Διακριτά Μαθηματικά ΙΙ

Χρήστος Νομικός

Τμήμα Μηχανικών Η/Υ και Πληροφορικής
Πανεπιστήμιο Ιωαννίνων

MMXXIII

Περιεχόμενα

Περιεχόμενα

Κρυπτογραφία

Η κρυπτογραφία χρησιμοποιείται όταν δύο άτομα θέλουν να ανταλλάξουν μηνύματα με ασφάλεια, χωρίς να μπορεί κάποιος τρίτος να τα διαβάσει, ακόμη και αν αποκτήσει πρόσβαση σε αυτά.

Για να γίνει εφικτό κάτι τέτοιο, το μήνυμα κρυπτογραφείται, δηλαδή μετασχηματίζεται, και ο αποστολέας στέλνει στον παραλήπτη το κρυπτογραφημένο μήνυμα.

Η ανάκτηση του αρχικού μηνύματος από το κρυπτογρφημένο απαιτεί μία πρόσθετη πληροφορία που είναι γνωστή στον παραλήπτη, ενδεχομένως και στον αποστολέα, αλλά δεν είναι γνωστή σε τρίτους.

Κρυπτογραφία

Οι πιο διαδεδομένες μέθοδοι κρυπτογράφησης βασίζονται στη θεωρία αριθμών.

Κρυπτογραφία

Στην κρυπτογραφία ιδιωτικού κλειδιού, δύο άτομα τα οποιά θέλουν να επικοινωνούν με ασφάλεια, μοιράζονται ένα μυστικό κλειδί.

Το μυστικό κλειδί χρησιμοποιειται για την κρυπτογράφηση και την αποκρυπτογράφηση των μηνυμάτων.

Αν υπάρχουν n άτομα που θέλουν ανά δύο να επικοινωνούν με ασφάλεια, τότε το κάθε ζεύγος θα πρέπει να έχει ένα ξεχωριστό μυστικό κλειδί.

Κρυπτογραφία

Στην κρυπτογραφία δημόσιου κλειδιού, κάθε άτομο διαθέτει δύο κλειδιά.

Το ένα κλειδί το ανακοινώνει σε όλα τα υπόλοιπα άτομα και ονομάζεται δημόσιο κλειδί.

Το άλλο το γνωρίζει μόνο το συγκεκριμένο άτομο και ονομάζεται ιδωτικό κλειδί.

Η κρυπτογράφηση ενός μηνήματος γίνεται με χρήση του δημόσιου κλειδιού. Ωστόσο η αποκρυπτογράφηση απαιτεί τη γνώση του ιδιωτικού κλειδιού.

Κρυπτογραφία

Αν ο B θέλει να στείλει ένα μήνυμα στον A, τότε το κωδικοποιεί χρησιμοποιώντας το δημόσιο κλειδί του A.

Η αποκωδικοποίηση του μηνήματος μπορεί να γίνει γρήγορα μόνο από τον A, οποίος είναι ο μόνος που γνωρίζει το ιδιωτικό κλειδί του A.

Οποιοδήποτε άλλο άτομο, ακόμη και αν αποκτήσει πρόσβαση στο κωδικοποιημένο μήνυμα δεν θα μπορέσει να το αποκωδικοποιήσει σε αποδεκτά μικρό χρονικό διάστημα.

Κρυπτογραφία

Στο σύστημα κρυπτογράφησης RSA το δημόσιο κλειδί είναι ένα ζεύγος ακεραίων αριθμών (n, e) όπου

- ο n είναι το γινόμενο δύο μεγάλων πρώτων αριθμών p και q.
- ο e είναι ένας θετικός ακέραιος αριθμός, τέτοιος ώστε $gcd(e, (p-1)\cdot(q-1)) = 1$.

Το ιδιωτικό κλειδί είναι το ζεύγος ακεραίων ακεραίων αριθμών (n, d) όπου

- ο n είναι ο ίδιος αριθμός όπως στο δημόσιο κλειδί.
- ο d είναι ο αντίστροφος του e modulo $(p-1)\cdot(q-1)$.

Σημειώνεται ότι ο αντίστροφος του e modulo $(p-1)\cdot(q-1)$ υπάρχει επειδή $gcd(e, (p-1)\cdot(q-1)) = 1$.

Ας υποθέσουμε αρχικά ότι το μήνυμα M που θέλουμε να κρυπτογραφήσουμε είναι ένας αριθμός μικρότερος του n.

Το κρυπτογραφημένο μήνυμα είναι ο αριθμός $C = M^e \bmod n$. Το C μπορεί να υπολογιστεί γρήγορα, εφαρμόζοντας τον αλγόριθμο για γρήγορη ύψωση σε εκθέτη $\bmod n$.

Το αρχικό μήνυμα προκύπτει από το κρυπτογραφημένο μήνυμα, όπως θα αποδείξουμε στο επόμενο θεώρημα, θέτοντας $M = C^d \bmod n$.

Κρυπτογραφία

Δεν υπάρχει αποδοτικός τρόπος για να ανακτηθεί το μήνυμα M από το C χωρίς να γνωρίζουμε το d.

Επίσης δεν υπάρχει αποδοτικός τρόπος να βρούμε το d χωρίς να γνωρίζουμε τους πρώτους αριθμούς p και q.

Τέλος δεν υπάρχει αποδοτικός αλγόριθμος για παραγοντοποίηση, έτσι ώστε να μπορέσουμε να βρούμε τους αριθμούς p και q γνωρίζοντας το n.

Από τα παραπάνω προκύπτει ότι μόνο ο κάτοχος του ιδιωτικού κλειδιού (n, d) μπορεί να αποκρυπτογραφήσει γρήγορα το κρυπτογραφημένο μήνυμα C.

Χωρίς τη γνώση του ιδωτικού κλειδιού ο χρόνος που απαιτείται για την αποκρυπτογράφηση είναι απαγορευτικά μεγάλος.

Θεώρημα

Έστω p, q πρώτοι αριθμοί, $n = p \cdot q$, e ένας θετικός ακέραιος αριθμός τέτοιος ώστε $gcd(e, (p-1) \cdot (q-1)) = 1$, d ο αντίστροφος του e modulo $(p-1) \cdot (q-1)$, M ένας μη αρνητικός ακέραιος μικρότερος του n και $C = M^e \bmod n$. Τότε ισχύει $M = C^d \bmod n$.

Απόδειξη

Ισχύει $e \cdot d \equiv 1 \ (mod \ (p-1) \cdot (q-1))$.

Συνεπώς $e \cdot d = 1 + k' \cdot (p-1) \cdot (q-1)$, για κάποιον ακέραιο k'.

Θέτοντας $k = k' \cdot (q-1)$, έχουμε $e \cdot d = 1 + k \cdot (p-1)$

Άρα $(M^e)^d = M^{e \cdot d} = M^{1+k \cdot (p-1)} = M \cdot M^{k \cdot (p-1)} = M \cdot (M^{p-1})^k$.

Απόδειξη

Αν $p \nmid M$, τότε

$$(M^e)^d \equiv M \cdot (M^{p-1})^k \equiv M \cdot 1^k \equiv M \ (mod\ p)$$

όπου το ότι $M^{p-1} \equiv 1 \ (mod\ p)$ προκύπτει από το μικρο θεώρημα του Fermat.

Απόδειξη

Αν $p \mid M$, τότε $p \mid (M^e)^d$ επειδή e και d είναι θετικοί αριθμοί.

Άρα $M \equiv 0 \ (mod \ p)$ και $(M^e)^d \equiv 0 \ (mod \ p)$. Συνεπώς ότι $(M^e)^d \equiv M \ (mod \ p)$.

Απόδειξη

Συνεπώς και στις δύο περιπτώσεις έχουμε $(M^e)^d \equiv M \ (mod \ p)$.

Ακριβώς με τον ίδιο τρόπο προκύπτει ότι $(M^e)^d \equiv M \ (mod \ q)$.

Άρα $p \mid ((M^e)^d - M)$ και $q \mid ((M^e)^d - M)$, που σενεπάγεται ότι οι πρώτοι αριθμοί p και q είναι πρώτοι παράγοντες του $(M^e)^d - M$.

Συνεπώς ισχύει $p \cdot q \mid ((M^e)^d - M)$, άρα $(M^e)^d \equiv M \ (mod \ p \cdot q)$.

Επειδή $n = p \cdot q$, από τα παραπάνω προκύπτει ότι
$C^d \equiv (M^e)^d \equiv M \ (mod \ n)$, που συνεπάγεται $C^d \bmod n = M$, καθώς $M < n$. □

Κρυπτογραφία

Το σύστημα RSA εκτός από την αποστολή κρυπτογραφημένων μηνημάτων, μπορεί να χρησιμοποιηθεί και για την ψηφιακή υπογραφή σε μηνήματα.

Έστω ότι ένας αποστολέας θέλει να στείλει ένα μήνημα σε πολλούς παραλήπτες. Δεν τον ενδιαφέρει να κρυπτογραφήσει το μήνημα, θέλει ωστόσο οι παραλήπτες να μπορούν να αναγνωρίσουν τη γνησιότητα του μηνήματος.

Κρυπτογραφία

Για να υπογράψει ψηφιακά ένα μήνυμα M, ο αποστολέας A αρκεί να κωδικοποιήσει το μήνυμα χρησιμοποιώντας το δικό του ιδιωτικό κλειδί.

Στη συνέχεια στέλνει στους παραλήπτες το M και το $S = M^d \bmod n$.

Ο κάθε παραλήπτης, όταν λάβει τα M και S, για να βεβαιωθεί ότι ο αποστολέας είναι πράγματι ο A, αποκωδικοποιεί το S χρησιμοποιώντας το δημόσιο κλειδί του A και το συγκρίνει με το M.

Αν ο αποστολέας είναι πράγματι ο A, τότε το μήνυμα που θα προκύψει από την αποκωδικοποίηση είναι το
$S^e \bmod n = (M^d)^e \bmod n = (M^e)^d \bmod n = M$ σύμφωνα με το προηγούμενο θεώρημα.

Κρυπτογραφία

Αν το μήνυμα που πρόκειται να κρυπτογραφηθεί δεν είναι αριθμός αλλά κείμενο που σχηματίζεται από ένα αλφάβητο Σ με $b = |\Sigma|$ σύμβολα τότε μπορούμε να θεωρήσουμε ότι τα σύμβολα του Σ αναπαριστούν τους αριθμούς $0, 1, \ldots, b-1$ και να θεωρήσουμε μία οποιαδήποτε ακολουθία συμβόλων ως την αναπαράσταση ενός αριθμού στο b-αδικό σύστημα αρίθμησης.

Για να κρυπτογραφήσουμε το κείμενο, το χωρίζουμε σε τμήματα μήκους k, όπου το k επιλέγεται έτσι ώστε ο μεγαλύτερος αριθμός μήκους k στο b-αδικό σύστημα να είναι μικρότερος του n και το k να είναι το μέγιστο με αυτή την ιδιότητα.

Συγκεκριμένα θέλουμε:

$$\begin{aligned} b^k - 1 < n \leq b^{k+1} - 1 &\Leftrightarrow b^k \leq n < b^{k+1} \\ &\Leftrightarrow k \leq \log_b n < k + 1 \\ &\Leftrightarrow k = \lfloor \log_b n \rfloor \end{aligned}$$

Αν το μήκος του μηνύματος δεν είναι πολλαπλάσιο του k τότε συμπληρώνουμε το τέλος του μηνύματος με ένα κατάλληλο πλήθος εμφανίσεων κάποιου χαρακτήρα (π.χ. κενό ή εναλλάκτικά κάποιον ειδικό χαρακτήρα που έχουμε συμπεριλάβει στο αλφάβητο για αυτό το σκοπό).

Με την παραπάνω διαδικασία έχουμε χωρίσει το αρχικό μήνυμα κειμένου T σε μία ακολουθία συμβολοσειρών $t_1, t_2, \ldots, t_\ell$, όπου το κάθε t_i έχει μήκος k.

Στη συνέχεια ερμηνεύουμε το κάθε t_i ως αριθμό στο b-δικό σύστημα αρίθμησης, θέτοντας $m_i = (t_i)_b$.

Με αυτό τον τρόπο σχηματίζεται μία ακολουθία αριθμών $m_1, m_2, \ldots, m_\ell$.

Λόγω του τρόπου επιλογής του k, κάθε αριθμός της ακολουθίας είναι μικρότερος του n.

Το κωδικοποιημένο μήνυμα αποτλείται από την ακολουθία
$m_1^e \bmod n, m_2^e \bmod n, \ldots, m_\ell^e \bmod n$

Ο παραλήπτης όταν λάβει μία ακολουθία αριθμών $c_1, c_2, \ldots, c_\ell$, πρώτα ανακτά την αρχική ακολουθία $m_1, m_2, \ldots, m_\ell$, θέτοντας $m_i = c_i^d \bmod n$.

Στη συνέχεια μετατρέπει τον κάθε αριθμό στο b-άδικό σύστημα αρίθμησης, ανακτώντας έτσι την ακολουθία $t_1, t_2, \ldots, t_\ell$.

Τέλος συνενώσει τα $t_1, t_2, \ldots, t_\ell$ για να ανακτήσει το αρχικό κείμενο.

Κρυπτογραφία

Δύο άτομα A και B μπορούν να συμφωνήσουν σε ένα κοινό μυστικό κλειδί χρησιμοποιώντας το παρακάτω πρωτόκολλο επικοινωνίας:

- Ο A και ο B επιλέγουν με κάποιον τρόπο (που δεν χρειάζεται να είναι μυστικός) έναν πρώτο αριθμό p και μία πρωταρχική ρίζα r modulo p.
- Ο A επιλέγει έναν μυστικό αριθμό a και στέλνει στον B το $r^a \bmod p$.
- Ο B επιλέγει έναν μυστικό αριθμό b και στέλνει στον A το $r^b \bmod p$.
- Ο A όταν λάβει το $r^b \bmod p$ υπολογίζει το $(r^b)^a \bmod p$, το οποίο είναι το μυστικό κλειδί
- Ο B όταν λάβει το $r^a \bmod p$ υπολογίζει το $(r^a)^b \bmod p$, το οποίο είναι το μυστικό κλειδί

Παρατηρούμε ότι

- Ο A και ο B έχουν υπολογίσει το ίδιο μυστικό κλειδί, επειδή $(r^b)^a = r^{b \cdot a} = r^{a \cdot b} = (r^a)^b$.
- Οποιοσδήποτε τρίτος, ακόμη και αν γνωρίζει τα p, r, $r^a \bmod p$, $r^b \bmod p$ δεν μπορεί να υπολογίσει σε εύλογο χρονικό διάστημα το $(r^a)^b \bmod p$, καθώς δεν υπάρχει γνωστός τρόπος για να γίνει αυτός ο υπολογισμός χωρίς να είναι γνωστά τα a και b και ο υπολογισμός των a και b ισοδυναμεί με την εύρεση διακριτών λογαρίθμων, πρόβλημα για το οποίο επίσης δεν είναι γνωστός κάποιος αποδοτικός αλγόριθμος.

Ο παρακάτω αλγόριθμος υπολογίζει το $b^n \bmod m$.

Αλγόριθμος για Γρήγορη Ύψωση σε Εκθέτη $\bmod m$

Είσοδος: θετικοί ακέραιοι αριθμοί b,n,m

```
x ← 1
p ← b mod m
a ← n mod 2
while n > 0 do
    if a = 1 then x ← x*p mod m
    p ← p*p mod m
    n ← n div 2
    a ← n mod 2
return x
```