Αριθμοθεωρητικοί Αλγόριθμοι και το Κρυπτοσύστημα RSA

Στην ενότητα αυτή θα μελετηθούν τα εξής θέματα:

Υπολογισμός Μέγιστου Κοινού Διαιρέτη

Αλγόριθμος του Ευκλείδη

Κλάσεις Ισοδυναμίας και Αριθμητική modulo n

Γραμμικές Εξισώσεις modulo n

Το Κινέζικο θεώρημα υπολοίπων

Το Κρυπτοσύστημα RSA

Κρυπτοσυστήματα

- Ένα κρυπτοσύστημα με δημόσια κλειδιά (public-key cryptosystem) επιτρέπει:
  1. την κωδικοποίηση μηνυμάτων έτσι ώστε, κάθε φορά που κάποιο μήνυμα m στέλνεται από τον Α στον Β, αν ο Γ κρυφακούσει τη συνομιλία να μην μπορεί να αποκωδικοποιήσει το m.
  2. την απλαστογράφητη ψηφιακή υπογραφή μηνυμάτων (digital signatures).

- Το κρυπτοσύστημα RSA βασίζεται στη σημαντική διαφορά μεταξύ:

  της ευκολίας με την οποία μπορούμε να βρούμε μεγάλους πρώτους αριθμούς και της δυσκολίας της παραγοντοποίησης του γινομένου δύο μεγάλων πρώτων αριθμών.

- Κάθε συμμετάσχων Α σε ένα κρυπτοσύστημα κατέχει
  1. ένα δημόσιο (κοινώς γνωστό) κλειδί P_A, και
  2. ένα μυστικό κλειδί S_A.

  τα οποία δημιουργεί ο ίδιος.

Κρυπτοσυστήματα

- Τα κλειδιά P_A και S_A χρησιμοποιούνται για κωδικοποίηση και αποκωδικοποίηση μηνυμάτων.

- Δηλαδή, αν D είναι το σύνολο όλων των μηνυμάτων, το P_A και το S_A αποτελούν 1-1 συναρτήσεις από το D στον εαυτό του και επίσης, για κάθε $m \in D$ πρέπει να ισχύει:

  $S_A(P_A(m)) = m$

  $P_A(S_A(m)) = m$

- Βασική υπόθεση: Μόνο ο Α μπορεί να υπολογίσει τη συνάρτηση S_A σε πρακτικά σύντομο χρόνο.

Κωδικοποίηση

- Έστω ότι ο Bob θέλει να στείλει στην Alice το μήνυμα m με τέτοιο τρόπο ώστε το m να είναι ακατανόητο σε οποιοδήποτε τρίτο. Τότε
  1. ο Bob βρίσκει το δημόσιο κλειδί της Alice, P_A.
  2. υπολογίζει το μήνυμα $m' = P_A(m)$, και το στέλνει στην Alice.
  3. όταν η Alice λάβει το μήνυμα m΄, χρησιμοποιεί το μυστικό της κλειδί S_A για την αποκωδικοποίηση του, $m'' = S_A(m')$.

- Προφανώς
  1. $m'' = m$, και
  2. οποιοσδήποτε τρίτος κρυφακούσει το m΄, μη κατέχοντας το S_A, δεν μπορεί να το αποκωδικοποιήσει.

Digital Signatures

- Έστω ότι η Alice θέλει να υπογράψει ένα μήνυμα m προς τον Bob. |Τότε
  1. Η Alice δημιουργεί την υπογραφή της ως $\sigma=S_A(m)$, και
  2. στέλλει στον Bob το ζεύγος (m,σ).
  3. Ο Bob λαμβάνοντας το ζεύγος (m,σ), χρησιμοποιεί το δημόσιο κλειδί της Alice, P_A, και υπολογίζει το $m'=P_A(\sigma)$.
  4. Αν $m=m'$ τότε συμπεραίνει πως το μήνυμα πράγματι στάλθηκε από την Alice.

- Ορθότητα;
- Οι δύο τεχνικές μπορούν να χρησιμοποιηθούν ταυτόχρονα για να σταλούν κωδικοποιημένα και υπογραμμένα μηνύματα;
- Πρόκληση: πως μπορούμε να διαλέξουμε κατάλληλα συναρτήσεις (κλειδιά) S_A, P_A που να ικανοποιούν τις προδιαγραφές;

Βασικές Έννοιες

$Z = \{\ldots,-2,-1,0,1,2,\ldots\}$ σύνολο *ακεραίων* αριθμών

$N = \{0,1,2,\ldots\}$ σύνολο *φυσικών* αριθμών

$d \mid a$: ο ακέραιος d διαιρεί τον ακέραιο α, δηλ. $\exists$ ακέραιος k τέτοιος ώστε $a = d \cdot k$. Ο a είναι πολλαπλάσιο του d.

$d \nmid a$: ο d δεν διαιρεί τον a

- Αν $a > 0$ και $d \mid a$, τότε $|d| \leq a$.
- Αν $d \geq 0$ και $d \mid a$, τότε λέμε ότι ο d είναι *διαιρέτης* του a.
- Κάθε ακέραιος a έχει τους *τετριμμένους διαιρέτες* a και 1. Οι μη-τετριμμένοι διαιρέτες του a λέγονται οι *παράγοντες* του a.
- Ένας ακέραιος $a>1$ του οποίου οι μόνοι διαιρέτες είναι οι τετριμμένοι διαιρέτες 1 και a λέγεται *πρώτος* αριθμός.
- Ένας ακέραιος $a>1$ είναι *σύνθετος* αριθμός αν δεν είναι πρώτος.

Βασικές Έννοιες

- Πρώτοι αριθμοί : 2,3,5,7,11,13,17,19,23,29,…
- Ο ακέραιος 39 είναι σύνθετος, αφού $3 \mid 39$.

ΘΕΩΡΗΜΑ ΤΗΣ ΔΙΑΙΡΕΣΗΣ

Για κάθε ακέραιο a και θετικό ακέραιο n, υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε $0 \leq r < n$ και $a = qn + r$.

- q : *πηλίκο* της διαίρεσης του a δια n
- $r = a \bmod n$: *υπόλοιπο* της διαίρεσης του a δια n
- $n \mid a \Leftrightarrow a \bmod n = 0$

ΟΡΙΣΜΟΣ

Αν $a \bmod n = b \bmod n$, γράφουμε

$a \equiv b \pmod n$

ο a είναι ισοδύναμος με τον b modulo n.

Βασικές έννοιες

- Έχουμε $a \equiv b \pmod{n} \Leftrightarrow n \mid a-b$

Παραδείγματα

1. $61 \equiv 6 \pmod{11}$, αφού $61 = 5 \cdot 11 + 6$ και $6 = 0 \cdot 11 + 6$
2. $-13 \equiv 22 \pmod{5}$, αφού $-13 = (-3) \cdot 5 + 2$ και $22 = 4 \cdot 5 + 2$

Μέγιστος Κοινός Διαιρέτης

- Αν ο d είναι διαιρέτης του a και επίσης διαιρέτης του b, τότε ο d είναι *κοινός διαιρέτης* των a και b.

- *Αν d | a και d | b τότε d |(a+b) και d |(a-b).*

  Απόδειξη:

  $d|a \Rightarrow a = kd$

  $\Rightarrow \quad a+b= (k+m)d, \qquad a-b=(k-m)d$

  $d|b \Rightarrow b = md$

- Πιο γενικά: *Αν d | a και d | b τότε d |(ax+by) για οποιουσδήποτε ακεραίους x και y.*

- Έστω ακέραιοι a και b, $a\neq0$ ή $b\neq0$. Ο *μέγιστος κοινός διαιρέτης* ΜΚΔ(a,b) των a και b είναι ο μεγαλύτερος από τους κοινούς διαιρέτες των a και b.

Μέγιστος Κοινός Διαιρέτης

- Παραδείγματα

  ΜΚΔ(24,30)=6 ΜΚΔ(5,7)=1 ΜΚΔ(0,9)=9

- Αν $a \neq 0$ ή $b \neq 0$, τότε $1 \leq$ ΜΚΔ$(a,b) \leq \min\{|a|,|b|\}$

Ιδιότητες του μέγιστου κοινού διαιρέτη

1. ΜΚΔ(a,b) = ΜΚΔ(b,a)
2. ΜΚΔ(a,b) = ΜΚΔ(-a,b)
3. ΜΚΔ(a,b) = ΜΚΔ(|a|,|b|)
4. ΜΚΔ(a,0) = |a|
5. ΜΚΔ(a,ka) = |a| για κάθε $k \in Z$

- Δύο ακέραιοι a και b λέγονται *σχετικά πρώτοι* αν ΜΚΔ(a,b)=1.

Μέγιστος Κοινός Διαιρέτης

ΘΕΩΡΗΜΑ 1

Έστω ακέραιοι a και b, $a \neq 0$ ή $b \neq 0$. Τότε ο ΜΚΔ(a,b) είναι το ελάχιστο θετικό στοιχείο του συνόλου $\{ax + by \mid x,y \in Z\}$ των γραμμικών, ακεραίων συνδυασμών των a και b.

ΠΟΡΙΣΜΑ 1

Για κάθε ακέραιους a και b αν $d \mid a$ και $d \mid b$, τότε $d \mid$ ΜΚΔ(a,b).

ΠΟΡΙΣΜΑ 2

ΜΚΔ(na,nb) = n·ΜΚΔ(a,b) για κάθε ακεραίους a και b και μη αρνητικό ακέραιο n.

ΠΟΡΙΣΜΑ 3

Για κάθε θετικούς ακέραιους n, a, και b αν $n|ab$ και ΜΚΔ(a,n)=1, τότε $n|b$.

Υπολογισμός μέγιστου κοινού διαιρέτη

- Έστω

$$a = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}, \qquad b = p_1^{f_1} p_2^{f_2} \ldots p_r^{f_r}$$

οι παραγοντοποιήσεις σε πρώτους ακεραίους των a και b.

- Τότε:

$$MK\Delta(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \ldots p_r^{\min(e_r,f_r)}$$

- Ο παραπάνω τύπος δείχνει ότι για να υπολογίσουμε τον μέγιστο κοινό διαιρέτη δύο ακεραίων αρκεί να τους παραγοντοποιήσουμε. Οι καλύτεροι αλγόριθμοι παραγοντοποίησης που είναι γνωστοί σήμερα δεν τρέχουν σε πολυωνυμικό χρόνο. Έτσι ο αλγόριθμος υπολογισμού του μέγιστου κοινού διαιρέτη μέσω της αναγωγής σε παραγοντοποίηση δεν θεωρείται πιθανό να δώσει ταχύ (πολυωνυμικό) αλγόριθμο.

Υπολογισμός ΜΚΔ

ΘΕΩΡΗΜΑ 2 (Θεώρημα αναδρομής μέγιστου κοινού διαιρέτη).
Για κάθε μη αρνητικό ακέραιο a και θετικό ακέραιο b,
ΜΚΔ(a,b) = ΜΚΔ(a mod b, b)

ΑΠΟΔΕΙΞΗ

ΛΗΜΜΑ 1 ΜΚΔ(a,b) | ΜΚΔ(a mod b, b).

ΑΠΟΔΕΙΞΗ

Έστω d=ΜΚΔ(a,b). Τότε d | a και d | b.

Αφού a mod b = a - ⌊a/b⌋·b, ο ακέραιος a mod b είναι *γραμμικός ακέραιος συνδυασμός* των a και b, έπεται ότι d | a mod b.

Αφού d|b και d | a mod b, έπεται από το Πόρισμα 1, ότι
d = ΜΚΔ(a,b) | ΜΚΔ(b, a mod b).

Υπολογισμός ΜΚΔ

ΛΗΜΜΑ 2 ΜΚΔ(a mod b, b) | ΜΚΔ(a,b).

ΑΠΟΔΕΙΞΗ

Έστω d = ΜΚΔ(a mod b,b). Τότε d | a mod b και d | b.

Αφού a = ⌊a/b⌋b + (a mod b), ο a είναι *γραμμικός ακέραιος συνδυασμός* των b και a mod b. Αφού d | a mod b και d | b, έπεται ότι d | a.

Συνεπώς d = ΜΚΔ(a mod b, b) | ΜΚΔ(a,b).

- Από τα Λήμματα 1 και 2, έχουμε
  ΜΚΔ(a mod b, b) = ΜΚΔ(a,b).

- Ο αλγόριθμος του Ευκλείδη είναι άμεση συνέπεια του Θεωρήματος 2.

Αλγόριθμος του Ευκλείδη

```
int GCD (int a, int b)
  if b == 0
      return a
  else
      return GCD(b,a mod b);
```

ΠΑΡΑΔΕΙΓΜΑ

ΜΚΔ(30,21) = ΜΚΔ(21,9)= ΜΚΔ(9,3)= ΜΚΔ(3,0)= 3

ΟΡΘΟΤΗΤΑ

Έπεται από το Θεώρημα 2 και το γεγονός ότι ΜΚΔ(a,0) = a.

ΤΕΡΜΑΤΙΣΜΟΣ

Έπεται από το ότι a > b $\Rightarrow$ a mod b < a.

Έτσι αφού ο ένας ακέραιος μειώνεται αυστηρά σε κάθε δεύτερη αναδρομή, η αναδρομή τελικά θα τερματίσει.

Ανάλυση χρονικής πολυπλοκότητας

- Υποθέτουμε, χωρίς βλάβη της γενικότητας, ότι $a > b \geq 0$. Ο συνολικός χρόνος που παίρνει ο αλγόριθμος του Ευκλείδη για να τερματίσει είναι ανάλογος του αριθμού των αναδρομών που εκτελούνται.

- Υπενθύμιση: Οι αριθμοί Fibonacci ορίζονται ως εξής:

  $F[0] = 0$ $\qquad\qquad$ $F[1] = 1$

  $F[i] = F[i-1] + F[i-2], \quad i \geq 2$

ΛΗΜΜΑ 2

Αν $a > b \geq 0$ και εκτελεσθούν k αναδρομές κατά την εκτέλεση του αλγορίθμου του Ευκλείδη πάνω στα a και b, τότε $a \geq F[k+2]$ και $b \geq F[k+1]$.

ΘΕΩΡΗΜΑ 3 (Θεώρημα του Lame)

Για κάθε ακέραιο $k \geq 1$, αν $a > b \geq 0$ και $b < F[k+1]$, τότε ο αλγόριθμος του Ευκλείδη κάνει λιγότερες από k αναδρομικές κλήσεις πάνω στα a και b.

Ανάλυση χρονικής πολυπλοκότητας

- Είναι πολυωνυμικός ο αλγόριθμος του Ευκλείδη;
- Αφού,

$$b < F[k+1] \approx \frac{\phi^{k+1}}{\sqrt{5}}, \quad \text{οπου} \quad \phi = \frac{1+\sqrt{5}}{2}$$

$$\lg b \approx (k+1)\lg\phi - \lg\sqrt{5},$$

$$k \in O(\lg b),$$

- και ο αριθμός των επαναλήψεων είναι γραμμικός στο μήκος εισόδου.
- Πάνω σε δυο αριθμούς με β bits ο καθένας, ο αλγόριθμος του Ευκλείδη θα στοιχίσει O(β) αριθμητικές πράξεις και $O(\beta^3)$ πράξεις πάνω σε bits, υποθέτοντας ότι ο πολλαπλασιασμός και η διαίρεση αριθμών με β bits ο καθένας παίρνουν $O(\beta^2)$ δυαδικές πράξεις.

Γενικευμένος Αλγόριθμος του Ευκλείδη

- Μπορούμε να γενικεύσουμε τον αλγόριθμο του Ευκλείδη έτσι ώστε να υπολογίζει, όχι μόνο τον d=ΜΚΔ(a,b), αλλά και τις τιμές x, y για τις οποίες d=ax+by.

```
int Extended_GCD(int a, int b)
  if b == 0
     return (a,1,0)
  else
     (d',x',y')=Extended_GCD(b,a mod b);
     (d,x,y)=(d',y',x'-⌊a/b⌋y');
      return (d,x,y)
```

- Ορθότητα;
- Χρονική Πολυπλοκότητα;

Κλάσεις Ισοδυναμίας modulo n

- Για κάθε ακέραιο n>0, το σύνολο των ακεραίων μπορεί να διαιρεθεί σε n κλάσεις ισοδυναμίας ανάλογα με το υπόλοιπο της διαίρεσης τους δια n.
- Η *κλάση της ισοδυναμίας modulo n* που περιέχει ένα ακέραιο a είναι το σύνολο
$$[a]_n = \{a + kn \mid k \in Z\}$$
- Το σύνολο όλων των κλάσεων ισοδυναμίας modulo n συμβολίζεται σαν
$$Z_n = \{[a]_n \mid 0 \le a \le n-1\}$$
- Κάθε κλάση
$$[0]_n, [1]_n, ..., [n-1]_n$$
αντιπροσωπεύεται από το ελάχιστο μη αρνητικό της στοιχείο 0, 1,…, n-1.
- Έτσι γράφουμε $Z_n = \{0,1,..., n-1\}$

Αριθμητική modulo n

- Μια *ομάδα* $(S,\oplus)$ είναι ένα σύνολο S μαζί με μια δυαδική πράξη $\oplus$ τα οποία ικανοποιούν τις πιο κάτω ιδιότητες:
  1. για κάθε $a,b \in S$, $a \oplus b \in S$
  2. υπάρχει $e \in S$ τέτοιο ώστε $a \oplus e = e \oplus a = a$
  3. για κάθε $a,b,c \in S$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
  4. για κάθε $a \in S$, υπάρχει $b \in S$ τέτοιο ώστε $a \oplus b = b \oplus a = e$
- Μια ομάδα ονομάζεται *Abelian ομάδα* αν για κάθε $a,b \in S$, $a \oplus b = b \oplus a$.
- Παραδείγματα:
  1. Το ζεύγος $(Z,+)$ είναι Abelian ομάδα.
  2. Το ζεύγος $(\{A \mid A \subseteq X\}, \cup)$;
- Παρατήρηση: Αν $a \equiv a' \pmod n$ και $b \equiv b' \pmod n$, τότε $a+b \equiv a'+b' \pmod n$ και $a \cdot b \equiv a' \cdot b' \pmod n$

Αριθμητική modulo n

- Ορίζουμε τις πράξεις $+_n$ (πρόσθεση modulo n) και $\cdot_n$ (πολλαπλασιασμός modulo n) πάνω στο σύνολο ως εξής:

$$[a]_n +_n [b]_n = [a+b]_n$$

$$[a]_n \cdot_n [b]_n = [a \cdot b]_n$$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

ΘΕΩΡΗΜΑ 4

- Το ζεύγος $(Z_n, +_n)$ είναι Abelian ομάδα.

Αριθμητική modulo n

- Ορίζουμε ως Z_n^* το υποσύνολο του που περιέχει τα στοιχεία του Z_n που είναι σχετικά πρώτα με το n:

$$Z_n^* = \{[a] \in Z_n \mid \text{ΜΚΔ}(a,n) = 1\}$$

- Για παράδειγμα: $Z_{15}^* = \{1,2,4,7,8,11,13,14\}$

$\cdot_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Αριθμητική modulo n

ΘΕΩΡΗΜΑ 5 Το ζεύγος $(Z_n^*, \cdot_n)$ είναι μια Abelian ομάδα.

- Ονομάζουμε την ομάδα $(Z_n^*, \cdot n)$ *πολλαπλασιαστική ομάδα modulo n*.
- Το μέγεθος του συνόλου Z_n^*, $|Z_n^*|$ δίνεται από τη συνάρτηση ϕ του Euler:

$$\phi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p})$$

όπου ο p παίρνει τιμές από τους περιττούς παράγοντες του n.

- Παράδειγμα:

ϕ(15)=15(1-1/3)(1-1/5)=2·4=8

- Αν ο p είναι πρώτος αριθμός τότε

ϕ(p) =

Γραμμικές Εξισώσεις modulo n

- Πρόβλημα: Με δεδομένα τιμές a, b, n, πως μπορούμε να βρούμε όλες τις τιμές x για τις οποίες

  $ax \equiv b \pmod{n}$;

ΘΕΩΡΗΜΑ 6

Έστω d=ΜΚΔ(a,n) και d=ax'+ny'. Η εξίσωση $ax \equiv b \pmod{n}$ έχει λύση μόνο όταν ο d | b και οι λύσεις της εξίσωσης είναι ακριβώς οι:

$$x_0 = x' \cdot (b/d) \bmod n$$

$$x_i = (x_0 + i \cdot (n/d)) \bmod n, \qquad 1 \le i \le d-1$$

- Αν b=1, δηλαδή αν $ax \equiv 1 \pmod{n}$, τότε ονομάζουμε το x *πολλαπλασιαστικό αντίστροφο* του a modulo n.

ΠΟΡΙΣΜΑ 4

Για κάθε n>1, αν ΜΚΔ(a,n)=1, τότε η εξίσωση $ax \equiv 1 \pmod{n}$ έχει ακριβώς μια λύση modulo n. Διαφορετικά δεν έχει καμιά λύση.

Γραμμικές Εξισώσεις modulo n

ΑΛΓΟΡΙΘΜΟΣ

```
LE_Solver(a,b,n){
  (d,x',y')=Extended_GCD(a,n);
  if (d | b)
      x[0] = x'(b/d) mod n;
      for (i=1; i<d; i++)
            x[i] = (x[0]+i(n/d))mod n
  else
      no solutions
```

Χρονική Πολυπλοκότητα: O(lg n + ΜΚΔ(a,n))

Το Κινέζικο θεώρημα υπολοίπων

- Μας επιτρέπει
  - Αν $n=n_1 \cdot n_2 \cdot \ldots \cdot n_k$ να περιγράψουμε μια 1-1 ισοδυναμία μεταξύ των δομών Z_n και $Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{nk}$. Δηλαδή, πράξεις στην πρώτη ομάδα μπορούν να επιτευχθούν ως πράξεις στη δεύτερη ομάδα.

- Σαν αποτέλεσμα, μπορούμε να σχεδιάσουμε αποδοτικότερους αλγόριθμους για πράξεις modulo n, δουλεύοντας modulo $n_i < n$.

ΘΕΩΡΗΜΑ

Έστω $n=n_1 \cdot n_2 \cdot \ldots \cdot n_k$, όπου οι n_i είναι μεταξύ τους σχετικά πρώτοι, τότε, για κάθε ακέραιο x και a,

$$x \equiv a \pmod{n_i} \text{ για } 1 \le i \le k \iff x \equiv a \pmod{n}.$$

Υπολογισμός δυνάμεων στην Z_n

- Σε πολλές περιπτώσεις είναι χρήσιμο να υπολογίσουμε την ακολουθία δυνάμεων ενός ακέραιου modulo n:

$$a^0, a^1, a^2, a^3, \ldots \qquad a \in Z_n^*$$

π.χ.

i	0	1	2	3	4	5	6	7	…
$3^i \bmod 7$	1	3	2	6	4	5	1	3	…

Θεώρημα του Euler

Για κάθε n>1 $\quad a^{\phi(n)} \equiv 1 \pmod{n}, \qquad \forall a \in Z_n^*$

Θεώρημα του Fermat

Αν ο p είναι πρώτος αριθμός, τότε $\quad a^{p-1} \equiv 1 \pmod{p}, \qquad \forall a \in Z_p^*$

- Ο πιο κάτω αλγόριθμος υπολογίζει την τιμή $a^b \bmod n$

Υπολογισμός δυνάμεων στην Z_n^*

```
Modular_Exponentiation(a,b,n)
   c=0;
   d=1;
   <b[k],…,b[1],b[0]> = η τιμή του b στο δυαδικό σύστημα
  for (i=k, i≥0, i--){
       c = 2c;
       d = d·d mod n
       if b[i]==1
              c = c+1;
              d = d·a mod n
   return d
```

Ορθότητα

- Ανά πάσα στιγμή η τιμή του d είναι ίση με $a^c \bmod n$
- Στο τέλος της διαδικασίας c = b. Άρα το ζητούμενο έπεται.

Χρονική Πολυπλοκότητα

- Αν οι a, b, n έχουν β bits ο καθένας, τότε η διαδικασία απαιτεί $O(\beta^3)$ βήματα.

Το Κρυπτοσύστημα RSA

- Στο κρυπτοσύστημα RSA, κάθε συμμετάσχων δημιουργεί τα κλειδιά του ως εξής:

1. Διάλεξε δύο μεγάλους πρώτους αριθμούς p και q (με ≈100 ψηφία ο καθένας).
2. Υπολόγισε τον $n=pq$.
3. Διάλεξε ένα μικρό περιττό ακέραιο, e, ο οποίος είναι σχετικά πρώτος με τον $\phi(n) = (p-1)(q-1)$.
4. Υπολόγισε το πολλαπλασιαστικό αντίστροφο modulo $\phi(n)$ του e, και ονόμασε το d.
5. Γνωστοποίησε το ζεύγος (e,n) ως το δημόσιο σου κλειδί.
6. Κράτα το ζεύγος (d,n) ως το μυστικό σου κλειδί.

Το Κρυπτοσύστημα RSA

- Θεωρούμε ότι $D=Z_n$
- Η συνάρτηση $P=(e,n)$ ορίζεται ως: $P(M) = M^e \bmod n$
- Η συνάρτηση $S=(d,n)$ ορίζεται ως: $S(C) = C^d \bmod n$
- Οι συναρτήσεις P και S ικανοποιούν τις απαιτούμενες προδιαγραφές;
- Θέλουμε:
  1. $P(S(M)) = M$, $S(P(M)) = M$
  2. Η τιμή του S (δηλαδή του d) να μην είναι υπολογίσιμη σε πολυωνυμικό χρόνο.

ΘΕΩΡΗΜΑ

$P(S(M)) = M$, $S(P(M)) = M$

Το Κρυπτοσύστημα RSA

ΑΠΟΔΕΙΞΗ

- Από τους ορισμούς των P και S, έχουμε $P(S(M)) = S(P(M)) = M^{ed} \bmod n$
- Αφού οι e και d είναι πολλαπλασιαστικά αντίστροφοι modulo $\phi(n)$, τότε
  $ed = 1 + k(p-1)(q-1)$ για κάποιο ακέραιο k.
- Υπάρχουν δύο περιπτώσεις:
  1. Αν $M \equiv 0 \pmod p$, τότε $\equiv M \pmod p$.
  2. Διαφορετικά από το Θεώρημα του Fermat,
     $$M^{ed} \equiv (M(M)^{p-1})^{k(q-1)} \pmod p$$
     $$\equiv M\,(1)^{k(q-1)} \pmod p$$
     $$\equiv M \pmod p$$
- Παρόμοια μπορεί να δειχθεί ότι $M^{ed} \equiv M \pmod q$.
- Από το Πόρισμα του Κινέζικου Θεωρήματος Υπολοίπου,
  $M^{ed} \equiv M \pmod n$ όπως χρειάζεται.

Το Κρυπτοσύστημα RSA

ΟΡΘΟΤΗΤΑ

- Προφανώς, αν η παραγοντοποίηση μεγάλων αριθμών ήταν πρακτικά δυνατή, τότε κάποιος θα μπορούσε να ‘σπάσει’ το κρυπτοσύστημα (παραγοντοποιώντας τον n και βρίσκοντας αρχικά τον $\phi(n)$ και στη συνέχεια τον d από τους e και $\phi(n)$).
- Μέχρι σήμερα η θεωρία και η τεχνολογία δεν επιτρέπουν γρήγορη παραγοντοποίηση.
- Επίσης, μέχρι σήμερα δεν έχει βρεθεί άλλος τρόπος για αποκωδικοποίηση μηνυμάτων που δεν περιέχει εύρεση των παραγόντων p και q.

ΠΟΛΥΠΛΟΚΟΤΗΤΑ

- Παράγοντες που επηρεάζουν τη χρονική πολυπλοκότητα της μεθόδου είναι
- Για δημιουργία κλειδιών
  - πολυπλοκότητα εύρεσης μεγάλων πρώτων αριθμών
  - πολυπλοκότητα λύσης γραμμικής εξίσωσης
- Για (απο)κωδικοποίηση μηνυμάτων
  - Υπολογισμός δυνάμεων, ο οποίος εξαρτάται από το μέγεθος του μηνύματος και τον n.