ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΚΡΥΠΤΟΓΡΑΦΙΑ

5η Διάλεξη

Κωνσταντίνου Ελισάβετ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

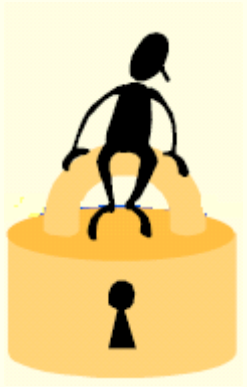
- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Κρυπτογραφία



Κωνσταντίνου Ελισάβετ
ekonstantinou@aegean.gr

http://www.icsd.aegean.gr/ekonstantinou

Ιστορία Ασύμμετρης Κρυπτογραφίας

Η αρχή έγινε το 1976 με την εργασία των Diffie-Hellman "*New Directions in Cryptography*".

Το 1977 παρουσιάστηκε το πρώτο σχήμα ασύμμετρης κρυπτογράφησης από τους Rivest-Shamir-Adleman (RSA).

Ακολούθησε το κρυπτοσύστημα ElGamal και στα μέσα της δεκαετίας του 1980 εμφανίστηκαν τα κρυπτογραφικά συστήματα ελλειπτικών καμπυλών από τον Koblitz.

Ωστόσο...

Μια παραλλαγή του RSA και του πρωτοκόλλου Diffie-Hellman είχαν εφευρεθεί από τους Ellis-Cocks-Williamson στα GCHQ (Government Communications Headquarters) στη Μεγάλη Βρετανία στις αρχές του 1970. Αυτό έμεινε μυστικό μέχρι το 1997.

Πρωτόκολλο Diffie-Hellman

1) Επιλέγεται ένας πρώτος αριθμός p και ένας γεννήτορας α του Z_p^*. Οι τιμές αυτές διαμοιράζονται στους δύο χρήστες.

2)

$a^x \bmod p$

$a^y \bmod p$

Alice
$(x, a^x \bmod p)$

Bob
$(y, a^y \bmod p)$

3) Υπολογίζουν και οι δύο:

$a^{xy} \bmod p$

Πρωτόκολλο Diffie-Hellman

Μια πολύ απλή επίθεση → Man-in-the-middle attack

Σε ποια μαθηματικά προβλήματα βασίζεται?

αν γνωρίζεις το $a^x \bmod p$ θα πρέπει να είναι υπολογιστικά αδύνατο να βρεις το x (πρόβλημα διακριτού λογαρίθμου)

αν γνωρίζεις το $a^x \bmod p$ και το $a^y \bmod p$ θα πρέπει να είναι υπολογιστικά αδύνατο να βρεις το $a^{xy} \bmod p$ (πρόβλημα Diffie-Hellman)

Κρυπτογράφηση κατά RSA

Βασίζεται στην δυσκολία επίλυσης του εξής προβλήματος (καλείται RSA problem):

> Δοθέντος ενός ακεραίου n που είναι το γινόμενο δύο διαφορετικών πρώτων αριθμών p και q, ενός ακεραίου e τέτοιου ώστε gcd(e, (p-1)(q-1)) = 1 και ενός ακεραίου c, βρες έναν ακέραιο m που να ικανοποιεί την ισοτιμία $m^e \equiv c \bmod n$.

Αποδεικνύεται ότι το RSA problem είναι ισοδύναμο με το integer factorization problem.

Δημιουργία Κλειδιών

Βήματα για κάθε χρήστη *A*:

1) Δημιουργεί δύο μεγάλους πρώτους αριθμούς p και q, περίπου του ίδιου μεγέθους.
2) Υπολογίζει την τιμή $n = pq$ και την $\varphi = (p-1)(q-1) = \varphi(n)$.
3) Επιλέγει ένα τυχαίο e με $1 < e < \varphi$, τέτοιο ώστε $\gcd(e, \varphi) = 1$.
4) Υπολογίζει τον μοναδικό ακέραιο d για τον οποίο ισχύει η ισοτιμία $ed \equiv 1 \bmod \varphi$ ($d = e^{-1} \bmod \varphi$).
5) Το δημόσιο κλειδί του *A* είναι το ζευγάρι (n, e) και ιδιωτικό το d.

Κρυπτογράφηση-Αποκρυπτογράφηση

Κρυπτογράφηση: Ο Β κρυπτογραφεί ένα μήνυμα m με το δημόσιο κλειδί του Α και στέλνει την κρυπτογραφημένη του μορφή

(α) Λαμβάνει το δημόσιο κλειδί (n, e) του Α.

(β) Μετατρέπει το μήνυμα m που θέλει να στείλει σε έναν ακέραιο στο διάστημα [0, n-1].

(γ) Υπολογίζει την τιμή $c = m^e \bmod n$ και την στέλνει στον Α.

Αποκρυπτογράφηση: Ο Α υπολογίζει τα παρακάτω

(α) Υπολογίζει την τιμή $m = c^d \bmod n$.

(β) Μετατρέπει τον ακέραιο m στο αρχικό κείμενο.

Λειτουργία Αποκρυπτογράφησης

Ισχύει ότι $ed \equiv 1 \bmod \varphi$. Δηλαδή υπάρχει ακέραιος k τέτοιος ώστε $ed = 1 + k\varphi$.

(A) Αν $\gcd(m, p) = 1$ τότε από το Μικρό Θεώρημα του Fermat ισχύει ότι $m^{p-1} \equiv 1 \bmod p \Rightarrow m^{(p-1)k(q-1)} \equiv 1 \bmod p \Rightarrow$

$m^{(p-1)k(q-1)+1} \equiv m \bmod p \Rightarrow m^{ed} \equiv m \bmod p$

(B) Αν $\gcd(m, p) = p$ τότε $m \equiv 0 \bmod p \equiv m^{ed} \bmod p$

Επομένως ισχύει σε κάθε περίπτωση ότι $m^{ed} \equiv m \bmod p$ και όμοια προκύπτει ότι $m^{ed} \equiv m \bmod q$.

CRT

$c^d \equiv m^{ed} \equiv m \bmod n$

Παράμετροι p και q

Πως θα μπορούσε να «σπάσει» το σύστημα?

Αν από το n βρεθούν οι πρώτοι του παράγοντες p και q, τότε μπορεί να υπολογιστεί η τιμή φ = φ(n), άρα και το d = e^{-1} mod φ.

Το RSA problem ισοδύναμο με το πρόβλημα της παραγοντοποίησης.

Οι παράμετροι p και q πρέπει να επιλέγονται με τέτοιο τρόπο ώστε η παραγοντοποίηση του n (με τους υπάρχοντες αλγορίθμους) να είναι δύσκολη.

Παράμετροι p και q

(α) Οι πρώτοι p και q πρέπει να έχουν το ίδιο μέγεθος σε bits. 512 bits θεωρείται ότι παρέχουν ένα καλό επίπεδο ασφάλειας.

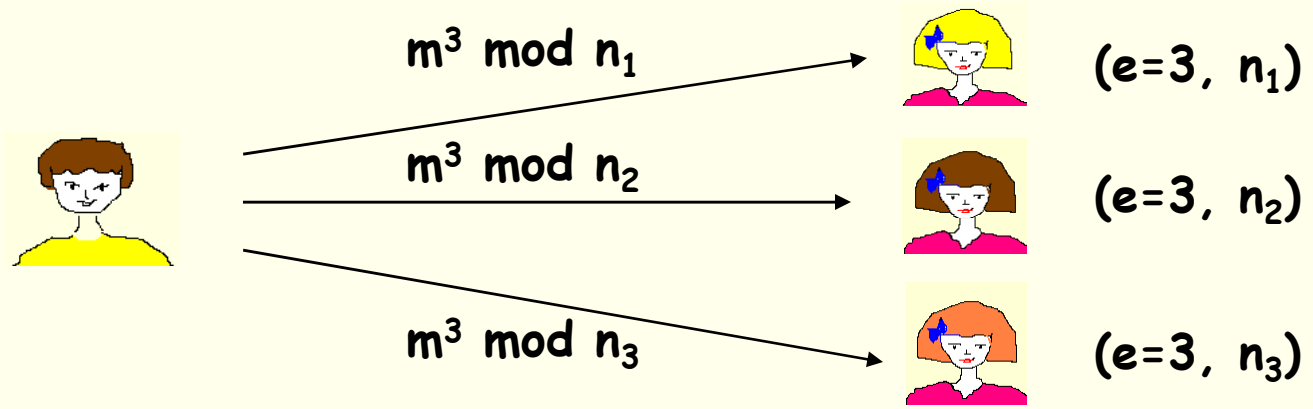
(β) Η διαφορά μεταξύ των p και q δεν πρέπει να είναι πολύ μικρή (π.χ. ο q να είναι ο επόμενος πρώτος μετά τον p). Το πρόβλημα που προκύπτει τότε είναι ότι $p \approx q \approx n^{1/2}$. Αν τα p και q επιλεγούν με τυχαίο τρόπο, η διαφορά $|p-q|$ θα είναι μεγάλη με πολύ μεγάλη πιθανότητα.

(γ) Πολλοί επιστήμονες συνιστούν οι πρώτοι p και q να είναι ισχυροί πρώτοι (strong primes). Δηλαδή:

1. Το p-1 να έχει έναν μεγάλο πρώτο παράγοντα r.
2. Το p+1 να έχει έναν μεγάλο πρώτο παράγοντα r_1.
3. Το r-1 να έχει επίσης έναν μεγάλο πρώτο παράγοντα.

Χρήση της Τιμής e = 3

Πολλές φορές για να επιτύχουμε γρήγορη κρυπτογράφηση επιλέγουμε έναν μικρό ακέραιο e. Συχνά e=3.



$$x \equiv m^3 \bmod n_1$$
$$x \equiv m^3 \bmod n_2$$
$$x \equiv m^3 \bmod n_3$$

CRT ⇒ $x \equiv m^3 \bmod n_1 n_2 n_3$ ⇒

Επειδή $m^3 < n_1 n_2 n_3$ ισχύει $x = m^3$ και ανακτούμε το m!

Χρήση της Τιμής e = 3

Παράδειγμα:

m=6

$m^3 \bmod n_1=6$ →  $(e=3,\ n_1=7)$

$m^3 \bmod n_2=7$ →  $(e=3,\ n_2=11)$

$m^3 \bmod n_3=8$ →  $(e=3,\ n_3=13)$

$x \equiv 6 \bmod 7$
$x \equiv 7 \bmod 11$
$x \equiv 8 \bmod 13$

CRT ⇒ $x \equiv 216 \bmod 1001$ ⇒

Επειδή $m^3 < n_1n_2n_3$ ισχύει $x = 216$ και επομένως m=6!

Χρήση της Τιμής e = 3

Για να αποφευχθεί αυτή η επίθεση:

(A) Είτε δεν θα πρέπει να χρησιμοποιείται μικρή τιμή για το e αν το ίδιο μήνυμα στέλνεται σε πολλούς χρήστες.

(B) Ή μπορεί να προστεθεί μια ψευδοτυχαία σειρά από bits μετά το μήνυμα (διαφορετική για κάθε χρήστη στον οποίο στέλνεται το κρυπτοκείμενο). Η διαδικασία αυτή καλείται salting του μηνύματος.

Κρυπτογράφηση κατά Rabin

Δημιουργία κλειδιών: Κάθε χρήστης *A* κάνει τα παρακάτω

1. Δημιουργεί δύο μεγάλους πρώτους αριθμούς p και *q* ίδιου μεγέθους
2. Υπολογίζει την τιμή n = pq.
3. Το δημόσιο κλειδί του *A* είναι το n και το ιδιωτικό το (p, *q*).

Κρυπτογράφηση: *O* B θέλει να στείλει ένα μήνυμα στον *A*

1. Λαμβάνει το δημόσιο κλειδί του *A*.
2. Μετασχηματίζει το μήνυμα σε έναν ακέραιο m < n.
3. Υπολογίζει την τιμή $c = m^2 \bmod n$.
4. Στέλνει το c στον *A*.

Κρυπτογράφηση-Αποκρυπτογράφηση

Αποκρυπτογράφηση: Ο Α ακολουθεί τα παρακάτω βήματα

- Βρίσκει τις 4 ρίζες του c mod n χρησιμοποιώντας τα p και q.
- Μία από τις 4 ρίζες αποτελεί το αρχικό μήνυμα m. Αποφασίζει με κάποιο τρόπο ποια από αυτές είναι και μετατρέπει το μήνυμα από ακέραιο στην αρχική του μορφή.

Πρόταση: Η ισοτιμία $x^2 \equiv a \bmod n$ έχει 2^k λύσεις x, όπου k είναι το πλήθος των πρώτων παραγόντων του n.

Εύρεση των 4 Ριζών

Αν $p \equiv q \equiv 3 \bmod 4$, τότε οι 4 ρίζες του c mod n υπολογίζονται πολύ εύκολα. Συγκεκριμένα, ο Α υπολογίζει τα εξής:

1. Βρίσκει ακεραίους a και b τέτοιους ώστε $ap + bq = 1$.
2. Υπολογίζει τις τιμές $r = c^{(p+1)/4} \bmod p$ και $s = c^{(q+1)/4} \bmod q$.
3. Υπολογίζει $x = (aps + bqr) \bmod n$.
4. Υπολογίζει $y = (aps - bqr) \bmod n$.
5. Οι 4 ρίζες του c mod n είναι οι x, $-x \bmod n$, y και $-y \bmod n$.

Πώς επιλέγεται η σωστή ρίζα?

Παράδειγμα Εφαρμογής

Έστω p = 277, q = 331 και n = 91687.

Υποθέστε ότι το μήνυμα που θέλουμε να κρυπτογραφήσουμε είναι σε δυαδική μορφή το m′ = 1001111001 (10 bits). Από το μήνυμα αυτό δημιουργούμε ένα καινούριο μεγέθους 16 bits, επαναλαμβάνοντας τα τελευταία 6 bits του m′. Δηλαδή,

$$m = 1001\ 111001\ 111001.$$

Αυτό αντιστοιχεί στον ακέραιο m = 40569 < n.

Ο Β υπολογίζει την τιμή $c = m^2 \bmod n = 62111$.

Ο Α που λαμβάνει το c, υπολογίζει τις 4 ρίζες του:

$m_1 = 69654$, $m_2 = 22033$, $m_3 = 40569$, $m_4 = 51118$.

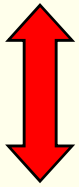
Μετατρέπει όλες τις τιμές σε δυαδική μορφή και βλέπει σε ποια επαναλαμβάνονται τα τελευταία 6 bits. Την ιδιότητα αυτή την έχει μόνο το m_3 και επιλέγοντάς το, βρίσκει τελικά το m′.

Πρόβλημα Εύρεσης Τετραγωνικής Ρίζας Modulo n

Η κρυπτογράφηση κατά Rabin βασίζεται στο εξής πρόβλημα:

> Δοθέντος ενός σύνθετου ακεραίου n και ενός τετραγωνικού υπολοίπου a modulo n, να βρεθεί μια τετραγωνική ρίζα του a mod n.

Square Root Modulo n Problem



ισοδύναμα

Integer Factorization Problem

Πρόβλημα Διακριτού Λογαρίθμου

Ορισμός: Έστω G μια κυκλική ομάδα τάξης n και α ένας γεννήτορας της G. Για οποιοδήποτε στοιχείο β που ανήκει στην ομάδα G, ο διακριτός λογάριθμος του β στην βάση α είναι ο μοναδικός ακέραιος x, με $0 \leq x \leq n-1$, για τον οποίο $\beta = \alpha^x$.

Παράδειγμα: Έστω $p = 97$ ένας πρώτος αριθμός. Το Z_{97}^* είναι κυκλική ομάδα με τάξη $n = 96$. Το στοιχείο $\alpha = 5$ αποτελεί γεννήτορα της ομάδας. Αν $\beta = 35$ στοιχείο της ομάδας τότε ο διακριτός λογάριθμος του β στη βάση α είναι το στοιχείο $x = 32$, αφού $\alpha^{32} \equiv \beta \bmod 97$.

Πρόβλημα Διακριτού Λογαρίθμου

Πρόβλημα Διακριτού Λογαρίθμου (Discrete Logarithm Problem - DLP): Δοθέντος ενός πρώτου p, ενός γεννήτορα α του Z_p^* και ενός στοιχείου β του Z_p^*, να βρεθεί ακέραιος x, με $0 \leq x \leq p-2$, για τον οποίο $\alpha^x \equiv \beta \bmod p$.

Πρόβλημα Diffie-Hellman (Diffie-Hellman Problem - DHP): Δοθέντος ενός πρώτου p, ενός γεννήτορα α του Z_p^* και δύο στοιχείων $g = \alpha^x \bmod p$ και $h = \alpha^y \bmod p$, να βρεθεί η τιμή $\alpha^{xy} \bmod p$.

Αν επιλύονταν εύκολα το πρόβλημα του διακριτού λογαρίθμου, τότε θα επιλύονταν και το πρόβλημα Diffie-Hellman.

Κρυπτοσύστημα ElGamal

Δημιουργία κλειδιών για κάθε χρήστη *A*:

1) Δημιουργεί έναν πρώτο, τυχαίο αριθμό p και έναν γεννήτορα α της ομάδας Z_p^*.
2) Επιλέγει ένα τυχαίο d με $1 \le d \le p-2$, και υπολογίζει την τιμή $\alpha^d \bmod p$.
3) Το δημόσιο κλειδί του *A* είναι το (p, α, α^d) και ιδιωτικό το d.

Παρατήρηση: Για να υπολογιστεί το ιδιωτικό κλειδί από το δημόσιο, χρειάζεται να επιλυθεί το πρόβλημα του διακριτού λογαρίθμου.

Κρυπτοσύστημα ElGamal

Κρυπτογράφηση: Ο Β κρυπτογραφεί ένα μήνυμα m με το δημόσιο κλειδί του Α και στέλνει την κρυπτογραφημένη του μορφή

(α) Λαμβάνει το δημόσιο κλειδί (p, α, α^d) του Α.

(β) Μετατρέπει το μήνυμα m που θέλει να στείλει σε έναν ακέραιο στο διάστημα $[0, p-1]$.

(γ) Επιλέγει μια τυχαία τιμή k, με $1 \leq k \leq p-2$.

(δ) Υπολογίζει την τιμή $\gamma = \alpha^k \bmod p$ και $\delta = m(\alpha^d)^k \bmod p = m\gamma^d \bmod p$. Στέλνει το κρυπτοκείμενο $c = (\gamma, \delta)$ στον Α.

Αποκρυπτογράφηση: Ο Α υπολογίζει τα παρακάτω

(α) Υπολογίζει την τιμή $\gamma^{p-1-d} \equiv \gamma^{-d} \bmod p$.

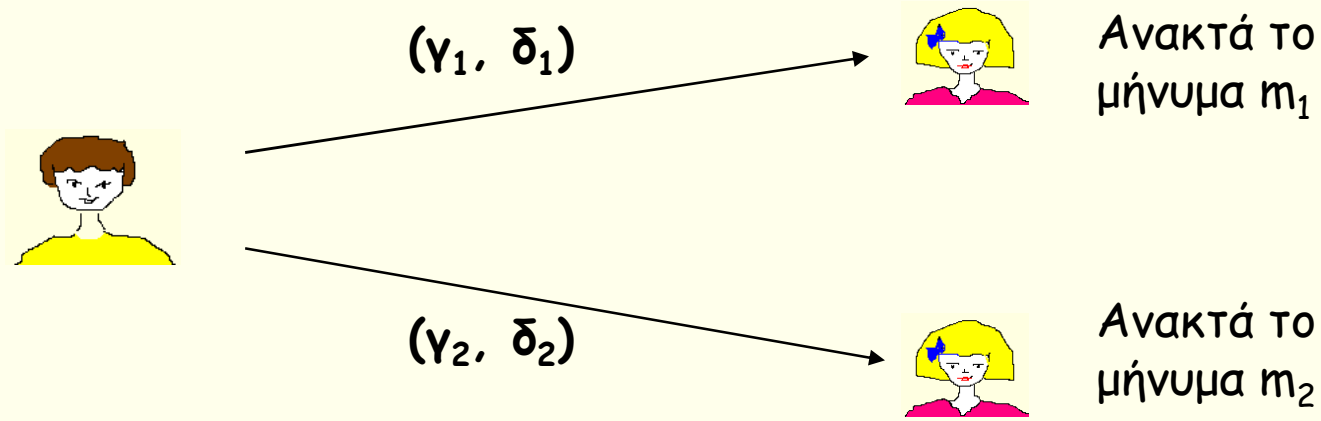
(β) Το $m = (\gamma^{-d})\delta \bmod p$.

Κρυπτοσύστημα ElGamal

Αν κάποιος επιτιθέμενος γνωρίζει την τιμή $\delta = m(a^d)^k \bmod p$ δεν μπορεί να υπολογίσει το m αν δεν ξέρει το $(a^d)^k$. Με άλλα λόγια, ο επιτιθέμενος θα πρέπει να λύσει το πρόβλημα Diffie-Hellman, αφού γνωρίζει τα $a^d \bmod p$ και $\gamma = a^k \bmod p$ και θέλει να υπολογίσει το $(a^d)^k$.

Αν υπάρχουν πολλοί χρήστες στο σύστημα, μπορούν να έχουν κοινά τα p και α, οπότε ως δημόσιο κλειδί του κάθε χρήστη να μην είναι η τριάδα (p, a, a^d) αλλά μόνο το a^d (αφού τα άλλα δύο στοιχεία είναι γνωστά σε όλους).

Κρυπτοσύστημα ElGamal



Αν έχει χρησιμοποιηθεί ο ίδιος τυχαίος ακέραιος k και στις δύο κρυπτογραφήσεις, τότε $\delta_1/\delta_2 = m_1(a^d)^k / m_2(a^d)^k = m_1/m_2$. Άρα σε κάθε κρυπτογράφηση θα πρέπει να αλλάζει ο τυχαίος αριθμός k.

Μέγεθος κλειδιών: Τουλάχιστον 512 bits για τον πρώτο p. Συνήθως έχει μέγεθος 1024 bits.

Γενικευμένος ElGamal

Ο αλγόριθμος κρυπτογράφησης ElGamal μπορεί να οριστεί και σε διαφορετικές ομάδες, εκτός της Z_p^*. Τα βήματα των αλγορίθμων κρυπτογράφησης-αποκρυπτογράφησης παραμένουν τα ίδια, μόνο που οι πράξεις πλέον δεν γίνονται στο Z_p^* αλλά στην ομάδα πάνω στην οποία ορίζεται το κρυπτοσύστημα.

Οι ομάδες που χρησιμοποιούνται συνήθως είναι:

(α) Η ομάδα F_{p^m} για p=2 ή p έναν περιττό πρώτο.

(β) Η ομάδα που ορίζεται από τα σημεία μιας ελλειπτικής καμπύλης.

Ελλειπτικές Καμπύλες

Ελλειπτική Καμπύλη (Elliptic Curve):

- ✓ Ορίζεται πάνω σε ένα πρώτο (F_p) ή δυαδικό σώμα.
- ✓ ΕΚ στο F_p (συμβολίζεται με $E(F_p)$): σύνολο λύσεων (x,y) στο F_p της εξίσωσης

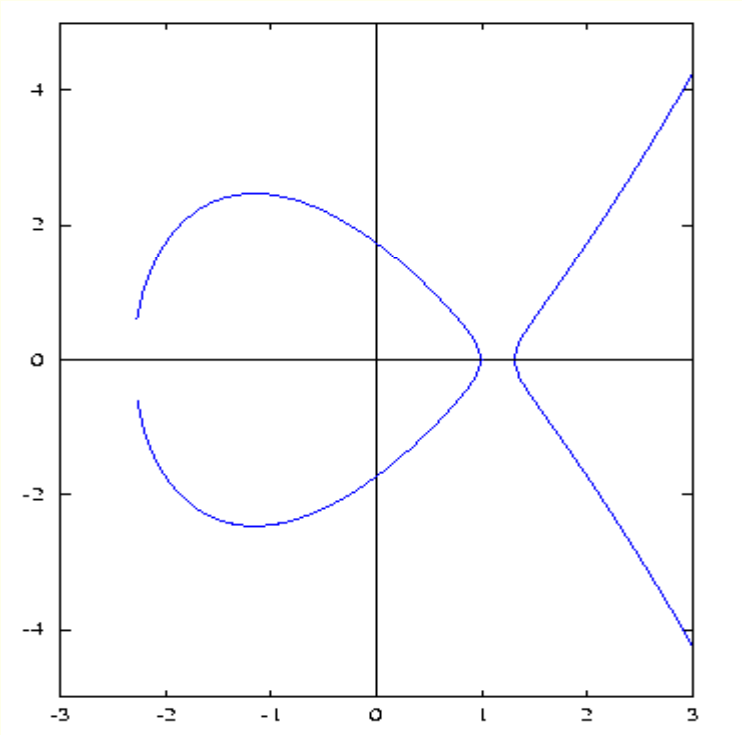
$$y^2 = x^3 + ax + b$$

μαζί με ένα ειδικό σημείο O , που ονομάζεται *σημείο στο άπειρο*.

Παράμετροι της ελλειπτικής καμπύλης είναι τα (a, b) και p.

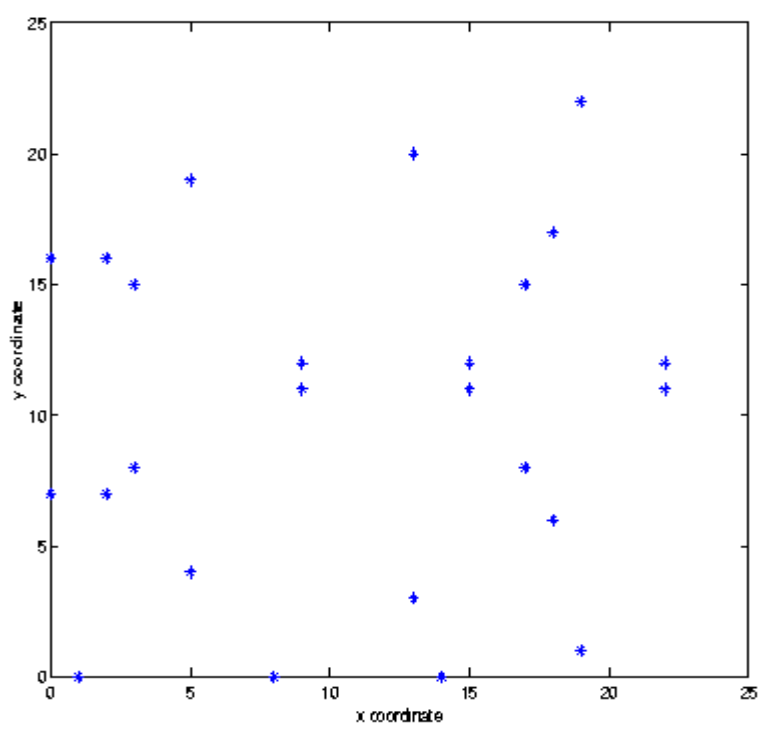
Ελλειπτικές Καμπύλες

$y^2 = x^3 - 4x + 3$



Q

Λύσεις (x,y) στο F_{23}

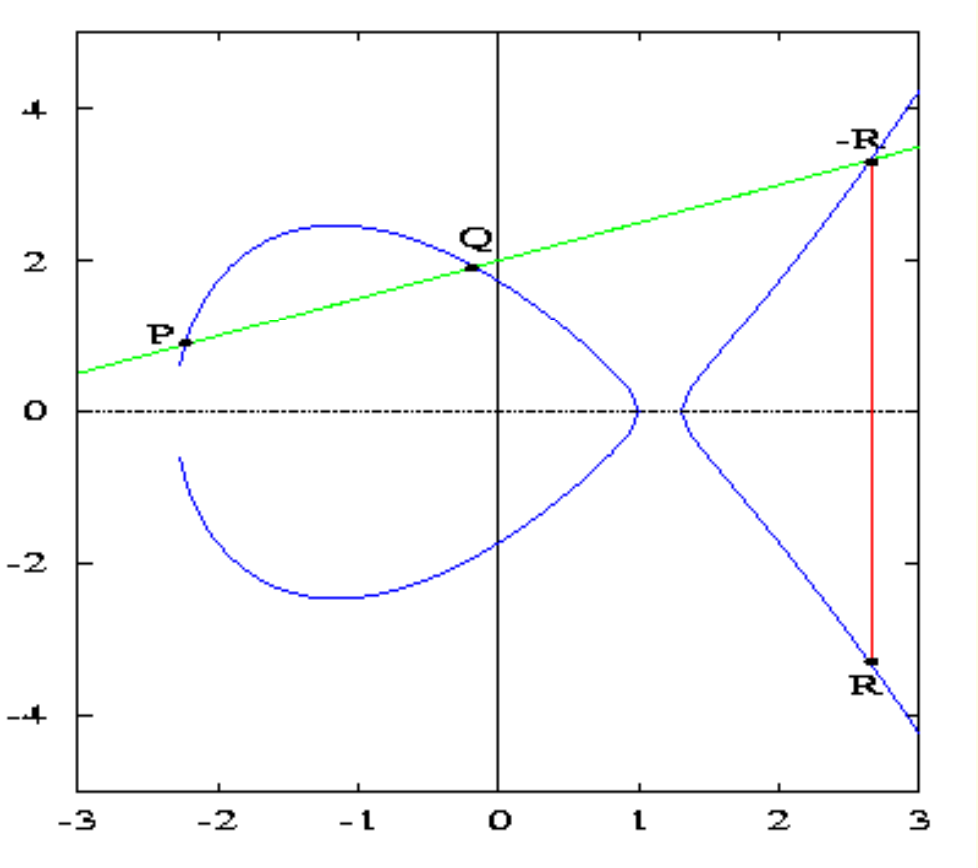


F_{23}

Βασικές Πράξεις

- **Πρόσθεση σημείων:** $P + Q = R$
- $(E(F_p), +)$: Αβελιανή ομάδα όπου το O είναι το ουδέτερο στοιχείο της
- **Πολλαπλασιασμός:**

$$Q = kP = \underbrace{P + \ldots + P}_{k \text{ φορές}}$$



Πρόβλημα Διακριτού Λογαρίθμου στις ΕΚ

Δοθέντων $P, Q \in E(F_p)$, ζητείται να βρεθεί ο μικρότερος t ($0 \leq t \leq m-1$, όπου m είναι η τάξη της ΕΚ), για τον οποίο ισχύει:

$$Q = tP$$

Εκθετική πολυπλοκότητα επίλυσης:

$$T(N) = O(2^{N/2}) \quad \text{όπου} \quad N = \lceil \log_2 p \rceil$$

Κρυπτογραφικά πρωτόκολλα που βασίζονται στο ECDLP:

- ✓ κρυπτογράφηση κατά El Gamal
- ✓ πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman
- ✓ αλγόριθμος δημιουργίας ψηφιακών υπογραφών ECDSA

(ακριβώς ίδια με τα πρωτόκολλα που βασίζονται στο DLP)

Δημιουργία Κλειδιών

Κρυπτογραφικά Συστήματα που βασίζονται στο DLP

1. Επιλέγεται τυχαία ένα ιδιωτικό κλειδί $d \in \{1, p-2\}$
2. Επιλέγεται ένα στοιχείο g του πεπερασμένου σώματος
3. Υπολογίζεται το δημόσιο κλειδί $e = g^d \bmod p$

Κρυπτογραφικά Συστήματα ΕΚ που βασίζονται στο ECDLP

1. Επιλέγεται τυχαία ένα ιδιωτικό κλειδί $d \in \{1, m-2\}$
2. Επιλέγεται ένα τυχαίο σημείο G στην ΕΚ
3. Υπολογίζεται το δημόσιο κλειδί $e = dG$

ορίζονται στο πρώτο σώμα F_p

Κρυπτογράφηση-Αποκρυπτογράφηση

Κρυπτογράφηση: Ο Β κρυπτογραφεί ένα μήνυμα Μ με το δημόσιο κλειδί του Α και στέλνει την κρυπτογραφημένη του μορφή

(α) Λαμβάνει το δημόσιο κλειδί (p, G, e) του Α.

(β) Μετατρέπει το μήνυμα Μ που θέλει να στείλει σε έναν ακέραιο στο διάστημα [0, p-1].

(γ) Επιλέγει μια τυχαία τιμή k, με $1 \leq k \leq n-2$, όπου n είναι ο μεγαλύτερος πρώτος παράγοντας της τάξης της ΕΚ.

(δ) Υπολογίζει την τιμή Γ = kG και Δ = ke. Στέλνει το κρυπτοκείμενο c = (Γ, δ) στον Α, όπου δ = Mx mod p και x είναι η x συντεταγμένη του σημείου Δ.

Αποκρυπτογράφηση: Ο Α υπολογίζει τα παρακάτω

(α) Υπολογίζει την τιμή dΓ = d(kG) = ke = Δ.

(β) Το $M = (x^{-1})\delta \bmod p$, όπου x είναι η x συντεταγμένη του σημείου Δ.

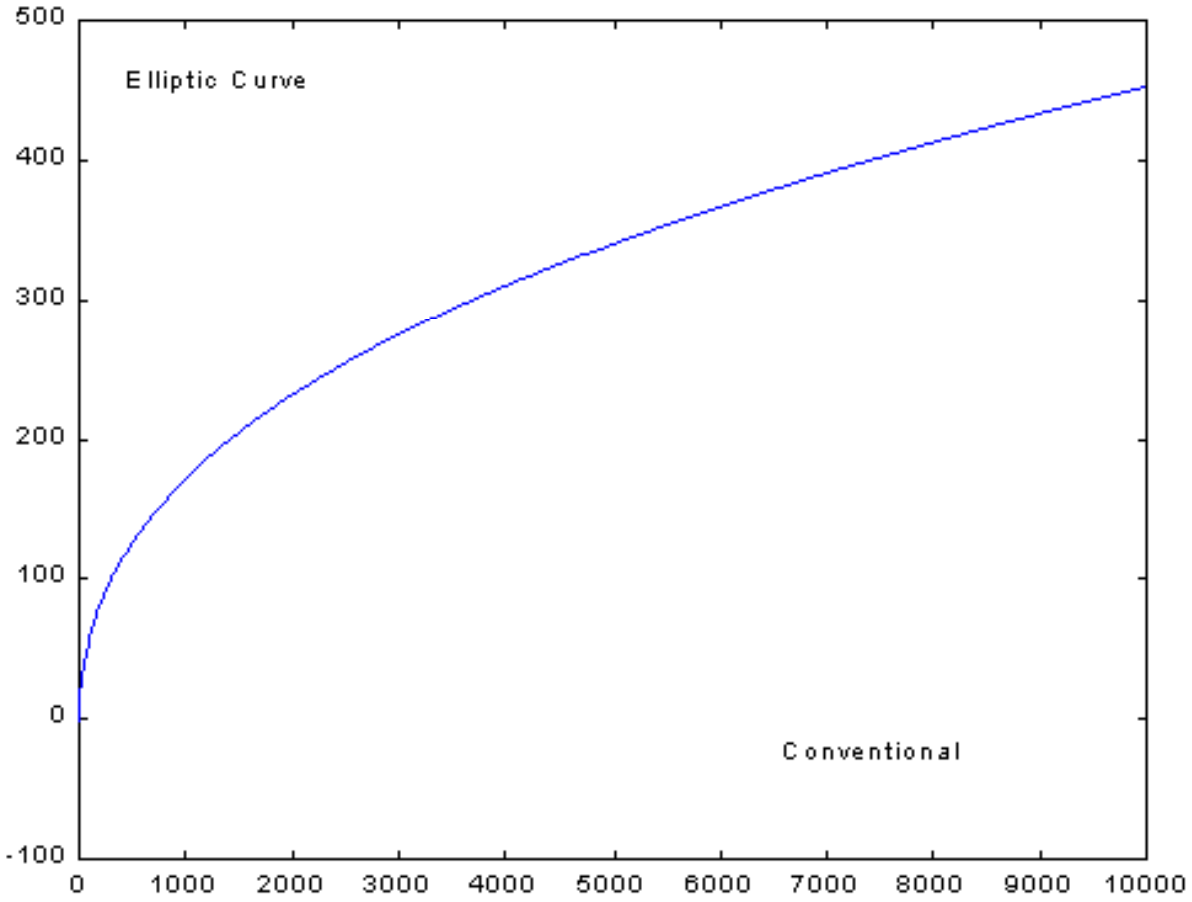
ECDLP vs DLP

Η επίλυση του ECDLP απαιτεί εκθετικό χρόνο, ενώ του DLP απαιτεί υποεκθετικό.

Αποτέλεσμα: Τα κρυπτογραφικά συστήματα ΕΚ χρησιμοποιούν μικρότερες παραμέτρους από ότι τα συμβατικά συστήματα διακριτού λογάριθμου για το ίδιο επίπεδο ασφάλειας.

Εφαρμογή: Σε συσκευές περιορισμένων πόρων (π.χ. έξυπνες κάρτες, κινητά τηλέφωνα) και όπου υπάρχουν γενικά περιορισμοί στη μνήμη, στην ταχύτητα κ.τ.λ.

ECDLP vs DLP


Elliptic Curve
Conventional
500
400
300
200
100
0
-100
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000

Διάβασμα…

Κεφάλαια 8.1, 8.2, 8.3 και 8.4 του
Handbook of Applied Cryptography