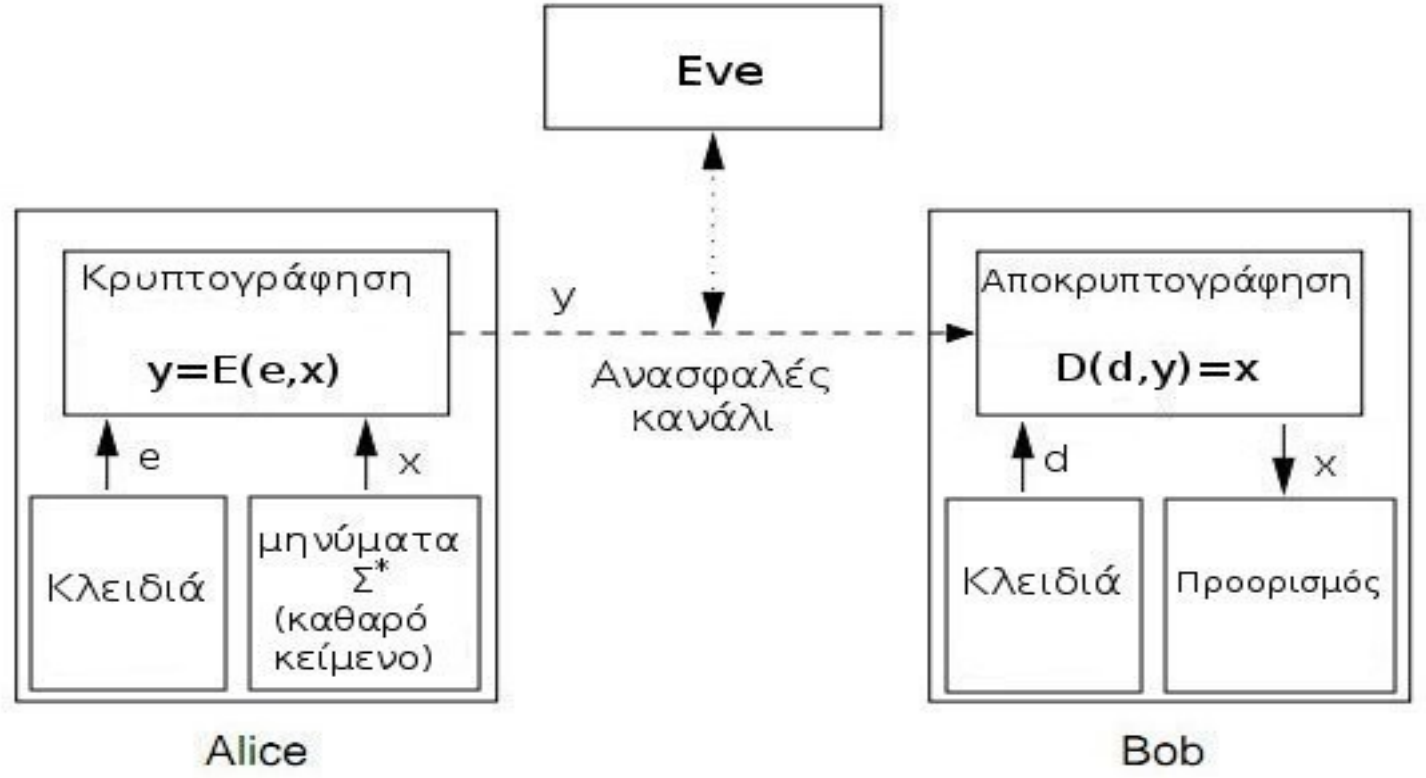
Chapter 12
Cryptography

Σακαβάλας Δημήτρης

ΔΠΜΣ “Εφαρμοσμένες μαθηματικές επιστήμες”

Σχηματική αναπαράσταση κρυπτοσυστήματος



- **Κλειδί κρυπτογράφησης** : e
- **Κλειδί αποκρυπτογράφησης** : d (*ιδιωτικό*)
- **Αλγόριθμος κρυπτογράφησης** : E (δημόσιος)
- **Αλγόριθμος αποκρυπτογράφησης** : D (δημόσιος)
- Πρόβλημα ***Π*** **(**" Σπάσιμο" κρυπτοσυστήματος**) :** Εξαγωγή του x από y χωρίς γνώση του d.

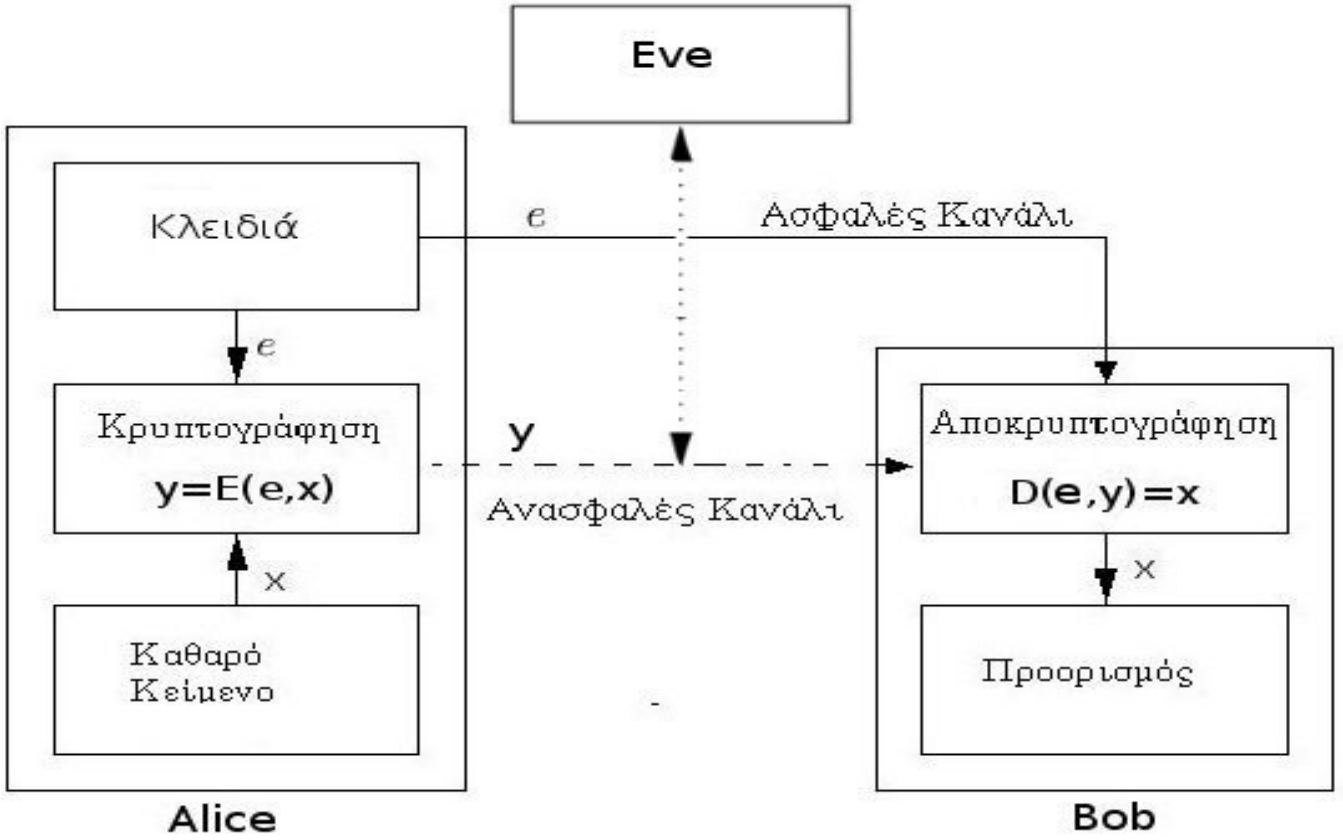
Ζητούμενες Ιδιότητες

i) E,D **πολυωνυμικοί αλγόριθμοι(συναρτήσεις)**

ii) Διαλέγουμε τα e,d έτσι ώστε **D αντίστροφη της E**, δηλαδή **D(d,E(e,x))=x.**

iii) **Η Eve** δεν μπορεί να λύσει το **Π.**

Συμμετρικά κρυπτοσυστήματα (ιδιωτικού κλειδιού)



- Κλειδί αποκρυπτογράφησης/κρυπτογράφησης ταυτίζονται : **d=e** (*ιδιωτικά*)
- *Μειονέκτημα* : Η ανταλλαγή του κλειδιού e είναι ασφαλής ;

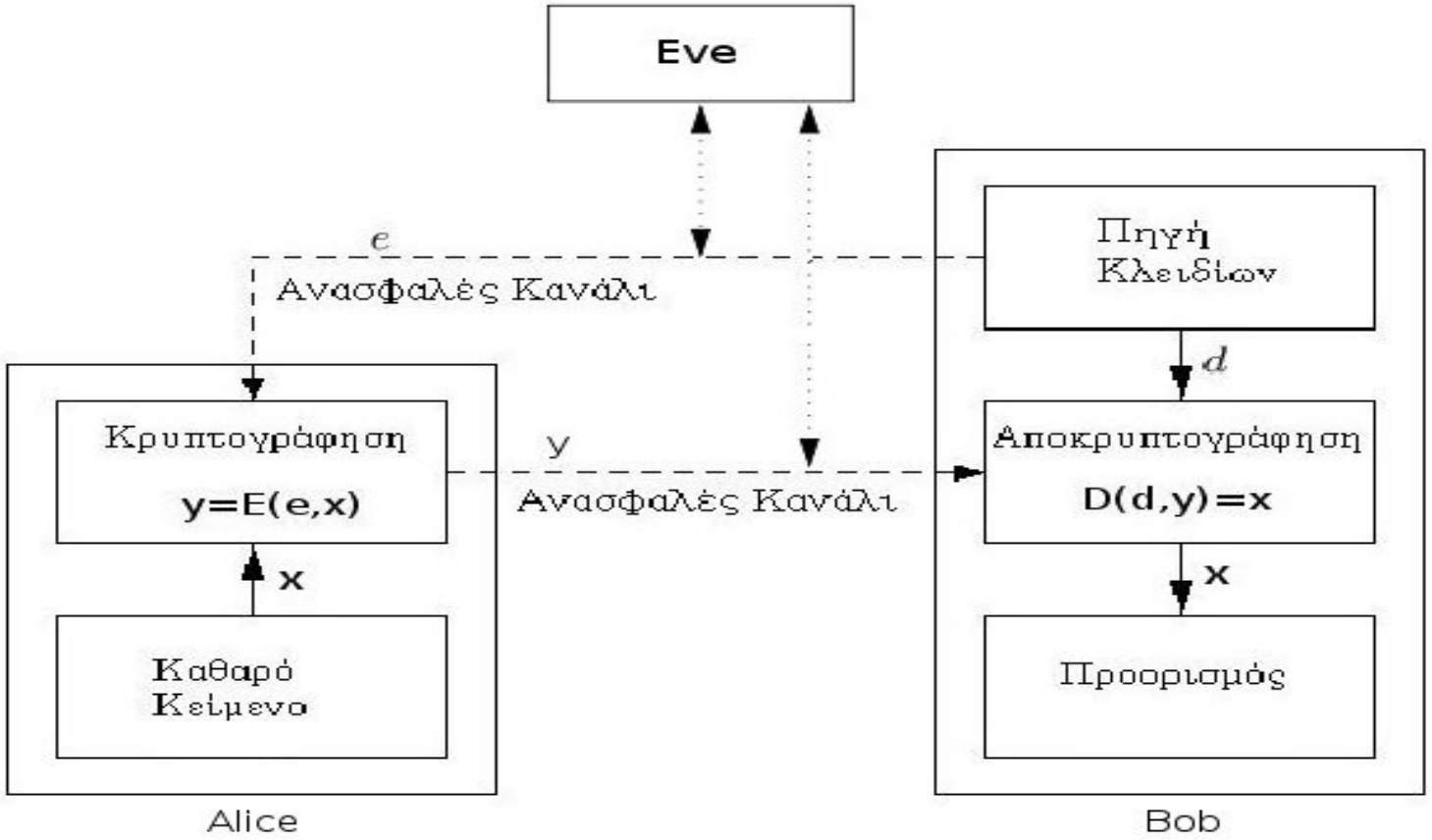
π.χ.(One time pad)

- y=E(e,x)= x ⊕ e (Όπου |e|=|x|) .
- D(e,y)= y ⊕ e =(x ⊕ e)⊕ e=x .
- Ισχύει Ιδιότητα (iii) επειδή : e = x ⊕ y .

$$\left.\begin{matrix} x=01101 \\ e=10011 \end{matrix}\right\} \Rightarrow y=E(e,x)=x\oplus e=11110$$

D(e,y)=y⊕e=01101=x

Ασύμμετρα κρυπτοσυστήματα (δημοσίου κλειδιού)



- **d** : *ιδιωτικό*
- **e :** *δημόσιο*

Παρατηρήσεις

- Δεν χρειαζόμαστε ασφαλή δίαυλο επικοινωνίας.
- Ζητούμενες ιδιότητες (i),(ii),(iii) και επιπλέον:

  (iv) **Η Eve** δεν μπορεί να εξάγει **το d από το e** (Γιατί τότε θα υπολόγιζε D(d,y)=x).
- ***Π*** ∈ **FNP**

  Μαντεύω ένα x(το μήνυμα) και ελέγχω αν E(e,x)=y σε πολυωνυμικό χρόνο.

Συναρτήσεις μονής κατεύθυνσης (One way functions)

Παρατήρηση

- Αναγκαία συνθήκη για ύπαρξη ασφαλούς κρυπτοσυστήματος: **P ≠ NP**

Επειδή αν P = NP $\Leftrightarrow$ FP = FNP $\overset{\Pi \in FNP}{\Rightarrow} \Pi \in$ FP

Ορισμός (one way function)

Έστω συνάρτηση **f από string σε string**. Είναι one way function αν ισχύουν τα παρακάτω :

i) H f είναι **1-1** συνάρτηση και $\forall\, x \in \Sigma^*, |x|^{1/k} \leqslant |f(x)| \leqslant |x|^k$, *για κάποιο* $k > 0$.
(πολυωνυμική διαφορά μήκους string).

ii) $f \in FP$, δηλαδή υπολογίζεται σε πολυωνυμικό χρόνο.

iii) $f^{-1} \notin FP$.

Παρατηρούμε ότι $f^{-1} \in FNP$ γιατί μπορούμε να μαντέψουμε ένα x και μετά να ελέγξουμε αν f(x)=y.

Υποψήφιες one way function

(1) $f_{mult}(p,q) = p \cdot q$, *όπου p,q πρώτοι (για να είναι η συνάρτηση 1-1).*

- $f_{mult} \in FP$ *(πολλαπλασιασμός δύο ακεραίων)*
- Πιθανόν $f_{mult}^{-1} \notin FP$ *(παραγοντοποίηση)*

- Δεν υπάρχει πολυωνυμικός αλγόριθμος για παραγοντοποίηση.
- *Υπάρχει υποεκθετικός αλγόριθμος -**Number field sieve** με πολυπλοκότητα* $L_{pq}[1/3, c]$.
- Πολυωνυμικός αλγόριθμος για κβαντικούς υπολογιστές (Shor).

Υποψήφιες one way function

(2) $f_{\exp}(p,r,x)=(p,r,r^x \bmod p)$, όπου p: πρώτος , r : πρωταρχική ρίζα modulo p, x<p .

- $f_{\exp}\in FP$ (ύψωση σε δύναμη modp με square and multiply).
- Πιθανόν $f_{mult}^{-1}\notin FP$ (διακριτός λογάριθμος).

-Δεν υπάρχει πολυωνυμικός αλγόριθμος για εύρεση διακριτού λογαρίθμου.
*-Υπάρχει υποεκθετικός αλγόριθμος – **Index Calculus** με πολυπλοκότητα* $L_p[1/3,c]$.

Κρυπτοσύστημα RSA

- **p,q** : πρώτοι
- **e** : ΜΚΔ(e , φ(pq))=1 (πρώτοι μεταξύ τους) ,όπου $\varphi(pq)=pq(1-\frac{1}{p})(1-\frac{1}{q})=pq-p-q+1$.
- **d** : ο αντίστροφος του e modulo φ(pq). Δλδ **e·d=1 modφ(pq)**. Υπάρχει λογω του ΜΚΔ(e , φ(pq))=1.
- 0< **x** <pq : το μήνυμα

$$f_{RSA}(x,e,p,q)=(x^e \bmod pq, pq, e)$$

Δημιουργία κρυπτοσυστήματος δημοσίου κλειδιού μέ βάση την f_{RSA} .

- **Ιδιωτικό κλειδί** κλειδί του Bob : **(p,q,d)** -(Ο Bob υπολογίζει το d ξέροντας το φ(pq) με Ευκλείδιο αλγόριθμο)
- **Δημόσιο κλειδί** του Bob : **(pq,e)**
  1) Η Alice κρυπτογραφεί το μήνυμα x κάνοντας : $y=x^e \bmod pq$
  2) Ο Bob αποκρυπτογραφεί το y κάνοντας : $y^d=x^{e\cdot d}=x^{1+k\cdot\varphi(pq)}=x \bmod pq$ (η f_{RSA} *είναι 1-1)*

Παρατήρηση: (**Πρόβλημα αντιστροφής της f_{RSA}) ≤$_p$ (Πρόβλημα παραγοντοποίησης)**

- Παραγοντοποιώ το pq και βρίσκω τα p,q .
- Υπολογίζω φ(pq)=pq-p-q+1.
- Βρίσκω το d και αποκρυπτογραφώ όπως ο Bob : $x=y^d \bmod pq$

Κρυπτογραφία και πολυπλοκότητα

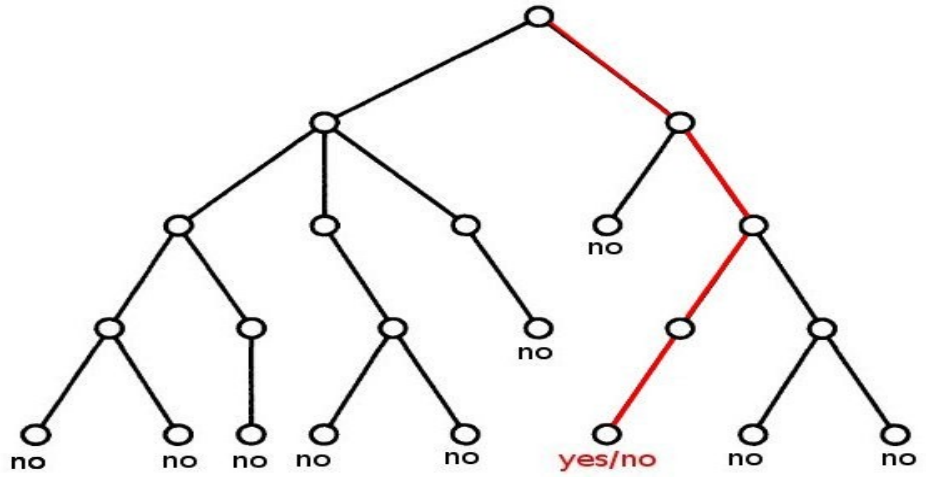
Η κλάση UP

• Μια μη ντετερμινιστική ΤΜ ονομάζεται **unambiguous** αν έχει την ιδιότητα:
"Για κάθε είσοδο x υπάρχει **το πολύ ένας** υπολογισμός(κλαδί) που την αποδέχεται."

• **UP** είναι η κλάση των γλωσσών που γίνονται αποδεκτές από unambiguous ΤΜ πολωνυμικά φραγμένες ως προς το χρόνο.

Παρατήρηση: $P \subseteq UP \subseteq NP$

• Κάθε ντετερμινιστική ΤΜ μπορεί να θεωρηθεί σαν μη ντετερμινιστική με μία επιλογή σε κάθε βήμα. (Αυτή η ΤΜ είναι σίγουρα unambiguous)
• Από τον ορισμό μια unambiguous ΤΜ είναι ειδική περίπτωση των μη ντετερμινιστικών.



Επίσης περιμένουμε : UP≠NP .
(SAT θα αποφασιζόταν από μια unambiguous ΤΜ)
Έτσι εστιάζουμε στο $P \stackrel{?}{=} UP$.

Θεώρημα

(UP=P)⇔ (Δεν υπάρχουν one way functions)

Παρατήρηση

Η πολυπλοκότητα χειρότερης περίπτωσης δεν είναι κατάλληλο κριτήριο στην κρυπτογραφία.
π.χ. : f: X→Y one way function αλλά για τα μισά στοιχεία του X αντιστρέφεται σε πολυωνυμικό χρόνο.

Βελτιώσεις της one way function

"Ισχυρή" one way function

Από την προηγούμενη παρατήρηση είναι προφανές ότι η ιδιότητα (iii) $f^{-1} \notin FP$,του ορισμού της one way function f δεν είναι επαρκής για κρυπτογραφική χρήση. Την αντικαθιστούμε με μία πιο ισχυρή:

-Δεν υπάρχει αλγόριθμος ο οποίος σε χρόνο $O(n^k)$ υπολογίζει την $f^{-1}(y)$ για $2^n / n^k$ ή περισσότερα strings y ,μήκους n . (**Η f αντιστρέφεται αποδοτικά για αμελητέο (negligible) πλήθος των τιμών της**)

Η Eve όμως μπορεί να χρησιμοποιήσει πιθανοτικούς αλγορίθμους.Άρα πιο σωστά:

-**Για κάθε πιθανοτικό πολυωνυμικό αλγόριθμο Α, η πιθανότητα ο Α να αντιστρέψει επιτυχώς την f(x) για τυχαίο x είναι αμελητέα.**

Παρατήρηση(δύο επιπλέον ιδιότητες)

Οι συναρτήσεις f_{mult} , $f_{\exp}$ και f_{RSA} είναι ισχυρές one way functions αλλά μόνο η f_{RSA} χρησιμοποιείται για δημιουργία κρυπτοσυστήματος. Τι παραπάνω ιδιότητες έχει?

(I) Μπορούμε αποδοτικά να βρούμε στοιχεία για το πεδίο ορισμού. (p,q πρώτοι , e πρώτος προς τον φ(pq))

(II)Είναι **trap door function**, **δλδ αντιστρέφεται τετριμένα μέσω μιας πολυωνυμικά υπολογίσιμης συνάρτησης d.** Για RSA : $d(x, e, p, q) = e^{-1} \bmod pq - p - q + 1$

Πιθανοτική κρυπτογράφηση

Πρόβλημα

Συγκεκριμένα μηνύματα είναι εύκολο να αποκρυπτογραφηθούν.

π.χ Η Alice θέλει να στείλει στον Bob ένα bit b με RSA. Όμως $b^e \bmod pq = b$, για $b \in \{0,1\}$.

Λύση

- Η Alice επιλέγει τυχαίο ακέραιο $x \leqslant pq/2$, και στέλνει στον Bob $y = (2x + b)^e \bmod pq$.
- Ο Bob αποκρυπτογραφεί το y παίρνει 2x+b , το τελευταίο ψηφίο είναι το b.

Αποδεικνύεται ότι η εξαγωγή του τελευταίου bit του κρυπτογραφημένου μηνύματος είναι το ίδιο δύσκολη με το "σπάσιμο" του RSA.

Ψηφιακές υπογραφές

Ψηφιακά υπογεγραμμένο μήνυμα

- Ενα μήνυμα $S_{Alice}(x)$ είναι ένα string που περιέχει το μήνυμα x τροποποιημένο έτσι ώστε να πιστοποιείται ο αποστολέας (Alice).
- Έτσι ο Bob είναι σίγουρος ότι επικοινωνεί με την Alice.

Διαδικασία

Σε ένα ασσύμετρο κρυπτοσύστημα έχουμε τα : $e_{Alice}, d_{Alice}, e_{Bob}, d_{Bob}, E, D$.

(I) Η Alice υπογράφει το μήνυμα x : $S_{Alice}(x) = (x, D(d_{Alice}, x))$ (σαν να το αποκρυπτογραφεί).

(II) Ο Bob υπολογίζει : $E(e_{Alice}, D(d_{Alice}, x)) \overset{*}{=} D(d_{Alice}, E(e_{Alice}, x)) \overset{**}{=} x$
και το συγκρίνει με το μήνυμα x. Αν είναι ίδια τότε "προφανώς" η Alice έχει υπογράψει με το d_{Alice}

Παρατηρήσεις

- Στο (I) η Alice μπορεί να κρυπτογραφήσει το υπογεγραμμένο μήνυμα $S_{Alice}(x)$ με το e_{Bob} .
- Στο (II) η ισότητα (**) ισχύει λόγω της αντιστροφής της E από την D
  Η ισότητα (*) ισχύει σε ορισμένα κρυπτοσυστήματα όπου ισχύει η **επιμεριστικότητα** της αντιστροφής.
  Δλδ ισχύει ότι η **E αντιστρέφει την D**.

Ψηφιακή υπογραφή RSA

- Το RSA έχει την ιδιότητα της επιμεριστικότητας γιατί:

$$D(d, E(e, x)) = (x^e)^d \bmod pq = x = (x^d)^e \bmod pq = E(e, D(d, x))$$

Poker μέσω τηλεφώνου

Πρόβλημα

Η Alice και ο Bob διαλέγουν 3 n-ψήφιους α < b < c (χαρτιά) .
Θέλουν να διαλέξουν ένα τυχαίο χαρτί ο καθένας έτσι ώστε :

(i) Τα χαρτιά τους είναι **διαφορετικά.**
(ii) Καθε ζευγάρι επιλογών είναι **ισοπίθανο.**
(iii)Το χαρτί του καθενός είναι **γνωστό μόνο σε στον κάτοχο του.**
(iv)Στο τέλος της παρτίδας, ο νικητής (αυτός με το μεγαλύτερο χαρτί) δεν μπορεί να αμφισβητηθεί.

Λύση

•Οι παίκτες συμφωνούν σε ένα μεγάλο **πρώτο p.**
•Καθένας έχει δύο ιδιωτικά κλειδιά: e_{Alice}, e_{Bob} (κρυπτογράφησης) και d_{Alice}, d_{Bob}(αποκρυπτογράφησης)
•Πρέπει να ισχύει : $e_{Alice} d_{Alice} = e_{Bob} d_{Bob} = 1 \, mod(p-1)$
Έτσι η ύψωση στο e modulo p αντιστρέφεται από την ύψωση στο d modulo p .

(1) Η Alice κρυπτογραφεί τα χαρτιά $\left(a^{e_{Alice}} \, modp, b^{e_{Alice}} \, modp, c^{e_{Alice}} \, modp\right)$, τα στέλνει στον Bob.
(2) Ο Bob διαλέγει ένα από τα τρία και το στέλνει στην Alice.
(3) Η Alice το αποκρυπτογραφεί (είναι το χαρτί της,έστω το b).
(4) Ο Bob κρυπτογραφεί τα δύο που μένουν $\left(a^{e_{Alice} e_{Bob}} \, modp, c^{e_{Alice} e_{Bob}} \, modp\right)$, τα στέλνει στην Alice.
(5) Η Alice διαλέγει ένα από αυτά (έστω το a) το αποκρυπτογραφεί $\left(a^{e_{Alice} e_{Bob} d_{Alice}} \, modp = a^{e_{Bob}}\right)$
και το στέλνει στον Bob.
(6)Ο Bob το αποκρυπτογραφεί και παίρνει το χαρτί του α.

Παρατήρηση

Ισχύουν οι ιδιότητες (i),(ii),(iii),(iv).

Διαλογικές αποδείξεις (Interactive proofs)

Παρατήρηση

L ∈ NP αν υπάρχει πολυωνυμικού χρόνου αλγόριθμος ο οποίος με είσοδο x και μια πιθανή απόδειξη y, ελέγχει αν η y είναι έγκυρη απόδειξη ότι x∈ L.

-Αν x∈ L υπάρχει μια έγκυρη απόδειξη.

-Αν x∉ L δεν υπαρχει έγκυρη απόδειξη.

Σενάριο

- Η Alice έχει **εκθετικές δυνάμεις υπολογισμού**
- Ο Bob μπορεί να εκτελέσει μόνο **πολυωνυμικούς υπολογισμούς.**
- Η Alice θέλει να πείσει τον Bob ότι π.χ. $x \in \bar{L}$ (πρόβλημα λόγω της παρατήρησης) .
- Αν ο Bob χρησιμοποιήσει **πιθανοτικούς αλγόριθμους** ?

Ορισμός (***Σύστημα διαλογικής απόδειξης (A,B)***)

- Η Alice (**proover**) εκτελεί **εκθετικού χρόνου αλγόριθμο Α**.
- Ο Bob (**verifier**) εκτελεί **πολυωνυμικού χρόνου πιθανοτικό αλγόριθμο Β.**
- Είσοδος του πρωτοκόλλου : string x.
- Alice και Bob ανταλλάζουν μηνύματα : $m_1, m_2, .., m_{2^k_{|x|}}$. Η Alice στέλνει τα m_{2i+1} και ο Bob τα m_{2i} .
- $|m_i| \leqslant |x|^k$ (πολυωνυμικού μήκους μηνύματα).
- $m_1 = A(x)$ και για $i \leqslant |x|^k$, $m_{2i} = B(x; m_1; ..; m_{2i-1}; r_i)$ και $m_{2i-1} = A(x; m_1; ..; m_{2i-2})$
- Όπου r_i το τυχαίο string που χρησιμοποιείται από τον Bob για την i-οστή ανταλλαγή.
- Τελικά αν το τελευταίο μήνυμα $m_{2|x|^k} \in \{yes, no\}$ ο Bob αποδέχεται ή απορρίπτει.

Ορισμός

Λέμε ότι το **(A,B) αποδέχεται μια γλώσσα L** αν ισχύουν τα παρακάτω για κάθε string x :

- Αν **x∈ L** τότε η πιθανότητα , το (A,B) να αποδέχεται το x είναι τουλάχιστον $1-\frac{1}{2^{|x|}}$.
- Αν x∉ L τότε η πιθανότητα , το (A',B) να αποδέχεται το x είναι το πολύ $\frac{1}{2^{|x|}}$.

  Όπου A' οποιοσδήποτε εκθετικός αλγόριθμος.

Ορισμός

IP, η κλάση όλων των γλωσσών που αποφασίζονται από ένα σύστημα διαλογικής απόδειξης.

Παρατηρήσεις

- $IP \supseteq NP$ (NP όταν ο Bob δε χρησιμοποιεί πιθανοτικό αλγόριθμο).
- $IP \supseteq BPP$ (BPP όταν ο Bob αγνοεί τις απαντήσεις της Alice).

Παράδειγμα συστήματος διαλογικής απόδειξης : Graph nonisomorphism

GRAPH ISOMORPHISM (GI)

Έστω δύο γραφήματα **G=(V,E)** και **G'=(V,E')** με τιο ίδιο σύνολο κόμβων, είναι **ισομορφικά ;**
Δλδ υπάρχει **μετάθεση π των κόμβων** τέτοια ώστε **G'=π(G),** όπου π(G)=(V,{[π(u),π(u)] : [u,v]∈ E}).

GRAPH NONISOMORPHISM (GNI)

Έστω δύο γραφήματα **G=(V,E)** και **G'=(V,E')** με τιο ίδιο σύνολο κόμβων, είναι μη-**ισομορφικά ;**

Παρατήρηση

- GI ∈ NP αλλά **??**(**NP-complete**, **P-complete** , ανήκει στην **coNP** ,ανήκει στην **BPP**)**??**
- GNI δεν ξέρουμε αν ανήκει στο **NP** ή στο **BPP.**

Διαλογική απόδειξη του GNI

Η Alice θέλει να δείξει στον Bob ότι τα G,G' δεν είναι ισομορφικά. (είσοδος **x=(G,G')**)

(I) Ο Bob επιλέγει ένα **τυχαίο** $b_i \in \{0,1\}$ και οριζει καινούργιο γράφημα $G_i = \begin{cases} G, \alpha\nu\, b_i = 1 \\ G', \alpha\nu\, b_i = 0 \end{cases}$

(II)Ο Bob επιλέγει **τυχαία μετάθεση** π_i των κόμβων του G_i και στέλνει το μήνυμα $m_{2i} - 1 = (G, \pi_i(G_i))$.
(III)Η Alice ελέγχει αν τα δύο γραφήματα είναι ισομορφικά. Απαντάει $m_{2i} = 1$ αν είναι και $m_{2i} = 0$ αλλιώς.
(IV)Η διαδικασία επαναλαμβάνεται $|x|$ φορές. Αν $(b_1, .., b_{|x|}) = (m_2, .., m_{2|x|})$ ο Bob αποδέχεται.

Παρατηρήσεις

- Αν G,G' : μη ισομορφικά η Alice διαλέγει κάθε φορά σωστά το m_{2i} και έτσι πείθει τον Bob.
- Αν G,G' : ισομορφικά. Τότε κάθε μήνυμα του Bob περιέχει δύο ισομορφικά γραφήματα.

Τότε η Alice πρέπει να μαντέψει κάθε φορά το τυχάιο ψηφίο του Bob.
Η πιθανότητα να μαντέψει σωστά $|x|$ ψηφία {0,1} είναι το πολύ $\frac{1}{2^{|x|}}$.

Συμπέρασμα

GNI ∈ IP

Αποδείξεις μηδενικής γνώσης (Zero knowledge proofs)

Πρόβλημα

Η Alice έχει λύση για ένα "δύσκολο" πρόβλημα. Θέλει να αποδείξει στον Bob ότι έχει τη λύση.
Αλλά δεν θέλει ο Bob να έχει στοιχεία για τη λύση.

Παράδειγμα

Η Alice έχει μια λύση του 3-COLORING για ένα γράφημα G=(V,E) (NP-complete).
Έστω ότι έχει ένα χρωματισμό χ:V→{00,11,01}

I) Η Alice παράγει μια **τυχαία μετάθεση π των χρωμάτων.** Έστω
II) Παράγει **δημόσιο και ιδιωτικό κλειδί RSA** $(p_i, q_i, d_i, e_i), \forall\, i \in V$.
III) Κρυπτογραφεί πιθανοτικά το χρώμα $\pi(\chi(i)) = b_i b_i'$, υπολογίζοντας (y_i, y_i') με :

$$y_i = (2x_i + b_i)^{e_i} \bmod p_i q_i \quad \text{και} \quad y_i' = (2x_i' + b_i')^{e_i} \bmod p_i q_i$$

IV) Η Alice στέλνει στον Bob: $(e_i, p_i q_i, y_i, y_i'), \forall\, i \in V$ (δημόσιο κλειδί και κρυπτογραφημένα χρώματα).
V) Ο Bob επιλέγει **τυχαία ακμή** $[i, j] \in E$.
VII) Η Alice στέλνει στον Bob : d_i **και** d_j και ο Bob υπολογίζει $b_i = (y_i^{d_i} \bmod p_i q_i) \bmod 2$.
Όμοια υπολογίζει τα b_i', b_j, b_j' και ελέγχει αν ισχύει $b_i b_i' \neq b_j b_j'$ (χρώματα γειτονικών κόμβων).

Η διαδικασία επαναλαμβάνεται **k |E| φορές.**

Παρατήρηση

Αν Η Alice δεν έχει λύση του 3-COLORING τότε υπάρχει τουλάχιστον μία ακμή $[i, j] \in E$ για την οποία **χ(i)=χ(j) ⇒π(χ(i))=π(χ(j))**. Σε κάθε επαναληψη ο Bob έχει πιθανότητα $\frac{1}{|E|}$ να την ανακαλύψει .
Μετά από **k |E|** επαναλήψεις η πιθανότητα , ο Bob να ανακαλύψει τον λανθασμενο χρωματισμό είναι $1 - e^{-k}$