Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής
ΠΜΣ στα Πληροφοριακά Συστήματα

Κρυπτογραφία και Εφαρμογές

Μαριάς Ιωάννης
marias@aueb.gr

Μαρκάκης Ευάγγελος
markakis@gmail.com

Outline

Public Key Cryptography

- RSA cryptosystem
  - ✓ Περιγραφή και κρυπτανάλυση
- ElGamal cryptosystem
  - ✓ Περιγραφή και κρυπτανάλυση
- Ψηφιακές Υπογραφές
  - ✓ RSA signature scheme
  - ✓ ElGamal signature scheme
- Ελλειπτικές Καμπύλες
  - ✓ Ελλειπτικές καμπύλες στους πραγματικούς, στο Z_p και στο $GF(2^m)$
  - ✓ Κρυπτογραφία ελλειπτικών καμπυλών

Κρυπτοσυστήματα δημόσιου κλειδιού

- ✓ Κύριο μειονέκτημα της συμμετρικής κρυπτογραφίας: Η Alice και ο Bob πρέπει να συμφωνήσουν εκ των προτέρων για το κλειδί K μέσω ασφαλούς καναλιού
- ✓ Αν αυτό δεν είναι εφικτό? Μπορεί να γίνει η κρυπτογράφηση χωρίς να υπάρξει επικοινωνία μεταξύ Alice και Bob?
- ✓ Ιδέα: Κάθε οντότητα κατέχει ένα **P**ublic και ένα private (**S**ecret) key.
- ✓ Κάθε κλειδί είναι ένα τμήμα πληροφορίας.
  - RSA: το δημόσιο κλειδί είναι ένα ζεύγος ακεραίων.
- ✓ Η Alice (**A)** και ο Bob (**B)** έχουν ως public και secret keys τα
  - $\mathbf{P_A}$, $\mathbf{S_A}$ για Alice
  - $\mathbf{P_B}$, $\mathbf{S_B}$ για Bob.

Κρυπτοσυστήματα δημόσιου κλειδιού

- ✓ Έστω **D** ο χώρος των αποδεκτών μηνυμάτων
- ✓ Στην απλούστερη μορφή της public-key cryptography, τα public και secret keys ορίζουν one-to-one μετασχηματισμούς από το **D** στο **D**
- ✓ Η encryption function που αντιστοιχεί στο public key της Alice δηλώνεται ως E_A και η decryption function που αντιστοιχεί στο secret key της Alice ως D_A.
  - Οι E_A, D_A είναι permutations στο **D**.
  - Οι E_A, D_A είναι υπολογιστικά εφικτές δεδομένων των $\mathbf{P_A}$ και $\mathbf{S_A}$, αντίστοιχα

- ✓ Πρόκληση για ανάπτυξη υπολογιστικά εφικτού public-key cryptosystem:
  - Δημιουργία ενός συστήματος στο οποίο μπορούμε να αποκαλύψουμε το μετασχηματισμό $\mathbf{E_A()}$ χωρίς να μπορεί να ανακαλυφθεί ο αντίστροφος μετασχηματισμός $\mathbf{D_A()}$
  - Αντιθέτως, στη συμμετρική κρυπτογραφία αν ξέρουμε το $\mathbf{E_A()}$ τότε εύκολα μαθαίνουμε και το $\mathbf{D_A()}$

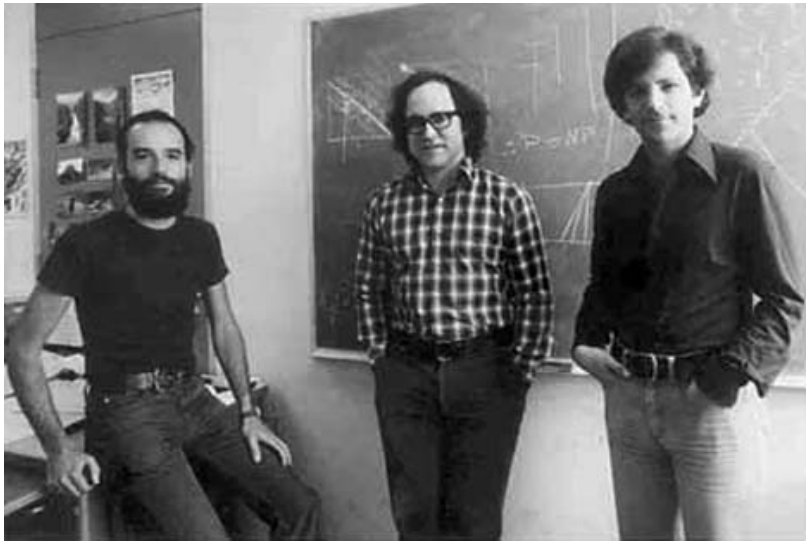
- Κρυπτοσυστήματα δημόσιου κλειδιού
- Συνοψίζοντας, σε ένα public key cryptosystem:
  - ✓ Είναι υπολογιστικά εφικτό για έναν χρήστη **B** να παράγει ένα ζεύγος κλειδιών (Public key $\mathbf{P_B}$, Secret key $\mathbf{S_B}$)
  - ✓ Είναι υπολογιστικά εφικτό για έναν αποστολέα **A**, που γνωρίζει το δημόσιο κλειδί του **B** και το plaintext **M** να δημιουργήσει το αντίστοιχο ciphertext: $\mathbf{C= E_B(M)}$
  - ✓ Είναι υπολογιστικά εφικτό για έναν παραλήπτη **B**, που γνωρίζει το ιδιωτικό του κλειδί και λαμβάνει το ciphertext **C** να ανακτήσει το αρχικό κείμενο **M**: $\mathbf{M=D_B(C)=D_B(E_B(M))}$
  - ✓ Είναι υπολογιστικά ανέφικτο γνωρίζοντας μόνο το δημόσιο κλειδί $\mathbf{P_B}$ να προσδιοριστεί το ιδιωτικό κλειδί $\mathbf{S_B}$
  - ✓ Είναι υπολογιστικά ανέφικτο γνωρίζοντας το δημόσιο κλειδί $\mathbf{P_B}$ και το ciphertext **C** να προσδιοριστεί το αρχικό μήνυμα **M**

Κρυπτοσυστήματα δημόσιου κλειδιού

- ✓ Trapdoor one way functions
- ✓ One-way functions: είναι συναρτήσεις που μπορούμε να τις υπολογίσουμε εύκολα, είναι όμως υπολογιστικά ανέφικτο να υπολογίσουμε την αντίστροφή τους
- ✓ Trapdoor: κάποια πληροφορία που μας επιτρέπει να υπολογίσουμε την αντίστροφη μιας one way function
- ✓ Ουσιαστικά στην κρυπτογραφία δημοσίου κλειδιού ψάχνουμε για trapdoor one-way functions
- ✓ [Diffie-Hellman, 1976]: New Directions in Cryptography

RSA

- RSA - Rivest, Shamir, Adleman (1978, MIT)
  - ✓ Turing award, 2003



- RSA - Rivest, Shamir, Adleman (1978, MIT)
- Χαρακτηριστικά
  - ✓ Block cipher
  - ✓ Ορίζεται στο $\mathbf{Z_n}$, δηλαδή ο χώρος των αποδεκτών μηνυμάτων **D** είναι οι αριθμοί modulo n (κλάσεις ισοδυναμίας)

Παραγωγή Κλειδιών

Επέλεξε πρώτους, μεγάλους, διαφορετικούς, αριθμούς	p, q
Υπολόγισε n:	$n = p \cdot q$
Υπολόγισε φ(n):	$\varphi(n) = (p-1)(q-1)$
Επέλεξε ακέραιο e	
(1<e<φ(n)), έτσι ώστε:	$\gcd(\varphi(n), e) = 1$
Υπολόγισε d, έτσι ώστε:	$de = 1 \bmod(\varphi(n))$
Public key	$P = \{e,n\}$
Secret key	$S = \{d, p, q\}$

Συνάρτηση Euler

- RSA - Rivest, Shamir, Adleman (1978, MIT)

✓ Μπορούμε να έχουμε ένα ευρετήριο με τα δημόσια κλειδιά όλων των χρηστών

Κρυπτογράφηση

Αρχικό κείμενο $M < n$

Ciphertext: $C = E(M) = M^e \bmod n$

Αποκρυπτογράφηση

Ciphertext $C < n$

Αρχικό κείμενο: $M = D(C) = C^d \bmod n$

✓ Για την ύψωση σε δύναμη: χρήση του repeated squaring algorithm

RSA

- Υλοποίηση παραγωγής κλειδιών
- Πώς επιλέγουμε το e?
  - ✓ Αρκεί κάποιος πρώτος αριθμός > max{p, q} (ίσως και μικρότεροι πρώτοι να είναι κατάλληλοι) - χρήση primality testing
  - ✓ Recommended value: $e = 2^{16} + 1 = 65537$
- Πώς υπολογίζουμε το d?
  - ✓ Χρήση του extended Euclidean algorithm

Παραγωγή Κλειδιών

Επέλεξε πρώτους, μεγάλους, διαφορετικούς, αριθμούς	p, q
Υπολόγισε n:	$n = p \cdot q$
Υπολόγισε φ(n):	$\varphi(n) = (p-1)(q-1)$
Επέλεξε ακέραιο e	
(1<e<φ(n)), έτσι ώστε:	$\gcd(\varphi(n), e) = 1$
Υπολόγισε d, έτσι ώστε:	$de = 1 \bmod(\varphi(n))$
Public key	$P = \{e,n\}$
Secret key	$S = \{d, p, q\}$

- Παράδειγμα

Παραγωγή Κλειδιών

Επέλεξε πρώτους, μεγάλους, διαφορετικούς, αριθμούς	p, q	p = 7, q = 17
Υπολόγισε n:	$n = p \cdot q$	n = 119
Υπολόγισε φ(n):	$\varphi(n) = (p-1)(q-1)$	φ(n) = 96
Επέλεξε ακέραιο e (1<e<φ(n)), έτσι ώστε:	$\gcd(\varphi(n), e) = 1$	e = 5
Υπολόγισε d, έτσι ώστε:	$de = 1 \bmod(\varphi(n))$	d = 77 γιατί 5*77=1 mod96
Public key	P = {e,n}	
Secret key	S = {d, p, q}	

Έστω M = **19**

Αποστολέας, encryption $C = M^5 \bmod n = 19^5 \bmod 119 = 66$ → Repeated Squaring Algorithm:

Παραλήπτης, decryption $M = C^{77} \bmod n = 66^{77} \bmod 119 = \mathbf{19}$

Απόδειξη ορθότητας

- ✓ Θεώρημα: Για κάθε **M** στο **D**
  - **E(D (M)) = M** και
  - **D(E (M)) = M** για κάθε **M** στο **D**
- ✓ Απόδειξη:

Έστω $M \in Z_n$. Επειδή ο d είναι ο πολλαπλασιαστικός αντίστροφος του e, modulo $\varphi(n) = (p - 1)(q - 1)$, έχουμε

$ed = 1 + k\,\varphi(n)$ για κάποιο ακέραιο k.

i) Αν $M \neq 0 \pmod p$, έχουμε

$$M^{ed} \pmod p \equiv M^{1 + k\,\varphi(n)} \pmod p$$
$$\equiv M\,(M^{\varphi(n)})^k \pmod p$$
$$\equiv M\,(M^{p-1})^{k(q-1)} \pmod p$$
$$\equiv M \pmod p \text{ (από θεώρημα Fermat)}$$

ii) Αν $M = 0 \pmod p$, τότε πάλι $M^{ed} \pmod p \equiv M \pmod p$

- Απόδειξη ορθότητας
  - ✓ Άρα για κάθε M, $M^{ed} \pmod p \equiv M \pmod p$
  - ✓ Ομοίως $M^{ed} \pmod q \equiv M \pmod q$
  - ✓ Από Chinese Remainder Theorem: όταν n=pq, τότε x = y mod n αν και μόνο αν x=y mod p και x=y mod q
  - ✓ $\Rightarrow$ **D(E(M)) =** $M^{ed} \pmod n = M \pmod n$
- Πιο απλή απόδειξη όταν $M \in Z_n^*$ (gcd(M, n)=1):
  - ✓ ed = 1 + k φ(n) για κάποιο ακέραιο k.

$$\textbf{D(E(M))} = M^{ed} \equiv M^{1 + k\,\varphi(n)} \pmod n$$
$$\equiv M\,(M^{\varphi(n)})^k \pmod n$$
$$\equiv M \pmod n \text{ (από θεώρημα Fermat-Euler)}$$

Ασυμμετρία του RSA

- Συνήθως το e είναι σχετικά μικρός αριθμός ⇒ **γρήγορη κρυπτογράφηση**
- Π.χ. με $e = 2^{16} + 1$, έχουμε κρυπτογράφηση με 17 πολλαπλασιασμούς
- Το d είναι συνήθως μεγάλος αριθμός ⇒ **πιο αργή αποκρυπτογράφηση**
- Περίπου 2000 πολλαπλασιασμοί ή περισσότεροι
- RSA-Chinese Remaindering (RSA-CRT): Παραλλαγή του RSA για την επιτάχυνση της αποκρυπτογράφησης
  - Λειτουργίες στην αποκρυπτογράφηση γίνονται modp και modq
  - ≈ 4 φορές πιο γρήγορο

Κρυπτανάλυση του RSA

- Δυσκολία RSA
- Ciphertext-only ή Chosen ciphertext attack:
- Δεδομένου ακέραιου n που είναι γινόμενο δύο διαφορετικών πρώτων p και q, ενός ακεραίου e τέτοιου ώστε $\gcd(e, (p-1)(q-1)) = 1$, και ενός ακεραίου C, βρες ακέραιο M έτσι ώστε $M^e = C \pmod n$ (ή διαφορετικά βρες τον εκθέτη d)
- Ο ορισμός του προβλήματος και οι παράμετροι n και e εξασφαλίζουν ότι για κάθε ακέραιο $C \in \{0, 1, ..., n-1\}$ υπάρχει ένας ακριβώς $M \in \{0, 1, ..., n-1\}$ τέτοιος ώστε $M^e \equiv C \pmod n$.
- Η δυσκολία έγκειται ουσιαστικά στον υπολογισμό του εκθέτη d (decryption exponent)
  - Αν και δεν μπορούμε να αποκλείσουμε το ενδεχόμενο να σπάσουμε το RSA χωρίς απαραίτητα να υπολογίσουμε το d

Κρυπτανάλυση του RSA

- ✓ Δυσκολία RSA
- ✓ Εικασία: η συνάρτηση $f(x) = x^b \bmod n$, όπου n είναι γινόμενο 2 πρώτων είναι one-way function
- ✓ Αυτή τη στιγμή δεν υπάρχει καμία συνάρτηση που να είναι **αποδεδειγμένα** one-way
- ✓ Θεώρημα: Αν υπάρχουν one-way functions, τότε **P ≠ NP**
- ✓ Trapdoor στο RSA: φ(n)

Κρυπτανάλυση του RSA

- Αναγωγή στο integer factorization problem:
- Έστω ότι ο Oscar μπορεί να παραγοντοποιήσει εύκολα το n
  - Με το να βρει τους p και q, μπορεί να υπολογίσει το φ(n)
  - Στη συνέχεια μπορεί εύκολα να βρει το d έτσι ώστε de = 1 mod(φ(n)) με χρήση του extended Euclidean algorithm
- Για το αντίθετο ξέρουμε ότι:
- Θεώρημα: Ένας αλγόριθμος που υπολογίζει τον εκθέτη d σε ένα σύστημα RSA, μπορεί να μετατραπεί σε έναν πιθανοτικό αλγόριθμο παραγοντοποίησης του n (απόδειξη στο Stinson)
  - Άρα, αν αποκαλυφθεί το d, δεν αρκεί να αλλάξουν τα d, e, πρέπει να αλλάξει και το n
- **Προσοχή:** δεν σημαίνει απαραίτητα ότι η παραγοντοποίηση είναι ισοδύναμη με την κρυπτανάλυση του RSA

Κρυπτανάλυση του RSA

- ✓ Παρατήρηση: Για την παραγοντοποίηση του n, αρκεί να γνωρίζουμε το φ(n)
- ✓ Έστω ότι φ(n) γνωστό
- ✓ Μπορούμε να λύσουμε το σύστημα:

$$n = pq$$

$$\varphi(n) = (p-1)(q-1)$$

- ✓ Αν q = n/p, οι παράγοντες θα προέλθουν από τη διωνυμική εξίσωση $p^2 – (N – \varphi(n)+1)p + N = 0$
- ✓ Πόρισμα: Ο υπολογισμός του φ(n) δεν είναι ευκολότερος από την παραγοντοποίηση του n.

- Κρυπτανάλυση του RSA
- Στην πράξη:
  - ✓ Αν δουλέψουμε με modulus 1024 bits, τότε δημιουργείται ένα public key που είναι απαραβίαστο σε εύλογο χρονικό διάστημα με βάση την τρέχουσα γνώση και τεχνολογία ($n \approx 200$ decimal digits)
  - ✓ Factoring αλγόριθμοι πάνε σχετικά καλά μέχρι το πολύ 130 decimal digits
  - ✓ Ίσως όχι τόσο ασφαλές για το μέλλον όμως
  - ✓ NIST guidelines (2010): Από 1/1/2011, 1024-bit κλειδιά είναι “deprecated” (αποδεκτά αλλά με κάποιο μικρό ρίσκο)
    - 1/1/2014: 1024 bits μη αποδεκτά, μόνο 2048-bit κλειδιά

- Κρυπτανάλυση του RSA
- Μερική ανάκτηση πληροφοριών – Είναι εφικτό να μάθουμε έστω κάποια bits του plaintext?
- Έστω $y = x^e \bmod n$
  - ✓ Παρατήρηση: $E(x \cdot x') = E(x) \cdot E(x')$
- Έστω οι συναρτήσεις:
  - ✓ Parity(y) := LSB(x)
  - ✓ Half(y) := 0 αν x<n/2, 1 αν x> n/2 (n είναι περιττός αφού n=pq)
- Οι 2 συναρτήσεις είναι polynomial-time equivalent
  - ✓ $\text{Half}(y) = \text{parity}(y \cdot E(2) \bmod n) = \text{parity}(E(2x))$
  - ✓ $\text{Parity}(y) = \text{half}(y \cdot E(2^{-1}) \bmod n) = \text{half}(E(x \cdot 2^{-1}))$

- Κρυπτανάλυση του RSA
- Θεώρημα: Ένας αλγόριθμος που μπορεί να υπολογίσει το parity(y) ή το half(y) για οποιοδήποτε ciphertext y = E(x), μπορεί να χρησιμοποιηθεί για να υπολογίσει ολόκληρο το αρχικό κείμενο x.
- Έστω π.χ. αλγόριθμος που μπορεί να υπολογίσει το half(y) για οποιοδήποτε y
- Υπολόγισε τα

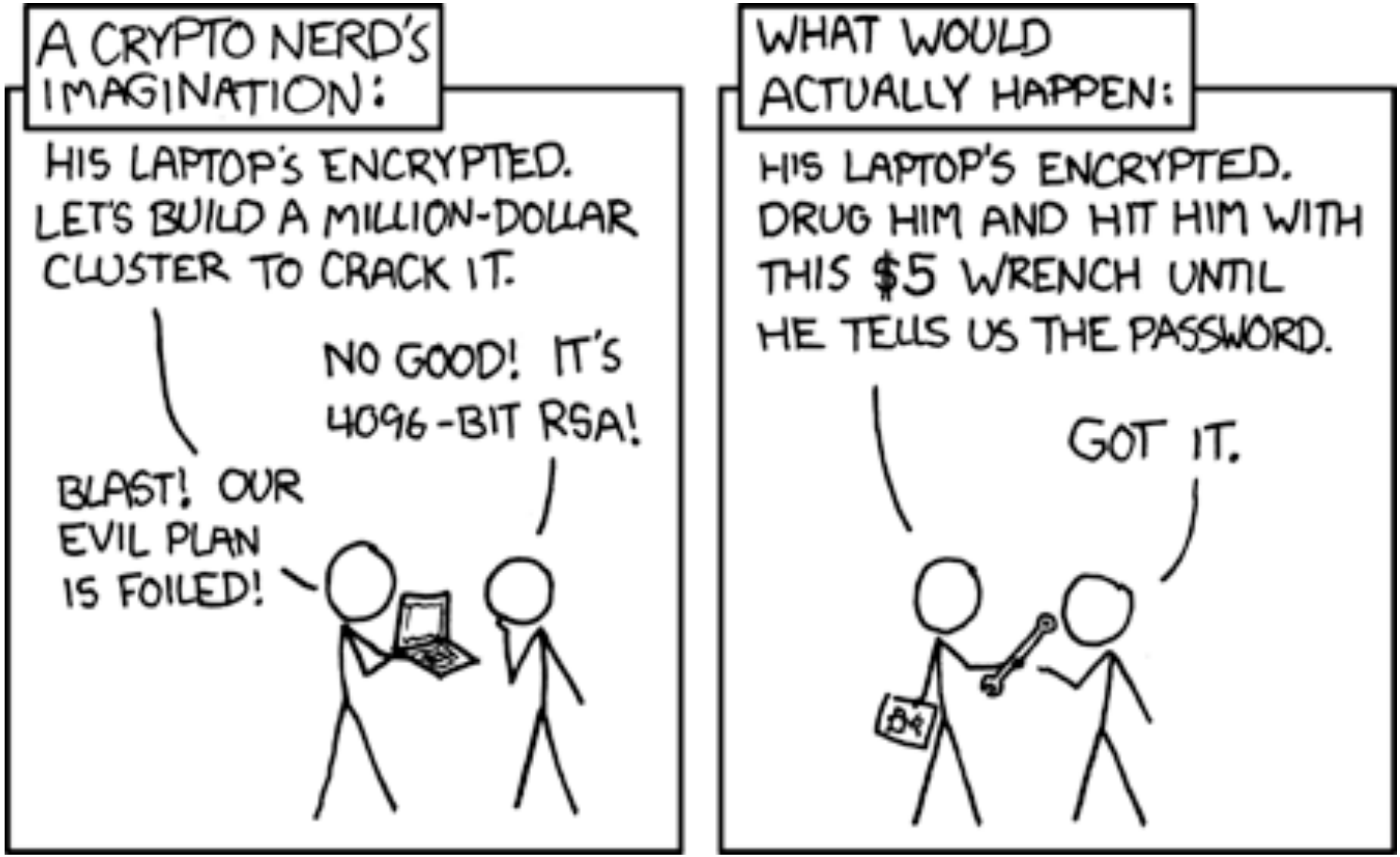
  $y_i = half(E(x \cdot 2^i))$ (τα οποία ισούνται με $half(E(x) \cdot E(2^i))$)
- Αν $half(E(x)) = 0 \Leftrightarrow x \in [0, n/2)$
- Αν $half(E(2x)) = 0 \Leftrightarrow x \in [0, n/4) \cup [n/2, 3n/4)$
- κ.ο.κ.
- Με binary search μπορούμε να βρούμε τελικά το x

- Κρυπτανάλυση του RSA
- Αλγόριθμος υπολογισμού του x, δεδομένου ενός αλγορίθμου για το half(y)

```
 k = ⌊logn⌋
for i=0 to k
    y_i = half(y)
    y = (y E(2)) modn
lo = 0
hi = n
for i=0 to k
   mid = (hi + lo)/2
   if y_i = 1 lo = mid
   else hi = mid
x = ⌊hi⌋
```

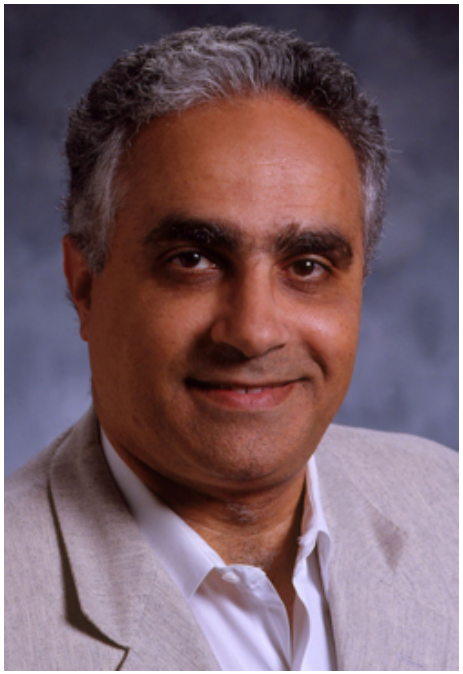
- Κρυπτανάλυση του RSA
- Άλλες γνωστές επιθέσεις (implementation attacks):
  - ✓ Timing attacks [Kocher '97]: Ο χρόνος υπολογισμού της αποκρυπτογράφησης μπορεί να δώσει πληροφορία για το d
  - ✓ Power attacks [Kocher '99]: Μετρώντας την κατανάλωση ενέργειας σε ένα smartcard κατά τη διάρκεια της εκτέλεσης του repeated squaring algorithm, μπορεί κανείς να διαβάσει τα bits του d
    - Πρέπει τα chips να μην επιδέχονται power analysis
  - ✓ Fault attacks [Lenstra '96, Boneh, de Millo, Lipton '97]: Αν γίνει έστω και ένα λάθος στον υπολογισμό της αποκρυπτογράφησης ο Oscar μπορεί να μαντέψει το d! (αφορά κυρίως το RSA-CRT)
    - Η μέθοδος δουλεύει αν έχουν γίνει σωστά οι υπολογισμοί modp και λάθος οι υπολογισμοί modq
    - Κοινή τακτική: Ελέγχουμε μετά την αποκρυπτογράφηση αν όντως έγιναν σωστά οι πράξεις. Θα πρέπει $(C^d)^e = C \bmod n$

- Κρυπτανάλυση του RSA



http://xkcd.com/538/

- Κρυπτοσύστημα ElGamal
  - ✓ T. Elgamal (1985)



- Προβλήματα διακριτού λογαρίθμου
  - ✓ Υπενθύμιση από προηγούμενα μαθήματα:
  - ✓ Αν p πρώτος, τότε το $Z^*_p = Z_p - \{0\}$ είναι κυκλική ομάδα
  - ✓ Αν g γεννήτορας (ή πρωτογενής ρίζα) τότε για κάθε a ε Z^*_p υπάρχει z τέτοιος ώστε $g^z \equiv a \pmod p$
    - Το z καλείται διακριτός λογάριθμος (discrete logarithm) του a, modulo p, με βάση το g
  - ✓ Αν θέλουμε να υπολογίσουμε την k-οστή δύναμη ενός στοιχείου:
    - Εύκολο πρόβλημα, χρήση του repeated squaring algorithm
    - Π.χ. στο Z^*_{17} με k=4, $3^4 \equiv 13 \bmod 17$

Προβλήματα διακριτού λογαρίθμου

- **Discrete logarithm στο Z_p (DLP)**: το αντίστροφο πρόβλημα της ύψωσης σε δύναμη
  - Δεδομένου ότι $3^k \equiv 13 \pmod{17}$, ποιο είναι το k?
  - Πιο γενικά: Δεδομένου γεννήτορα $g \in Z^*_p$, και ενός στοιχείου $\beta \in Z^*_p$, βρες το μοναδικό ακέραιο $k \in \{0, \ldots, p-1\}$ για τον οποίο $g^k \equiv \beta \pmod{p}$

- Θεωρείται δύσκολο πρόβλημα όταν το p έχει επιλεγεί προσεκτικά
  - Π.χ. για $p \approx 1024$ bits και όταν το p-1 έχει ένα «μεγάλο» πρώτο παράγοντα

- Σύστημα ElGamal (T. ElGamal, 1985)
- Βασίζεται στο DLP
- Ορίζεται στο $(Z^*_p, *)$
  - ✓ Παραγωγή κλειδιών
    - Αρχικά επιλέγεται ένας πρώτος τέτοιος ώστε το DLP να είναι δύσκολο στο $(Z^*_p, \cdot)$. Ενδεικτικός τρόπος:
    - Επέλεξε μεγάλο πρώτο p έτσι ώστε $p-1 = mq$ για κάποιο μικρό ακέραιο m και μεγάλο πρώτο q.
    - Π.χ., με m=2, επιλέγουμε πρώτα ένα μεγάλο πρώτο q και ελέγχουμε αν το p=2q+1 είναι πρώτος
      - Χρήση primality testing
    - Επέλεξε γεννήτορα $g \in Z^*_p$, (άρα $g^{p-1} \equiv 1 \bmod p$)
    - Επέλεξε στοιχείο $\alpha \in \{2,...,p-2\}$

Κρυπτοσύστημα ElGamal

- ✓ Παραγωγή κλειδιών
  - Έστω $\boldsymbol{K} = \{(p,g,\alpha,\beta): \beta \equiv g^{\alpha} \bmod p)\}$
  - Public Key: Οι τιμές p, g, β
  - Private Key: ο εκθέτης α
- ✓ Αλγόριθμος κρυπτογράφησης (μηνύματος x)
  - Για K=(p,g,α,β) η Alice διαλέγει μυστικό τυχαίο αριθμό *k* ε Z^*_{p-1} και στέλνει $E_K(x,k) = (y_1, y_2)$, όπου
    - $y_1 = g^k \bmod p$
    - $y_2 = x\beta^k \bmod p$ //μάσκα πάνω στο x
- ✓ Αλγόριθμος αποκρυπτογράφησης
  - Για τα y_1, y_2 η συνάρτηση αποκρυπτογράφησης ορίζεται ως:
    - $D_K(y_1, y_2) = y_2(y_1^{\alpha})^{-1} \bmod p$
      - Η οποία παράγει το x

- Κρυπτοσύστημα ElGamal
- Απόδειξη ορθότητας
  - Η $D_K(y_1, y_2)=y_2(y_1^{\alpha})^{-1} \mod p$ παράγει το x
    - Πράγματι:

$$y_2(y_1^{\alpha})^{-1}$$
$$= x\beta^k ((g^k)^{\alpha})^{-1}$$
$$= x\beta^k ((g^{\alpha})^k)^{-1}$$
$$= x\beta^k ((\beta)^k)^{-1} \quad (\text{γιατί } \beta \equiv g^{\alpha} \mod p)$$
$$= x$$

- Χαρακτηριστικά
  - ✓ Το plaintext **x** «μασκαρεύεται» με πολλαπλασιασμό με $\boldsymbol{\beta^k}$ (παράγεται το $\mathbf{y_2}$)
  - ✓ Στο ciphertext μεταδίδεται και η τιμή $\mathbf{g^k}$
  - ✓ Ο Bob που γνωρίζει το ιδιωτικό του κλειδί **α** μπορεί να παράγει το $(y_1)^{\alpha}$
  - ✓ Κατόπιν αφαιρεί τη μάσκα με το να πολλαπλασιάζει το $\mathbf{y_2}$ με τον αντίστροφο του $\boldsymbol{\beta^k}$

Παράδειγμα

- ✓ Έστω p = 2579, g = 2, α = 765
- ✓ $\beta = 2^{765} \bmod 2579 = 949$
- ✓ Έστω ότι η Alice θέλει να στείλει το μήνυμα x = 1299
- ✓ Έστω επίσης ότι διαλέγει τυχαίο k = 853

- ✓ Τότε:
  - $y_1 = 2^{853} \bmod 2579 = 435$
  - $y_2 = 1299\ (949)^{853} \bmod 2579 = 2396$

- ✓ ο Bob υπολογίζει το
  - $2396\ (435^{765})^{-1} \bmod 2579 = 1299$

- Κρυπτανάλυση του ElGamal
  - ✓ Για known ciphertext attack, η κρυπτανάλυση μπορεί να αναχθεί στο discrete logarithm problem
- Δεδομένων των (p, g, β) και των (y_1, y_2), ο Oscar θα πρέπει
  - ✓ είτε να υπολογίσει τον εκθέτη α, από τη σχέση $\beta = g^{\alpha} \bmod p$ (DLP)
  - ✓ είτε να βρει το k από τη σχέση $y_1 = g^{k} \bmod p$ (πάλι DLP)

- Κρυπτανάλυση του ElGamal
- Γνωστοί αλγόριθμοι για το Discrete Logarithm problem
  - ✓ Shank's algorithm
  - ✓ Pohlig-Hellman algorithm
  - ✓ The Index Calculus method (μοιάζει με αλγορίθμους παραγοντοποίησης)

- Κρυπτανάλυση - Bit Security των διακριτών λογαρίθμων
  - ✓ Στο κρυπτοσύστημα ElGamal, το LSB του εκθέτη α μπορεί να υπολογιστεί σε πολυωνυμικό χρόνο
  - ✓ Από θεωρία τετραγωνικών υπολοίπων mod p, ισούται με:
    - 0, αν $\beta^{(p-1)/2} \equiv 1 \bmod p$
    - 1, διαφορετικά
  - ✓ Τα υπόλοιπα bits όμως είναι (μάλλον) δύσκολο να υπολογιστούν
  - ✓ Θεώρημα: Αν $p \equiv 3 \bmod 4$, ένας αλγόριθμος που υπολογίζει το 2^o bit του εκθέτη μπορεί να χρησιμοποιηθεί για να λύσει το DLP

- Άλλα public key cryptosystems

  - ✓ Merkle-Hellman Knapsack systems, all broken except:
    - Chor-Rivest
  - ✓ McEliece
  - ✓ Elliptic Curve systems

Γενικά Χαρακτηριστικά - Απαιτήσεις

- Bit pattern που εξαρτάται από το μήνυμα που θα υπογραφεί
- Χρησιμοποιεί κάποιου είδους πληροφορία που είναι μοναδική για τον αποστολέα (π.χ., δημόσιο κλειδί)
  - ✓ Για αποφυγή πλαστογραφίας και απάρνησης
- Πρέπει να:
  - ✓ Είναι υπολογιστικά εύκολο να δημιουργηθεί
  - ✓ Είναι εύκολα αναγνωρίσιμη και επαληθεύσιμη
  - ✓ Είναι υπολογιστικά ανέφικτο να πλαστογραφηθεί με τους εξής τρόπους:
    - Με το να παραχθεί ένα νέο μήνυμα με χρήση της ίδιας ψηφιακής υπογραφής
    - Με το να παραχθεί μία άλλη ψηφιακή υπογραφή για ένα δεδομένο μήνυμα

Προϋποθέσεις και λύσεις

- Υποθέτει ότι ο παραλήπτης διαθέτει το δημόσιο κλειδί του αποστολέα
- Η συνολική ασφάλεια του σχήματος εξαρτάται από το ιδιωτικό κλειδί του αποστολέα

- Δύο προσεγγίσεις του σχήματος
  - ✓ Direct Digital Signature (άμεση)
  - ✓ Arbitrated Digital Signature (με μεσολάβηση διαιτητή)

Direct Digital Signature

- Εμπλέκει μόνο αποστολέα και παραλήπτη

- Ένα σύστημα υπογραφών (signature scheme) αποτελείται από:
  - ✓ *P*: χώρος μηνυμάτων e.g. Z_n
  - ✓ *S*: χώρος πιθανών υπογραφών
  - ✓ Signing algorithm sig_A (.): $P \rightarrow S$ για κάθε χρήστη A (secret)
  - ✓ Verification algorithm ver(x,y) (public)
  - ✓ Ο αποστολέας στέλνει το μήνυμα x και την υπογραφή y
  - ✓ Για μήνυμα που ήλθε από A, ver(x,y) = true iff $y = sig_A(x)$

Direct Digital Signature

- Μπορεί να υλοποιηθεί με χρήση μεθόδων δημόσιου κλειδιού
- Ιδέα: χρήση του decryption algorithm από ένα public key cryptosystem ως signing algorithm
- Αδυναμία:
  - ✓ Ο αποστολέας μπορεί να αποποιηθεί την αποστολή του μηνύματος
    - Μπορεί να ισχυριστεί ότι το ιδιωτικό του κλειδί έχει παραβιαστεί η κλαπεί
    - Ότι ο κλέπτης χρησιμοποίησε το ιδιωτικό κλειδί για πλαστογραφία
  - ✓ Αναγκαία μέθοδος προσδιορισμού του επιπέδου εμπιστοσύνης του αποστολέα

- RSA signature scheme
  - ✓ Έστω ότι η Alice έχει διαλέξει (n, p, q, d, e), με n=pq, de = 1 mod φ(n)
  - ✓ Signing algorithm of Alice: $sig_A(x) = x^d \bmod n = D_A(x)$
  - ✓ Verification: ver(x, y) = true iff $x = y^e \bmod n$

Άρα όταν η Alice θέλει να στείλει υπογεγραμμένο μήνυμα x:

- ✓ Υπογράφει το x, παράγοντας το $y = sig_A(x)$
- ✓ Κρυπτογραφεί το ζεύγος (x, y), και τα στέλνει στον Bob
- ✓ Ο Bob τα αποκρυπτογραφεί και μετά ελέγχει αν ver(x, y) = true

- RSA signature scheme

1. Καθένας μπορεί να παράγει υπογραφή για ένα «τυχαίο» μήνυμα

   - Διάλεξε y. Υπολόγισε το x = e(y). Το y είναι η υπογραφή του x

   - μπορούμε να προσθέσουμε πληροφορίες (ημερομηνία κτλ) ώστε το x να μην αντιστοιχεί σχεδόν ποτέ σε κάποιο meaningful μήνυμα

2. Αν πρώτα κρυπτογραφήσει το x και μετά το υπογράψει?

   - ο Oscar τότε μπορεί να έχει πρόσβαση στο e(x). Μπορεί να το υπογράψει με τη δική του υπογραφή και να το στείλει στον Bob

   - Συνήθης τακτική: πρώτα υπογράφουμε και μετά κρυπτογραφούμε

- ElGamal signature scheme

  - ✓ Έστω ότι η Alice διαλέγει (p,g,α,β), όπου, g είναι γεννήτορας του Z_p^*, $\beta \equiv g^{\alpha} \bmod p$ και ο p έχει επιλεγεί έτσι ώστε το discrete logarithm να είναι δύσκολο στο Z_p.
  - ✓ Public: (p, g, β), secret: α
  - ✓ Signing algorithm: διάλεξε τυχαίο ακέραιο k και:

$$sig(x, k) = (\gamma, \delta),$$

$$\gamma = g^k \bmod p, \quad \delta = (x - \alpha\gamma)k^{-1} \bmod (p-1)$$

  - ✓ Verification:

$$ver(x, (\gamma, \delta)) = true \text{ iff } \beta^{\gamma} \gamma^{\delta} = g^x \bmod p$$

- ElGamal signature scheme

  - ✓ Ορθότητα:
  - ✓ $\beta^{\gamma}\ \gamma^{\delta} \equiv g^{\alpha\gamma+\kappa\delta}$
  - ✓ $\alpha\gamma+\kappa\delta \equiv x \bmod (p-1)$
  - ✓ $\alpha\gamma+\kappa\delta = \lambda(p-1) + x$
  - ✓ Η ορθότητα προκύπτει από θεώρημα Fermat.

- ElGamal signature scheme
  - ✓ Ασφάλεια του συστήματος:
  - ✓ Έστω ότι ο Oscar θέλει να υπογράψει ως Alice ένα μήνυμα x
  - ✓ Πρέπει να υπολογίσει τα (γ, δ)
  - ✓ Αν διαλέξει ένα γ και προσπαθεί να βρει το δ πρέπει να βρει το διακριτό λογάριθμο του $g^x(\beta^\gamma)^{-1}$ με βάση το γ
  - ✓ Αν διαλέξει ένα δ, τότε πρέπει να λύσει ως προς γ την εξίσωση $\beta^\gamma \gamma^\delta = g^x \bmod p$
    - Δεν σχετίζεται με διακριτό λογάριθμο αλλά θεωρείται δύσκολο πρόβλημα
  - ✓ Αν διαλέξει ένα ζεύγος (γ, δ), για να βρει σε ποιο μήνυμα αντιστοιχούν πρέπει πάλι να βρει το διακριτό λογάριθμο του $\beta^\gamma \gamma^\delta$ με βάση το g.

- Signature schemes και Hash functions

  - ✓ Το μέγεθος των υπογραφών μπορεί να είναι μεγάλο
  - ✓ Π.χ. Στο ElGamal θέλουμε 2048 bits!
  - ✓ Σχεδόν σε όλα τα συστήματα στην πράξη χρησιμοποιούμε και μια hash function για να μειώσουμε το μέγεθος (υπογράφουμε το hash του μηνύματος)

Plaintext x

⬇

z = h(x)

⬇

Υπογραφή $y = sig_K(z)$

Χρειάζεται όμως η hash function να ικανοποιεί κάποιες προδιαγραφές (επόμενη διάλεξη)

Ψηφιακές υπογραφές

- Digital Signature Standard (or the Digital Signature Algorithm- DSA)
  - ✓ Παραλλαγή του ElGamal scheme
  - ✓ Αρχική πρόταση NIST (1991): $p \approx 512$ bits
  - ✓ Μετέπειτα (2001): Recommendation για $p \approx 1024$ bits
  - ✓ Από 1/1/2014: $p \approx 2048$ bits
  - ✓ Εφαρμογή υπογραφής σε hash του μηνύματος
  - ✓ Μειώνει σημαντικά το μέγεθος της υπογραφής
  - ✓ Με $p \approx 1024$ bits, μέγεθος υπογραφής $\approx 2 \times 160 = 320$ bits

- DSA signature scheme

  - ✓ Έστω ότι η Alice διαλέγει (p,g,α,β), όπου, g είναι γεννήτορας του Z_p^*, $\beta \equiv g^{\alpha} \bmod p$ και ο p έχει επιλεγεί έτσι ώστε το discrete logarithm να είναι δύσκολο στο Z_p
  - ✓ Μπορούμε να διαλέξουμε τον p με L bits, όπου $512 \leq L \leq 1024$ και $L \equiv 0 \bmod 64$
  - ✓ Η Alice διαλέγει επίσης έναν πρώτο q με 160 bits έτσι ωστε $q \mid p-1$
  - ✓ Public: (p,q, g, β), secret: α

DSA signature scheme

- ✓ Public: (p,q, g, β), secret: α
- ✓ Signing algorithm: διάλεξε τυχαίο ακέραιο k με $1 \le k \le q-1$ και:

$$sig(x, k) = (\gamma, \delta),$$

$$\gamma = (g^k \bmod p) \bmod q, \quad \delta = (SHA\text{-}1(x) + \alpha\gamma)k^{-1} \bmod q$$

- ✓ Verification:

$$e1 = SHA\text{-}1(x)\, \delta^{-1} \bmod q$$

$$e2 = \gamma\delta^{-1} \bmod q$$

$$ver(x, (\gamma, \delta)) = true \text{ iff } (g^{e1}\, \beta^{e2} \bmod p) \bmod q = \gamma$$

- ✓ SHA-1: Secure Hash Algorithm

Ψηφιακές υπογραφές

- Other signature schemes
- One-time signatures (ασφαλείς όταν υπογράφεται μόνο ένα μήνυμα)
  - ✓ Με χρήση one-way functions
- Undeniable signatures (χρειάζονται τη συνεργασία της Alice για την επιβεβαίωση)
  - ✓ Αποτρέπει τον Bob από το να αναπαράγει και να προωθήσει σε άλλους υπογεγραμμένα μηνύματα της Alice
  - ✓ Verification algorithm: Challenge-and-response protocol
  - ✓ Disavowal protocol (για να μην μπορεί να αποποιηθεί την υπογραφή της η Alice, αλλά και για να μπορεί η Alice να αποδείξει αν έγινε πλαστογραφία)
  - ✓ Chaum-van Antwerpen scheme, βασισμένο στο DLP
- Fail-stop signatures (αυξημένη ασφάλεια κατά της πλαστογραφίας)
  - ✓ Έχουν και "proof of forgery" algorithm

Arbitrated Digital Signatures

- Εμπλέκει αρχή ***Δ α τησ ας*** (Arbiter)
- Υποβάλει το μήνυμα του αποστολέα και την υπογραφή του σε σειρά δοκιμασιών για να ελέγξει την αυθεντικότητα του
- Μετά από έλεγχο, ο ***Δ α τητής***
  - ✓ Προσθέτει ημερομηνία στο μήνυμα
  - ✓ Προσθέτει ένδειξη επικύρωσης από ***Δ α τητή***
  - ✓ Αποστέλλει στον παραλήπτη:
    - Μήνυμα με υπογραφή αποστολέα, ημερομηνία, ένδειξη διαιτησίας
- Απαιτεί ισχυρό επίπεδο εμπιστοσύνης και των δύο μερών απέναντι στον ***Δ α τητή***
- Μπορεί να υλοποιηθεί με χρήση συμμετρικής ή κρυπτογραφίας δημοσίου κλειδιού

Ελλειπτικές Καμπύλες

- Κρυπτογραφία ελλειπτικών καμπυλών
- [Miller ’86, Koblitz ’87]
- Ευρύτερη χρήση από το 2004 και μετά
- NIST approval: 2006
- Σημαντικό πλεονέκτημα: μείωση του μεγέθους του κλειδιού για ίδιο επίπεδο ασφάλειας με άλλα public-key systems
- Εφαρμογές: Bitcoin, SSH (about 10% of ssh implementations), Austrian citizen card, etc

Ελλειπτικές Καμπύλες

- Ιδέα: Ψάχνουμε αβελιανές ομάδες όπου το πρόβλημα διακριτού λογαρίθμου είναι δύσκολο (γενίκευση του συστήματος ElGamal)

- **Το Πρόβλημα Διακριτού Λογαρίθμου (DLP) σε μία ομάδα (G, ⊗)**:

  Έστω G πεπερασμένη ομάδα, g ϵ G, και β ϵ H, όπου H = $\{g^{(r)}, r \geq 0\}$, είναι η κυκλική υποομάδα που δημιουργείται από το g.

  Βρες το μοναδικό ακέραιο k ϵ {0,…, |H|-1} για τον οποίο $g^{(k)} = \beta$,

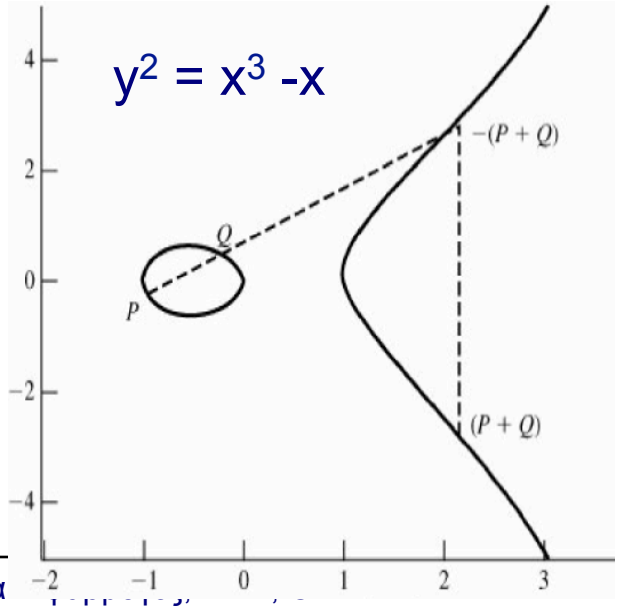
  - Όπου $g^{(k)} = g \otimes g \otimes g \otimes \ldots \otimes g$ (k φορές)
  - Π.χ. Στο $(Z_n, +)$, $g^{(k)} = kg$

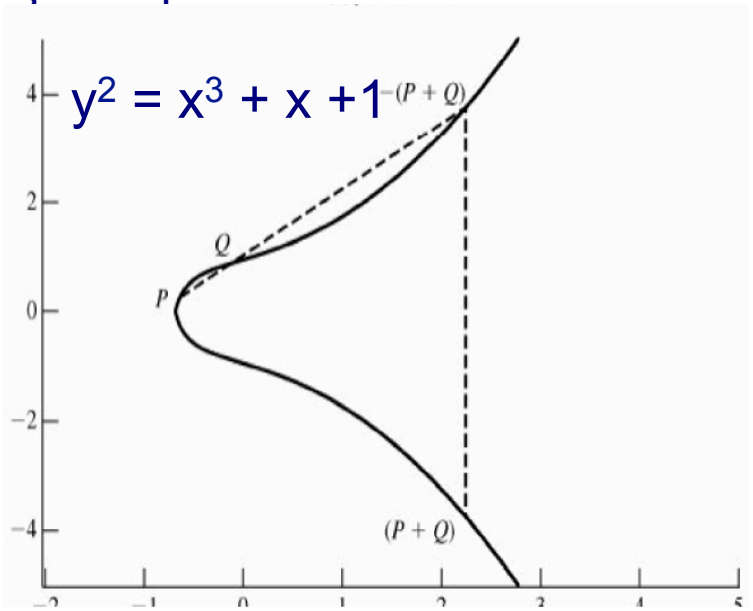
Κρυπτογραφία Ελλειπτικών Καμπυλών

- ✓ Ελλειπτικές Καμπύλες στο σώμα των πραγματικών
- ✓ Ελλειπτικές Καμπύλες ορισμένες modp
- ✓ Ελλειπτικές Καμπύλες στο $GF(2^m)$
- ✓ Ελλειπτικές Καμπύλες και πρόβλημα διακριτού λογαρίθμου

Ελλειπτικές Καμπύλες

- ✓ Δεν είναι ελλείψεις
- ✓ Στη γενική μορφή τους ορίζονται από:
  - $y^2 + axy + by = x^3 + cx^2 + dx + e$
  - a, b, c, d, e πραγματικοί αριθμοί
  - x και y παίρνουν τιμές από το R
- ✓ Περιοριζόμαστε στην ειδική μορφή
  - **$y^2 = x^3 + ax + b$** Εξίσωση 1

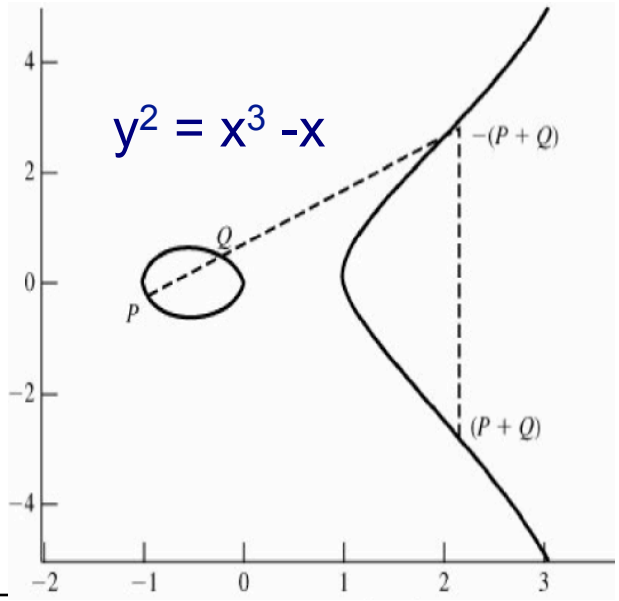


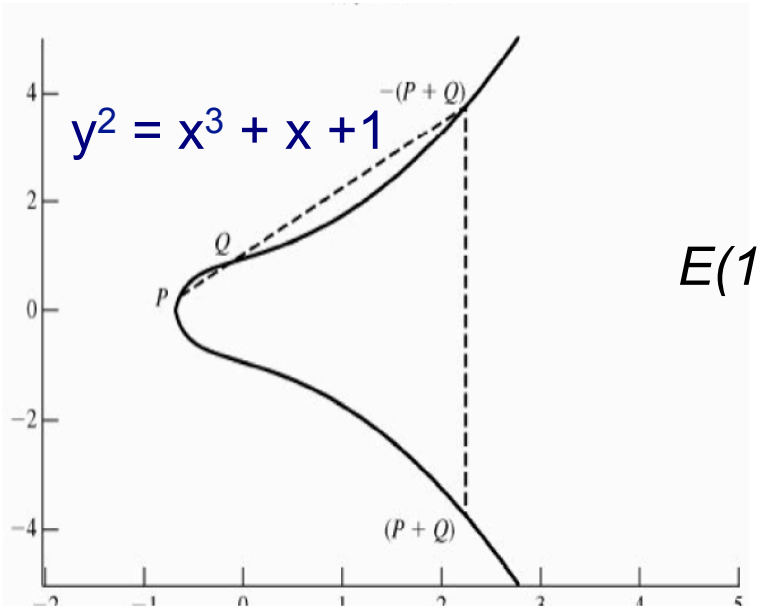


Ελλειπτικές Καμπύλες

- ✓ Ορισμός: Για a,b ∈R, η ελλειπτική καμπύλη $\mathbf{y^2 = x^3 + ax + b}$ είναι το σύνολο των σημείων (x, y) που ικανοποιούν την εξίσωση μαζί με ενα ειδικό σημείο O που καλείται *σημείο στο άπειρο* (point at infinity or zero point)
- ✓ Ορολογία: *E(a, b)* = τα σημεία (x, y) της ελλειπτικής καμπύλης μαζί με το σημείο *O*.
- ✓ Οι ελλειπτικές καμπύλες που θεωρούμε είναι συμμετρικές ως προς τον άξονα x

E(-1,0)





E(1, 1)

- Ελλειπτικές Καμπύλες
  - ✓ Θα δείξουμε ότι τα σημεία της ελλειπτικής καμπύλης αποτελούν αβελιανή ομάδα (abelian group) με βάση μία ειδική πράξη που θα την λέμε «πρόσθεση»
  - ✓ Υπό τη συνθήκη όμως ότι $4a^3 + 27b^2 \neq 0$
  - ✓ Γεωμετρική ερμηνεία της πρόσθεσης: Αν τρία σημεία στην *E* ανήκουν σε ευθεία, το άθροισμα τους πρέπει να είναι το ουδέτερο στοιχείο
  - ✓ Ουδέτερο στοιχείο: το σημείο *O*. Για κάθε σημείο P στην *E*, P+*O* = O + P = P
  - ✓ Ύπαρξη αντιστρόφου: για κάθε P ≠ O, ο αντίστροφος ορίζεται ως το mirror image ως προς τον άξονα x
    - Αν P = (x, y), τότε -P = (x, -y), P + (-P) = O
    - Ενώνονται με κατακόρυφη ευθεία

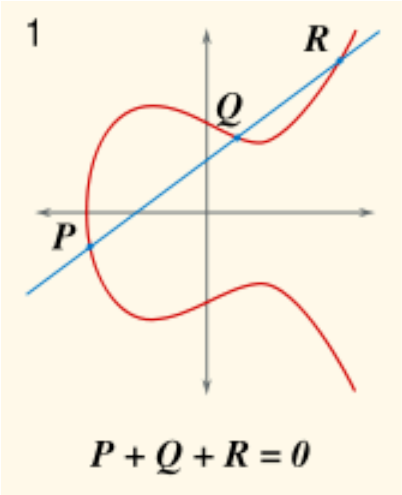
- Ελλειπτικές Καμπύλες – Γεωμετρική ανάλυση
  - ✓ Ορισμός της πρόσθεσης
  - ✓ Έστω ότι θέλουμε να προσθέσουμε τα σημεία $P=(x_1, y_1)$, και $Q=(x_2, y_2)$ της *E*. Το αποτέλεσμα θα είναι κάποιο σημείο $R = (x_3, y_3)$ της *E*
  - ✓ $1^η$ περίπτωση: $x_1 != x_2$
    - Έστω L η γραμμή που διέρχεται από P και Q
    - Έστω R' το 3ο σημείο τομής (πλην P και Q) της L με *E* (υπάρχει λόγω της συνθήκης $4a^3 + 27b^2 \neq 0$)
    - Το αποτέλεσμα της πρόσθεσης είναι το είδωλο του R' ως προς άξονα x, δηλαδή ο αντίστροφος του R'
    - P+Q = R, όπου R = -R'
    - Ποιες είναι οι συντεταγμένες του;
    - Η ευθεία L έχει εξίσωση $y = λx+μ$, όπου $λ=(y_2-y_1) / (x_2-x_1)$ και $μ =y_1 - λx_1 = y_2-λx_2$
    - Για να βρούμε το σημείο τομής L και *E* αντικαθιστούμε την $y=λx+ μ$ στην εξίσωση της καμπύλης

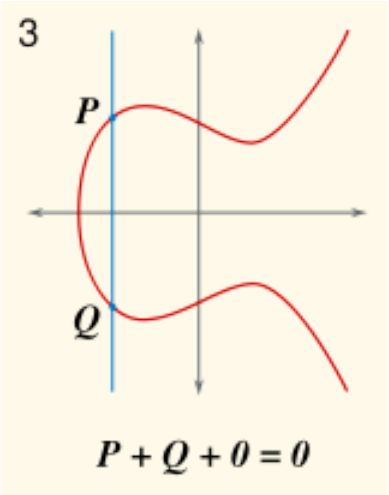
- Ελλειπτικές Καμπύλες – Γεωμετρική ανάλυση
  - ✓ 1η περίπτωση: $x_1 != x_2$ (συνέχεια)
    - $(\lambda x+\mu)^2= x^3 + ax^2 + b =>$
      $x^3 – \lambda^2x^2 + (a – 2\lambda\mu)x + b – \mu^2 = 0$ (Εξ. 2)
    - Οι ρίζες τις εξίσωσης είναι οι χ συντεταγμένες του σημείου τομής *E* και L
    - Αλλά ήδη ξέρουμε τις δύο λύσεις: x_1 και x_2
    - Εφόσον δύο λύσεις είναι στους πραγματικούς, τότε και η τρίτη λύση x_3 στους πραγματικούς. Μάλιστα, το άθροισμα θα πρέπει να είναι ίσο με το μείον του συντελεστή του τετραγώνου: $x_1 + x_2 + x_3 = \lambda^2 => x_3 = \lambda^2 - x_1 - x_2$
    - Έστω ότι η y-συντεταγμένη του R’ είναι $–y_3$
    - Η κλίση της L γράφεται και ως $\lambda=(-y_3-y_1) / (x_3-x_1)$. Άρα από εδώ προσδιορίζουμε το $y_3= \lambda (x_1-x_3)-y_1$
    - Ορίστηκε επομένως η πρόσθεση για $x_1 != x_2$

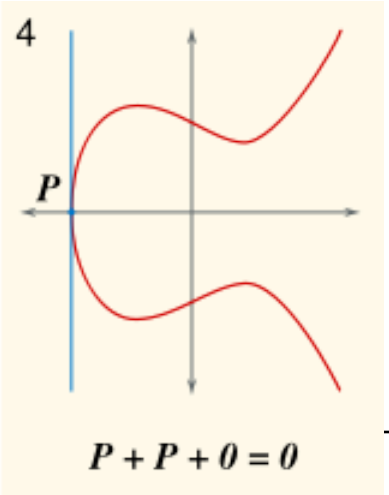
- Ελλειπτικές Καμπύλες – Γεωμετρική ανάλυση
  - ✓ $2^{η}$ περίπτωση: $x_1 = x_2$ και $y_1 = - y_2$
    - Απλή. Τα σημεία είναι αντίθετα
    - (x,y) + (x,-y) = *O* για κάθε (x,y) της *E*
  - ✓ $3^{η}$ περίπτωση: $x_1 = x_2$ και $y_1 = y_2$
    - Πρόσθεση σημείου $P = (x_1, y_1)$ στον εαυτό του
    - Αν $y_1 = 0$, P + P = *O*
    - Αλλιώς, παίρνουμε ως L την εφαπτομένη της *E* στο P
    - Το P+P είναι το είδωλο του σημείου όπου η εφαπτομένη τέμνει την *E*
    - Η κλίση λ της L θα προκύψει με μερική παράγωγο της *E*
    - $2y\,(dy/dx) = 3x^2+a \rightarrow \lambda = (3x^2+a)/2y$
    - Αντικαθιστώντας το x με x_1 και y με y_1 έχουμε γνωστό το $\lambda=(3x_1^2+a)/2y_1$
    - Η υπόλοιπη ανάλυση όπως στην περίπτωση 1

Ελλειπτικές Καμπύλες – Γεωμετρική ανάλυση

- ✓ Με βάση τα ανωτέρω, ορίσαμε σε μία ελλειπτική καμπύλη την πράξη + για την οποία ισχύουν οι ιδιότητες:
  - Κλειστή
  - Αντιμεταθετική
  - *O* είναι το ουδέτερο στοιχείο
  - Κάθε σημείο στο *E* έχει αντίθετο
  - Προσεταιριστική (πιο δύσκολη απόδειξη αλλά θα την παραλείψουμε)
- ✓ (*E*, +) είναι αβελιανή ομάδα







Ελλειπτικές Καμπύλες στο σώμα Z_p

- ✓ p πρώτος αριθμός
- ✓ cubic equation στην οποία οι μεταβλητές και οι συντελεστές έχουν τιμές από 0 έως p-1
- ✓ Οι υπολογισμοί γίνονται modulo p.
  - **$y^2 \bmod p = (x^3 + ax + b) \bmod p$** Εξίσωση 3
- ✓ Παράδειγμα: Η εξίσωση 3 ικανοποιείται για a=1, b=1, x=9, y=7, p=23:

$7^2 \bmod 23 = (9^3 + 9 + 1) \bmod 23$

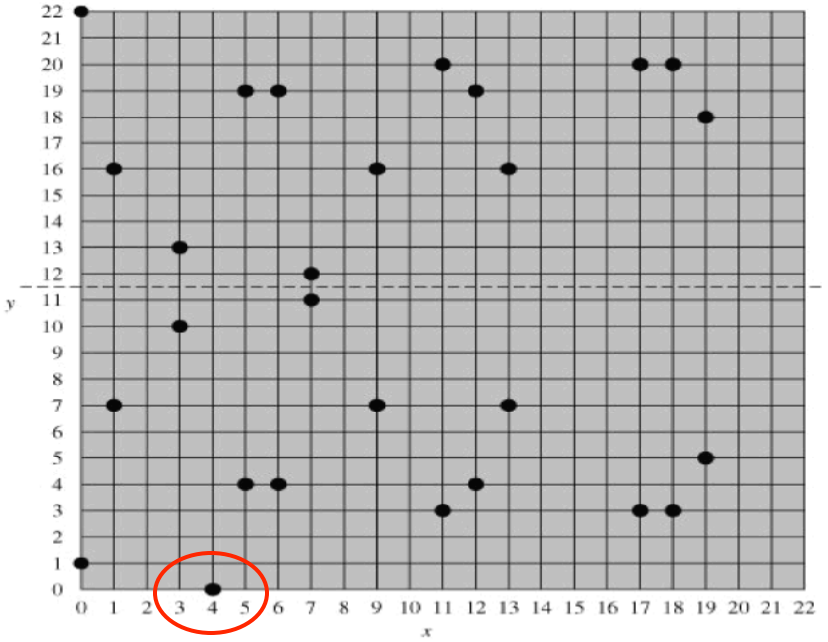
$49 \bmod 23 = 739 \bmod 23$

$3 = 3$

- Ελλειπτικές Καμπύλες στο σώμα Z_p
  - ✓ Έστω σύνολο $E_p(a, b)$ από τα ζεύγη (x,y) που ικανοποιούν την Εξίσωση 3 μαζί με ένα σημείο στο άπειρο *O*.
  - ✓ Απαιτούμε πάλι $4a^3 + 27b^2 \neq 0 \pmod p$,
  - ✓ Έστω p=23 και έστω η "καμπύλη" $E_{23}(1,1)$: $y^2 = x^3 + x + 1$ δηλαδή a=b=1.
  - ✓ Η καμπύλη τώρα περιέχει σημεία στο grid `{0, p-1}x{0, p-1}` που ικανοποιούν την εξίσωση

- Ελλειπτικές Καμπύλες στο σώμα Z_p
  - ✓ Ο πίνακας περιέχει όλα τα σημεία (εκτός *O*) που ανήκουν στην $E_{23}(1,1)$.
  - ✓ Όλα (πλην ενός) είναι συμμετρικά στο y=11,5

(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13, 16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 3)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)



- Ελλειπτικές Καμπύλες στο σώμα Z_p
  - ✓ Οι κανόνες άθροισης στο $E_p(a,b)$ αντιστοιχούν στις αλγεβρικές τεχνικές για EC στο σώμα των πραγματικών
  - ✓ Για όλα τα σημεία P, Q του $E_p(a, b)$
  - ✓ $P + O = P$
  - ✓ Αν $P = (x_P, y_P)$ τότε $P + (x_P, -y_P) = O$. Το σημείο $(x_P, -y_P)$ είναι το αντίθετο του P, που συμβολίζεται ως –P.
    - ✓ Π.χ. $E_{23}(1,1)$, για P = (13,7), έχουμε -7 mod23 = 16.
    - ✓ Άρα –P = (13, -7)=(13, 16), που ανήκει στο $E_{23}(1,1)$.
  - ✓ Αν $P = (x_P, y_Q)$ και $Q = (x_Q, y_Q)$ με $P \neq Q$, τότε R=P+Q= (x_R,y_R) όπου

    $x_R = (\lambda^2 - x_P - x_Q) \bmod p$

    $y_R = (\lambda(x_P - x_R) - y_P) \bmod p$ και

$$\lambda = \begin{cases} \left(\frac{y_Q - y_P}{x_Q - x_P}\right) \bmod p & \text{if } P \neq Q \\ \left(\frac{3x_P^2 + a}{2y_P}\right) \bmod p & \text{if } P = Q \end{cases}$$

- Ελλειπτικές Καμπύλες στο σώμα Z_p

Ο πολλαπλασιασμός ορίζεται ως επαναληπτική πρόσθεση: 4P = P + P + P + P.

- ✓ Έστω P=(3,10) και Q = (9,7) στην $E_{23}(1,1)$ τότε
  - ✓ λ=(7-10)/(9-3)mod23=((-1)/2)mod23=11 (από EEA)
  - ✓ $x_R = (11^2 - 3 - 9) \bmod 23 = 109 \bmod 23 = 17$
  - ✓ $y_R = (11(3 - 17) - 10) \bmod 23 = -164 \bmod 23 = 20$
  - ✓ Άρα P + Q = (17, 20).
- ✓ Για να βρω P+P=2P χρήση 2ης περίπτωσης λ (P=Q)
  - ✓ λ=[(3(3)^2+1)/(2x10)]mod23=(5/20)mod23=(1/4)mod23=6 (από EEA)
  - ✓ $x_R = (6^2 - 3 - 3) \bmod 23 = 30 \bmod 23 = 7$
  - ✓ $y_R = (6(3 - 7) - 10) \bmod 23 = (-34) \bmod 23 = 12$
  - ✓ Άρα 2P = (7, 12).

- Ελλειπτικές Καμπύλες στο σώμα Z_p
  - ✓ Για τον υπολογισμό της ασφάλειας των Elliptic Curve Cryptosystems, είναι ενδιαφέρον να γνωρίζουμε τον αριθμό των σημείων στην αβελιανή ομάδα, και την ύπαρξη «μεγάλων» κυκλικών υποομάδων.
  - ✓ Στην περίπτωση του $E_p(a,b)$, ο αριθμός N των σημείων οριοθετείται από

$$p + 1 - 2\sqrt{p} \leq N \leq p + 1 + 2\sqrt{p}$$

  - ✓ Θεώρημα: Υπάρχουν πάντα ακέραιοι n_1, n_2 με $n_2 \mid n_1$, έτσι ώστε το (E, +) να είναι ισομορφικό με το

$$Z_{n_1} \times Z_{n_2}$$

  - ✓ Πόρισμα: Το (E,+) έχει κυκλική ομάδα ισομορφική με το Z_{n1} (υποψήφια για χρήση στο ElGamal). Αν το N είναι πρώτος ή γινόμενο πρώτων, τότε το ίδιο το (E, +) είναι κυκλική ομάδα

ECC – GF(2^m)

- Ελλειπτικές Καμπύλες στο σώμα GF(2^m)
  - ✓ Το πεδίο GF(2^m) αποτελείται από 2^m στοιχεία και είναι εφοδιασμένο με πρόσθεση και πολλαπλασιασμό επί πολυωνύμων.
  - ✓ Για ελλειπτικές καμπύλες στο GF(2^m) οι μεταβλητές και οι συντελεστές παίρνουν τιμές από το GF(2^m)
  - ✓ Αριθμητική πραγματοποιείται με κανόνες στο GF(2^m)
  - ✓ Εξίσωση ελλειπτικής καμπύλης:
    - **$y^2 + xy = x^3 + ax^2 + b$** Εξίσωση 4
    - Λίγο διαφορετική από τις άλλες (παράγοντας xy)
  - ✓ Όπου x, y και συντελεστές a,b είναι στοιχεία του GF(2^m)
  - ✓ Έστω σύνολο $E_{2m}(a, b)$ από τα ζεύγη (x,y) που ικανοποιούν την Εξίσωση 4 μαζί με ένα σημείο στο άπειρο *O*.

- Ελλειπτικές Καμπύλες στο σώμα GF(2^m)
  - ✓ Έστω GF(2^4) με irreducible polynomial $f(x) = x^4 + x + 1$.
  - ✓ Ο γεννήτορας από $f(g)=0$, με τιμή $g^4 = g + 1$, ή δυαδικό 0011.
  - ✓ Οι δυνάμεις του g θα είναι :

g^0=0001	g^4=0011	g^8=0101	g^{12}=1111
g^1=0010	g^5=0110	g^9=1010	g^{13}=1101
g^2=0100	g^6=1100	g^{10}=0111	g^{14}=1001
g^3=1000	g^7=1101	g^{11}=1110	g^{15}=0001

Π.χ. το g^5 υπολογίζεται ως $g^5=(g^4)(g)=(g+1)g=g^2+g=0100+0010=0110$

Έστω EC: $y^2 + xy = x^3 + g^4x^2 + 1$ (Δηλαδή $a=g^4$ και $b=g^0=1$)

Σημείο που ικανοποιεί την EC είναι (g^5, g^3):

$(g^3)^2 + (g^5)(g^3) = (g^5)^3 + (g^4)(g^5)^2 + 1$ =>

$g^6 + g^8 = g^{15} + g^{14} + 1$ =>

1100 + 0101 = 0001 + 1001 + 0001 =>

1001 = 1001

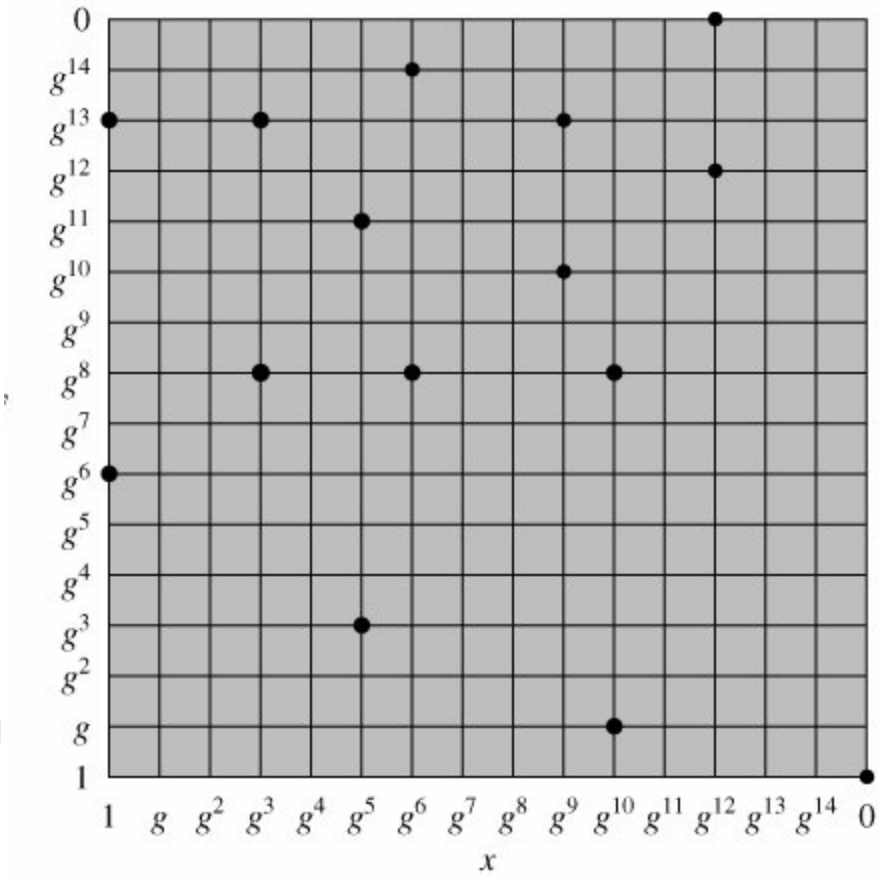
- Ελλειπτικές Καμπύλες στο σώμα GF(2^m)

Σημεία στην καμπύλη $E_{2m}(g^4, b)$

$(0, 1)$	(g^5, g^3)	(g^9, g^{13})
$(1, g^6)$	(g^5, g^{11})	(g^{10}, g)
$(1, g^{13})$	(g^6, g^8)	(g^{10}, g^8)
(g^3, g^8)	(g^6, g^{14})	$(g^{12}, 0)$
(g^3, g^{13})	(g^9, g^{10})	(g^{12}, g^{12})

Cryptography and Network Security Principles and Practices, 4th ed. W. Stallings Prentice Hall

Η καμπύλη $E_{2m}(g^4, b)$



ECC – GF(2^m)

- Ελλειπτικές Καμπύλες στο σώμα GF(2^m)
  - ✓ Κανόνες άθροισης στο $E_{2m}(a, b)$
  - ✓ P + *O* = P . *O* ουδέτερο
  - ✓ Αν P = (x_P, y_P), τότε P + (x_P, x_p+y_P) = *O*. Άρα το σημείο (x_P, x_P+y_P) είναι ο αντίθετος του P, δηλαδή ο –P
  - ✓ Αν P = (x_P, y_P), και Q = (x_Q, y_Q) (P ≠ -Q και P ≠ Q) τότε το άθροισμα ορίζεται ως R = P + Q = (x_R, y_R) όπου:

    $x_R = \lambda^2 + \lambda + x_P + x_Q + a$

    $y_R = \lambda(x_P + x_R) + x_R + y_P$ και

    $\lambda = (y_Q+y_P) / (x_Q+x_P)$
  - ✓ Αν P = (x_P, y_P) ο πολλαπλασιασμός 2P=R=(x_R, y_R) ορίζεται ως :

    $x_R = \lambda^2 + \lambda + a$

    $y_R = x^2_P + (\lambda+1)x_R$ και

    $\lambda = x_P + (y_P / x_P)$

Κρυπτογραφία Ελλειπτικών Καμπυλών

- Χρειαζόμαστε να βρούμε ένα "hard problem"
  - ισοδύναμο του discrete logarithm
  - Αλλά εύκολο σε υπολογισμούς κρυπτογράφησης και αποκρυπτογράφησης
- Έστω η σχέση Q = kP όπου Q, P δύο σημεία της καμπύλης $E_p(a, b)$ και k<p.
- Εύκολο να υπολογίσεις Q δεδομένου k και P
- Δύσκολο να υπολογίσεις k δεδομένου Q και P.
- Αυτό καλείται πρόβλημα διακριτών λογαρίθμων (discrete logarithm) σε elliptic curves
- Our task: πρέπει να βρούμε σημείο της καμπύλης που παράγει μεγάλη κυκλική ομάδα

Κρυπτογραφία Ελλειπτικών Καμπυλών

- Παράδειγμα
- Έστω καμπύλη $E_{23}(9, 17)$.
- Πρόκειται για την Αβελιανή ομάδα που ορίζεται από την εξίσωση $y^2 \bmod 23 = (x^3 + 9x + 17) \bmod 23$.
- Ερώτημα: Ποιος είναι ο διακριτός λογάριθμος k του Q = (4, 5) στη βάση P=(16, 5);
- Η brute-force μέθοδος είναι να υπολογιστούν πολλαπλάσια του P μέχρι να βρούμε το Q.
- Δηλαδή:
- P=(16, 5) 2P=(20, 20) 3P=(14, 14) 4P=(19, 20) 5P=(13, 10) 6P= (7, 3) 7P = (8, 7) 8P (12, 17) 9P = (4, 5) = Q
- Επειδή 9P = (4, 5) = Q, ο διακριτός λογάριθμος του Q=(4, 5) στη βάση P=(16, 5) είναι k = 9
- Στην πράξη το k το πρέπει να είναι πολύ μεγάλο για να αποτρέψει το brute-force

Ασφάλεια Ελλειπτικών Καμπυλών

Symmetric Scheme (key size in bits)	ECC-Based Scheme (size of *n* in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
92	384	7680
256	512	15360

Source: Certicom

Με elliptic curves μειώνεται σημαντικά το μήκος του κλειδιού

Διακριτοί λογάριθμοι στην πράξη

- Οι ομάδες που παρουσιάζουν πρακτικό ενδιαφέρον:
- $(Z_p^*, \cdot)$, p μεγάλος πρώτος και g γεννήτορας του Z_p^*
- $(Z_p^*, \cdot)$, p, q πρώτοι, και g στοιχείο με τάξη q (δηλ. γεννήτορας κυκλικής υποομάδας με q στοιχεία)
- $(GF(2^m), *, +)$, και g γεννήτορας του πεδίου ως προς *
- (E, +), όπου E ελλειπτική καμπύλη modp και $g \in E$ με τάξη $|E|/h$ (με h = 1, 2 ή 4)
- (E,+) όπου E ελλειπτική καμπύλη στο $GF(2^m)$ και $g \in E$ με τάξη $|E|/h$ (με h = 2 ή 4)