γράμματα που έχουν αποθηκευτεί στην λίστα message να τα μετατρέπετε σε αριθμούς κάνοντας χρήση της υπορουτίνας lettertonumber, και να κρυπτογραφήσετε το μήνυμα αποθηκεύοντας το σε μία λίστα με όνομα cmessage.

Επίσης να υλοποιήσετε την αντίστροφη πορεία η οποία θα αποκρυπτογραφεί το μήνυμα διαβάζοντας τα στοιχεία της λίστας cmessage θα αποκρυπτογραφεί κάθε αριθμό και θα επιστρέφει το αντίστοιχο γράμμα που αντιστοιχεί σε αυτό τον αριθμό.

Την εργασία μπορείτε να την δουλέψετε σε τριάδες, και η ημερομηνία παράδοσης θα είναι η 15/12/2002.