

Ασφάλεια Υπολογιστικών Συστημάτων

7ο Εξάμηνο

Ασύμμετρη Κρυπτογράφηση
(Κρυπτογραφία Δημόσιου Κλειδιού)

Διδάσκων : Δρ. Παρασκευάς Κίτσος

<https://ecsalab.ece.uop.gr/>

Καθηγητής

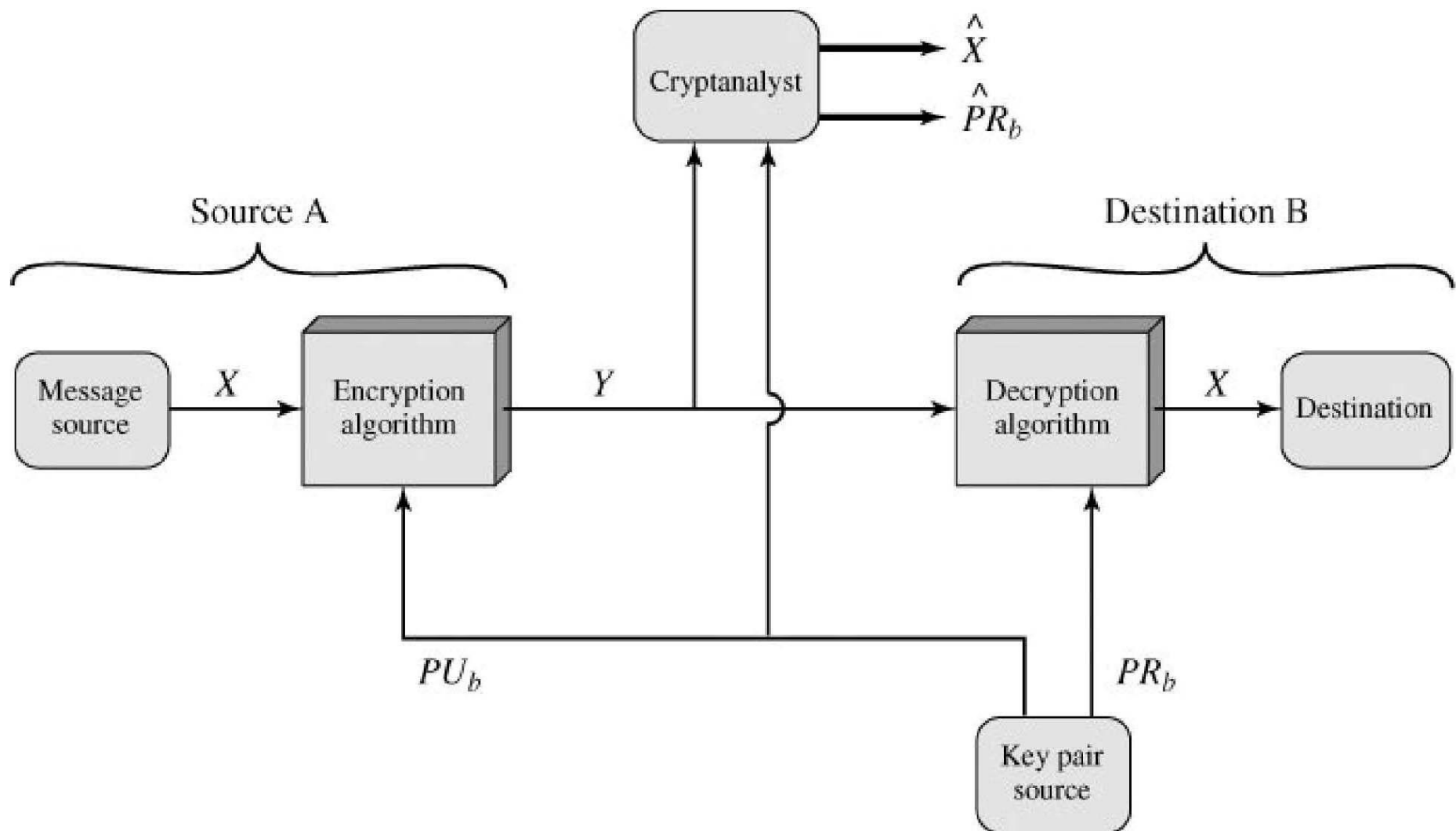
Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και
Εφαρμογών (ECSA Lab.)

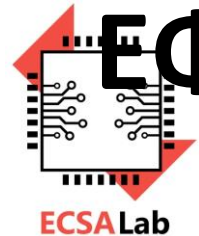
e-mail: kitsos@go.uop.gr

ΔΙΑΡΘΡΩΣΗ ΕΝΟΤΗΤΑΣ

- Αρχές Κρυπτογράφησης Δημοσίου Κλειδιού
- Κρυπτογραφία Δημοσίου Κλειδιού
 - Θεωρία Αριθμών (η συνάρτηση $\phi(n)$ του Euler)
- Ο Αλγόριθμος RSA
- Ο Αλγόριθμος DIFFIE-HELLMAN
- Ελλειπτικές Καμπύλες
- Διανομή Κλειδιού

ΣΕΝΑΡΙΟ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ: ΜΥΣΤΙΚΟΤΗΤΑ





ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΩΝ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

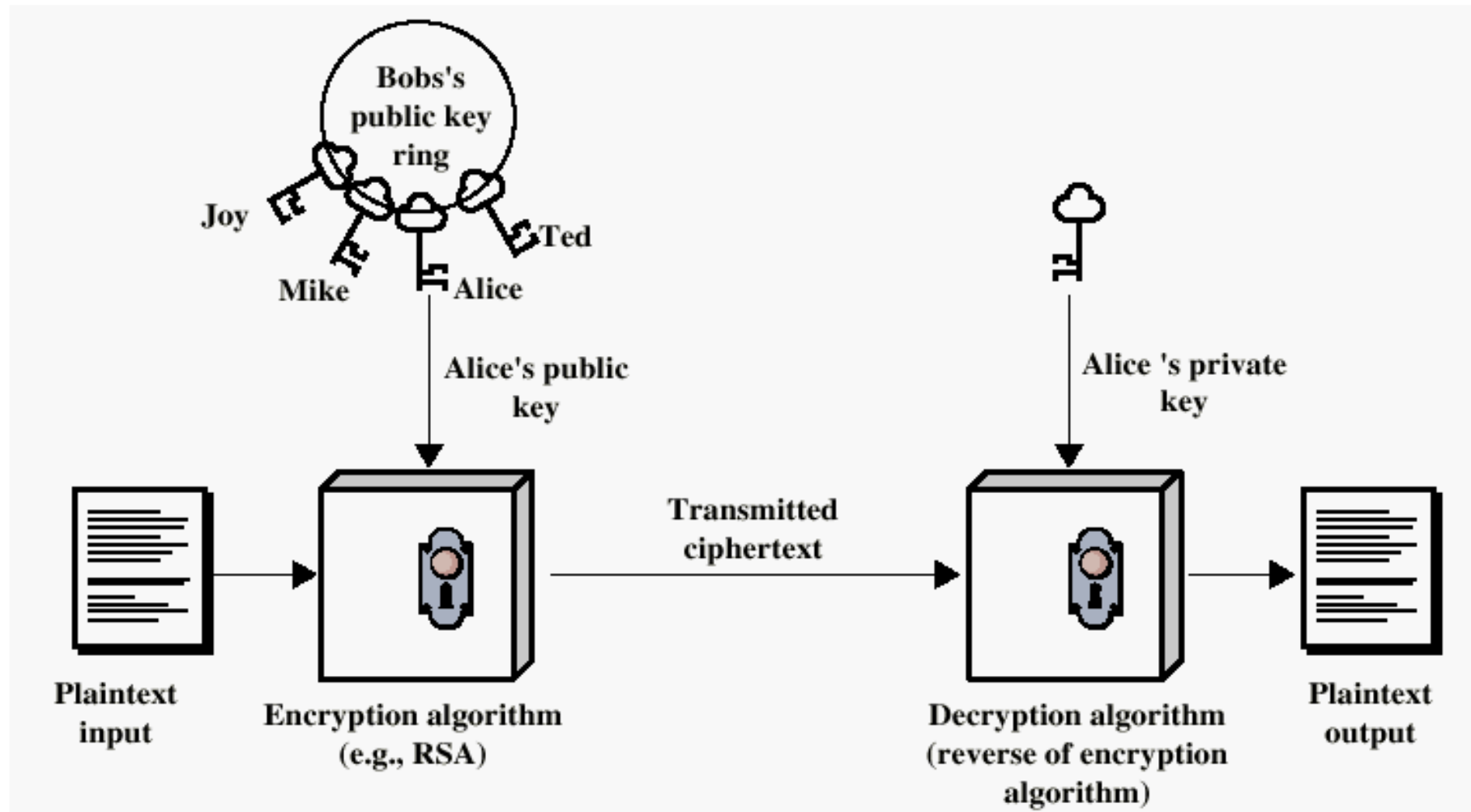
- Χρήσεις / Εφαρμογές:
 - **Encryption/decryption:**

Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη.
Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το μυστικό κλειδί του
 - **Digital Signature:**

Ο αποστολέας υπογράφει ένα μήνυμα με το προσωπικό του μυστικό κλειδί. Ο παραλήπτης πιστοποιεί το μήνυμα με το δημόσιο κλειδί του αποστολέα
 - **Key Exchange:**

Οι δύο πλευρές συνεργάζονται για να ανταλλάξουν το κλειδί συνοδού (session key)

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ



ΑΠΑΙΤΗΣΕΙΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (1/2)

- Είναι υπολογιστικά εφικτό για μια οντότητα B να δημιουργήσει ένα ζεύγος κλειδιών:

Public key KUb , *Private key* KRb : $\{KUb, KRb\}$

- Είναι εύκολο για τον αποστολέα να δημιουργήσει το **κρυπτογράφημα**

$$C = E_{KUb}(M)$$

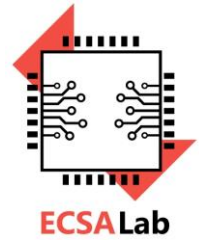
- Είναι εύκολο για το δέκτη να **αποκρυπτογραφήσει** το μήνυμα

$$M = D_{KRb}(C) = D_{KRb}[E_{KUb}(M)]$$

ΑΠΑΙΤΗΣΕΙΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (2/2)

- Είναι υπολογιστικά αδύνατο να δημιουργηθεί το private key (KR_b) γνωρίζοντας το public key (KU_b)
- Είναι υπολογιστικά αδύνατο να ανακτηθεί ένα μήνυμα M , γνωρίζοντας το Public key KU_b και το κρυπτογραφημένο κείμενο C
- Ένα από τα δύο κλειδιά μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση ενώ το άλλο μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση

$$M = D_{KRb}[E_{KU_b}(M)] = D_{KU_b}[E_{KRb}(M)]$$



ΑΛΓΟΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (1/2)

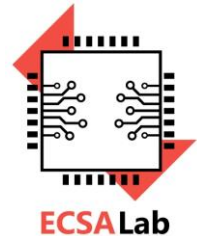
- **RSA, Diffie-Hellman, DSS, Elliptic Curve**

RSA :

- Ron Rivest, Adi Shamir & Len Adleman, MIT 1977
- Ιδιαίτερα γνωστός και χρησιμοποιούμενος αλγόριθμος

Diffie-Hellman :

- Επιτρέπει την ασφαλή ανταλλαγή κλειδιού
- Οι υπολογισμοί στηρίζονται στην κατηγορία των discrete logarithms



ΑΛΓΟΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (2/2)

- **Digital Signature Standard (DSS)**
 - Επιπλέον χρησιμοποιεί την Hash Function SHA-1
 - Δεν χρησιμοποιείται για σκοπούς κρυπτογράφησης ή για σκοπούς ανταλλαγής κλειδιών, αλλά μόνο για **πιστοποίηση**
- **Elliptic-Curve Cryptography (ECC)**
 - Καλή προσέγγιση για μικρά μεγέθη δεδομένων
 - Ιδιαίτερα πολύπλοκος μηχανισμός

ΕΦΑΡΜΟΓΕΣ ΑΡΓΟΡΙΘΜΩΝ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

	Encryption/ Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No
Elliptic Curve	Yes	Yes	Yes

Η ΣΥΝΑΡΤΗΣΗ $\phi(n)$ ΤΟΥ EULER

- Αν ένας ακέραιος p είναι πρώτος ισχύει:
 - $\phi(p) = p - 1$
- Επίσης αν υποθέσουμε ότι έχουμε δύο πρώτους αριθμούς p και q με $p \neq q$. Το γινόμενο τους είναι $n = p * q$
- Και τότε ισχύει:
 - $\phi(n) = \phi(p*q) = \phi(p)*\phi(q) = (p - 1)*(q - 1)$
- Π.χ. $\phi(11) = 11-1=10$ και
 $\phi(33)=\phi(3*11)=(3-1)*(11-1)=20$

Ο ΑΛΓΟΡΙΘΜΟΣ RSA

- Ο RSA δέχεται απλό κείμενο μεγέθους από 0 έως $n - 1$ bits
- Ο RSA εξάγει κρυπτογράφημα από 0 έως $n - 1$ bits
 - Τυπικές τιμές του n είναι 512-, 1024- ή 2048-bit
 - Το απλό κείμενο συμβολίζεται με M
 - Το κρυπτογράφημα συμβολίζεται με C

ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΛΟΓΗΣ ΚΛΕΙΔΙΩΝ ΣΤΟΝ RSA

1. Επιλογή με τυχαίο τρόπο δύο πρώτων μεγάλων αριθμών:
 p, q
2. Υπολογισμός του γινομένου: $n = p * q$
3. Επιλογή ενός περιττού ακέραιου αριθμού e , ο οποίος είναι πρώτος σε σχέση με τη συνάρτηση $\phi(n)$. Θα πρέπει να ισχύει $1 < e < \phi(n)$.
4. Υπολογισμός $d = e^{-1} \bmod \{ (p-1) * (q-1) \}$
5. Δημόσιο Κλειδί: $P_B = (e, n)$, Μυστικό Κλειδί: $S_B = (d, n)$

Κρυπτογράφηση m (message): $Cipher = M^e \bmod (n)$

Αποκρυπτογράφηση $Cipher$: $M = Cipher^d \bmod (n)$

ΑΝΑΛΥΣΗ ΤΟΥ RSA...

- Δεν υπάρχει αλγόριθμος ο οποίος να εντοπίζει τους πρώτους παράγοντες ενός σύνθετου ακεραίου
 - Οι πρώτοι αριθμοί p , q θα πρέπει να είναι αρκετά μεγάλοι ώστε ο καλύτερος γνωστός αλγόριθμος παραγοντοποίησης να απαιτεί μεγαλύτερο χρόνο από αυτόν με τον οποίο πρέπει να προστατευτούν τα δεδομένα

p, q	n	χρόνος προστασίας
256 bits	512 bits	Μερικές εβδομάδες
512 bits	1024 bits	50-100 χρόνια
1024 bits	2048 bits	> 100 χρόνια
2048 bits	4096 bits	Περίπου την ηλικία του σύμπαντος

...ΑΝΑΛΥΣΗ ΤΟΥ RSA

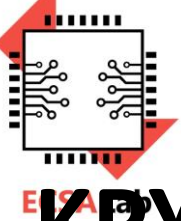
- Ο υπολογισμός μεγάλης δύναμης ενός αριθμού σε modular αριθμητική μπορεί να γίνει σε επιτρεπτό χρόνο
 - Οι αλγόριθμοι εκθετοποίησης παρουσιάζουν πολυπλοκότητα που είναι γραμμικώς ανάλογη με το μέγεθος των ακεραίων που λαμβάνουν μέρος στην εκθετική πράξη

ΠΑΡΑΔΕΙΓΜΑ RSA: ΕΠΙΛΟΓΗ ΚΑΙ ΔΗΜΙΟΥΡΓΙΑ ΚΛΕΙΔΙΩΝ

- $p = 11, q = 3 \rightarrow$ τυχαία επιλογή
- $n = pq = 33$
- $\phi(n) = (p - 1)(q - 1) = 20$
- Επιλογή του e έτσι ώστε να είναι αμοιβαία πρώτος του $\phi(n) = 20$, $e = 3 \rightarrow$ επιλογή
- Υπολογισμός d έτσι ώστε $de \equiv 1 \pmod{20}$, $d < 20$, $d = 7$ αφού $3 \times 7 = 21$ και $21 \equiv 1 \pmod{20} \rightarrow$ υπολογισμός

ΔΗΜΟΣΙΟ
3, 33

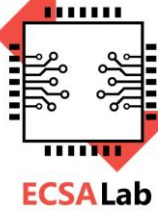
ΙΔΙΩΤΙΚΟ
7, 33



ΠΑΡΑΔΕΙΓΜΑ RSA:

ΚΡΥΠΤΟΓΡΑΦΗΣΗ/ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ

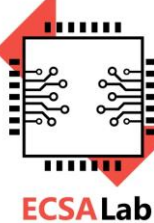
- Κρυπτογράφηση του μηνύματος $M = 7$:
 - $C = 7^3 \bmod 33 = 13$.
- Αποκρυπτογράφηση του κρυπτογραφήματος $C = 13$:
 - $M = 13^7 \bmod 33 = (13^3 \times 13^3 \times 13) \bmod 33 = (19 \times 19 \times 13) \bmod 33 = 7$.



ECSA Lab

ΛΥΣΗ ΤΗΣ $de \equiv 1 \pmod{\phi(n)}$ (1/2)

- Επίλυση με χρήση της ανεπτυγμένης μορφής του αλγορίθμου του Ευκλείδη



ΛΥΣΗ ΤΗΣ $de \equiv 1 \pmod{\phi(n)}$ (2/2)

- **Απλοϊκή λύση:**

Υπολογισμός του d έτσι ώστε να ισχύει $ed \equiv 1 \pmod{\phi(n)}$ ή $d = 3^{-1} \pmod{20}$ ή υπολογισμός του d έτσι ώστε η $\phi(n) = 20$ να διαιρεί τη παράσταση $ed = 3d$ και να έχει υπόλοιπο 1 [$ed \equiv 1 \pmod{\phi(n)}$] ή

$$ed \pmod{\phi(n)} = 1 \pmod{\phi(n)} \Rightarrow ed \pmod{\phi(n)} = 1$$

- Δοκιμές για $d = 2, 3, 4, \dots$
- Υπολογίζεται ότι $d = 7$

ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ RSA

- Υπάρχουν 3 συνολικά τρόποι επίθεσης στον RSA
 - Επίθεση βίαιης δύναμης.
 - Εξαντλητική δοκιμή όλων των πιθανών κλειδιών
 - Μαθηματικές επιθέσεις
 - Παραγοντοποίηση του γινομένου δύο πρώτων αριθμών
 - Χρονικές επιθέσεις
 - Καταμέτρηση του χρόνου αποκρυπτογράφησης

Ο ΑΛΓΟΡΙΘΜΟΣ DIFFIE-HELLMAN:

ΕΙΣΑΓΩΓΙΚΑ ΣΤΟΙΧΕΙΑ

- Ο πρώτος αλγόριθμος δημόσιου κλειδιού που εφευρέθηκε το 1976 είναι ο Diffie-Hellman
- Το πρωτόκολλο Diffie-Hellman αναφέρεται στην κρυπτογραφία δημόσιου κλειδιού αλλά χρησιμοποιείται κατά βάση σαν πρωτόκολλο ανταλλαγής (κρυφού ιδιωτικού) κλειδιού
- Στόχος είναι η ανταλλαγή (εγκατάσταση) ενός μυστικού ιδιωτικού κλειδιού μεταξύ δύο (άγνωστων) χρηστών μέσω ενός μη ασφαλούς καναλιού επικοινωνίας

Ο ΑΛΓΟΡΙΘΜΟΣ DIFFIE-HELLMAN

(1/3)

- Θεωρούμε την Αλίκη (Alice) και τον Βύρωνα (Bob) που θέλουν να επικοινωνήσουν μέσω του πρωτοκόλλου Diffie-Hellman
- Αρχικά τα δύο πρόσωπα συμφωνούν σε δύο (δημόσιους) μεγάλους πρώτους αριθμούς τον g και τον p
- Η επιλογή των αριθμών γίνεται με τέτοιο τρόπο ώστε ο g να είναι πρωτογενής ρίζα του p

Ο ΑΛΓΟΡΙΘΜΟΣ DIFFIE-HELLMAN

(2/3)

- Πρωτογενής ρίζα (primitive root) ονομάζουμε τον ακέραιο αριθμό g , του οποίου οι δυνάμεις παράγουν όλους τους αριθμούς από το 1 έως το $p-1$.
- Αυτό σημαίνει ότι, αν g είναι πρωτογενής ρίζα του πρώτου αριθμού p , τότε οι αριθμοί $g \bmod p$, $g^2 \bmod p$, ..., $g^{p-1} \bmod p$ είναι διαφορετικοί και αποτελούν τους ακεραίους από το 1 μέχρι το $p-1$.
 - Π.χ. $n = 14$.
 - Ο αριθμός 14 είναι αμοιβαία πρώτος με τους 1, 3, 4, 9, 11 και 13.
 - Ο αριθμός 3 είναι πρωτογενής ρίζα του αριθμού 14 αφού:
 - $3 \bmod 14 = 3$, $3^2 \bmod 14 = 9$, $3^3 \bmod 14 = 13$, $3^4 \bmod 14 = 11$, $3^5 \bmod 14 = 5$
 - ...

Ο ΑΛΓΟΡΙΘΜΟΣ DIFFIE-HELLMAN

(3/3)

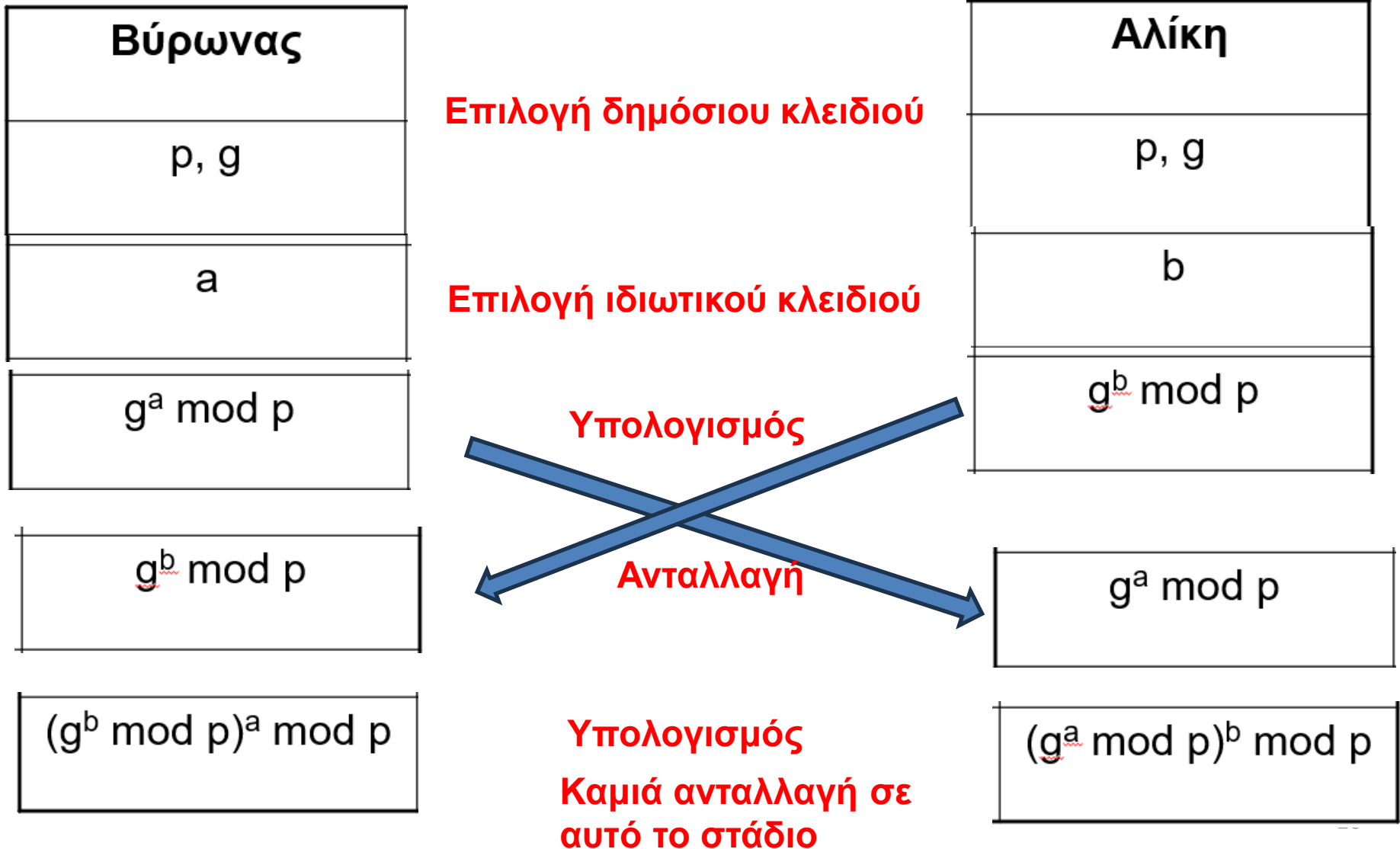
- Στη συνέχεια η Αλίκη επιλέγει έναν (μυστικό) τυχαίο αριθμό a και στέλνει το αποτέλεσμα της παράστασης $g^a \bmod p$ στον Βύρωνα
- Ταυτόχρονα ο Βύρωνα επιλέγει έναν (μυστικό) τυχαίο αριθμό b και στέλνει το αποτέλεσμα της παράστασης $g^b \bmod p$ στην Αλίκη
- Από την πλευρά της η Αλίκη υπολογίζει την παράσταση $(g^b \bmod p)^a \bmod p = g^{ba} \bmod p$
- Από την πλευρά του ο Βύρωνα υπολογίζει την παράσταση $(g^a \bmod p)^b \bmod p = g^{ab} \bmod p$
- Με αυτό τον τρόπο οι δύο πλευρές ανταλλάσσουν ένα κοινό ιδιωτικό κλειδί, το $g^{ab} \bmod p$

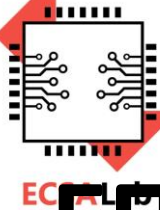
ΤΑ ΚΛΕΙΔΙΑ ΤΟΥ DIFFIE-HELLMAN

Βύρωνας		Αλίκη
p, g	Δημόσια	p, g
a	Ιδιωτικό	b
$g^a \bmod p$	Αποστολή	$g^b \bmod p$
$(g^b \bmod p)^a \bmod p$	Υπολογισμός	$(g^a \bmod p)^b \bmod p$

ΣΧΗΜΑΤΙΚΟ ΠΑΡΑΔΕΙΓΜΑ

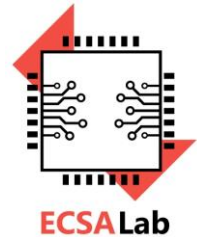
ΑΛΓΟΡΙΘΜΟΥ DIFFIE-HELLMAN





ΠΑΡΑΔΕΙΓΜΑ DIFFIE-HELLMAN: ΕΠΙΛΟΓΗ ΚΑΙ ΔΗΜΙΟΥΡΓΙΑ ΚΛΕΙΔΙΩΝ

- Η Αλίκη και ο Βύρωνας συμφωνούν σε δύο πρώτους αριθμούς $p = 23$ και $g = 5$. Ο αριθμός 5 είναι πρωτογενής ρίζα του 23
 - Η Αλίκη επιλέγει έναν (μυστικό) τυχαίο αριθμό $a = 6$ και στέλνει στο Βύρωνα το αποτέλεσμα της παράστασης $g^a \bmod p \rightarrow 5^6 \bmod 23 = 8$
 - Ο Βύρωνας επιλέγει έναν (μυστικό) τυχαίο αριθμό $b = 15$ και στέλνει στην Αλίκη το αποτέλεσμα της παράστασης $g^b \bmod p \rightarrow 5^{15} \bmod 23 = 19$
 - Η Αλίκη υπολογίζει το κοινό μυστικό κλειδί $(g^b \bmod p)^a \bmod p = 19^6 \bmod 23 = 2$
 - Ο Βύρωνας υπολογίζει το κοινό μυστικό κλειδί $(g^a \bmod p)^b \bmod p = 8^{15} \bmod 23 = 2$



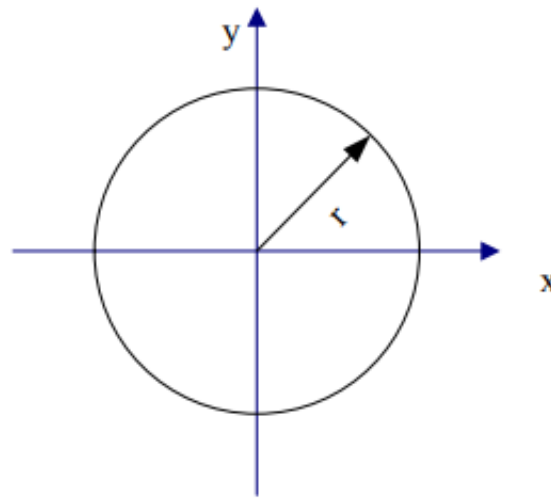
ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ

Τα κρυπτοσυστήματα των Ελλειπτικών Καμπυλών εξασφαλίζουν ίδια επίπεδα ασφάλειας σε σχέση με τον RSA (ή τον Diffie-Hellmann) αλλά με πολύ μικρότερο αριθμό bits κλειδί

<i>Symmetric Encryption Key Size in bits</i>	<i>RSA and Diffie-Hellman Key size in bits</i>	<i>Elliptic Curve Key Size in bits</i>
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

ΚΡΥΠΤΟΣΥΣΤΗΜΑ ΕΛΛΕΙΠΤΙΚΩΝ ΚΑΜΠΥΛΩΝ (I)

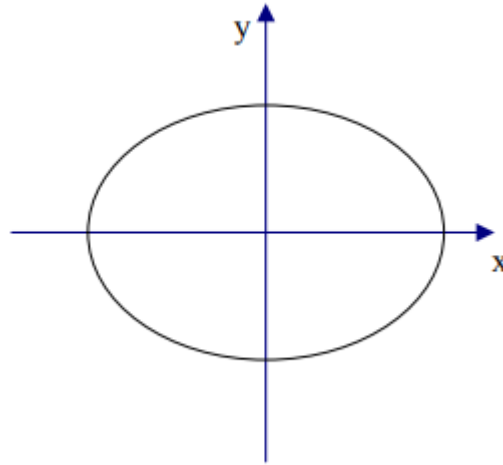
- Κύκλος



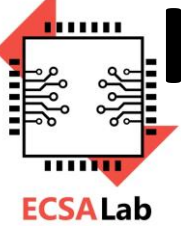
- Έχει εξίσωση $x^2+y^2=r^2$
- Ο κύκλος είναι ειδική περίπτωση έλλειψης που έχει εξίσωση $ax^2+by^2=c$ με $a=b$

ΚΡΥΠΤΟΣΥΣΤΗΜΑ ΕΛΛΕΙΠΤΙΚΩΝ ΚΑΜΠΥΛΩΝ (II)

- Εξίσωση $ax^2+by^2=c$



- Στην εξίσωση κύκλου, και στην εξίσωση έλλειψης, οι μεταβλητές x, y συνδέονται με δευτεροβάθμιες εξισώσεις
- Αυτό έχει σαν αποτέλεσμα σε μια δοσμένη τιμή του x να αντιστοιχούν δύο τιμές για το y , και αντίστροφα



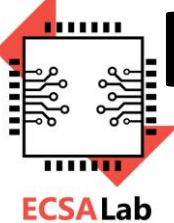
ΚΡΥΠΤΟΣΥΣΤΗΜΑ ΕΛΛΕΙΠΤΙΚΩΝ ΚΑΜΠΥΛΩΝ (III)

- Η Ελλειπτική καμπύλη έχει εξίσωση της μορφής $y^2 = x^3 + ax + b$
- Έστω δύο διαφορετικά σημεία $P(x_1, y_1)$ και $Q(x_2, y_2)$ και έστω η ευθεία $y = \lambda x + c$ η οποία τέμνει την ελλειπτική καμπύλη στα σημεία αυτά. Αντικαθιστώντας την ευθεία στην εξίσωση της καμπύλης έχουμε

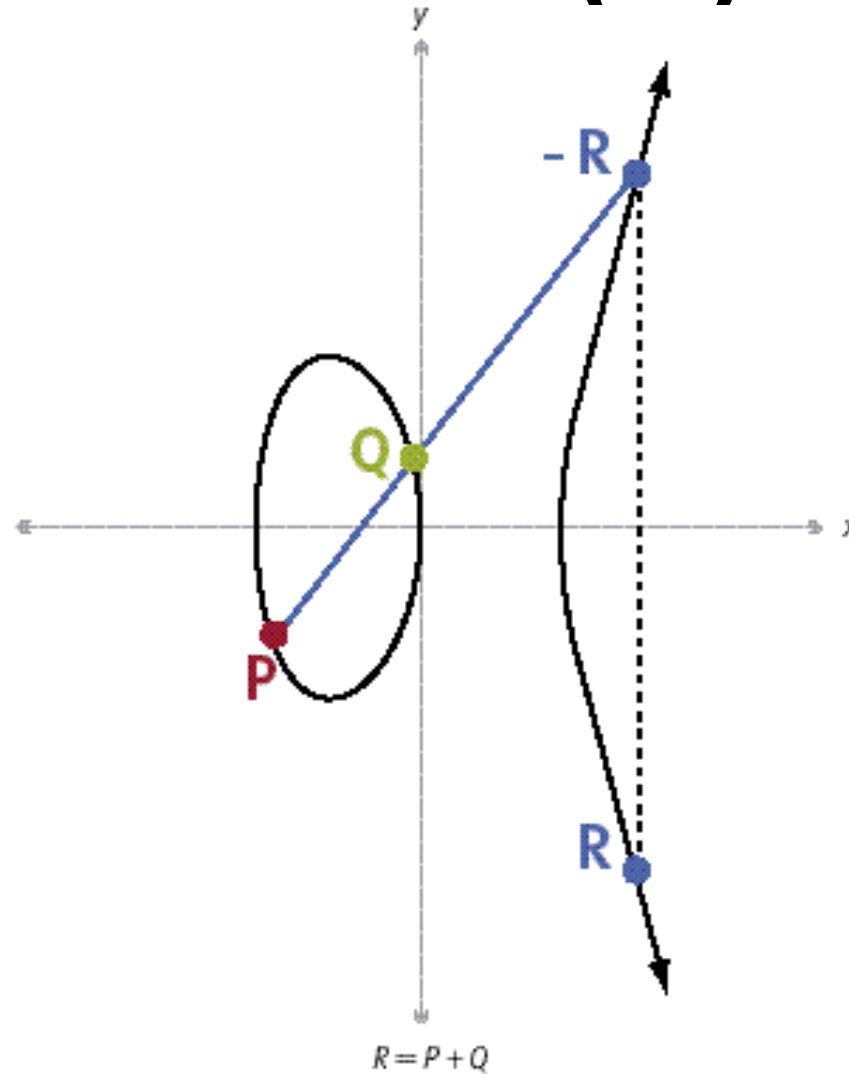
$$(\lambda x + c)^2 = x^3 + ax + b$$

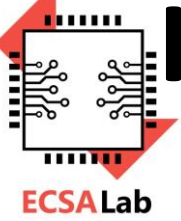
που έχει ρίζες τις x_1 και x_2

- Υπάρχει και μια τρίτη ρίζα που αντιστοιχεί στο σημείο της ευθείας $(x_3, \lambda x_3 + c)$. Δηλαδή η ευθεία τέμνει την καμπύλη σε τρία σημεία



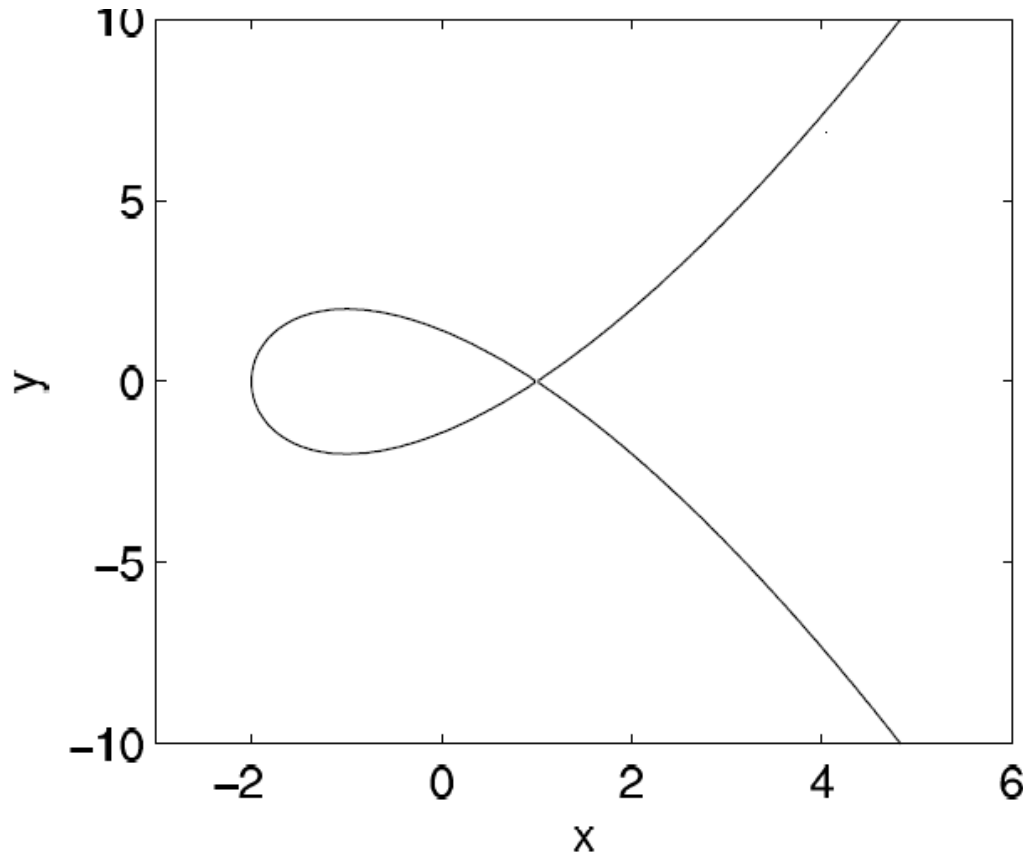
ΚΡΥΠΤΟΣΥΣΤΗΜΑ ΕΛΛΕΙΠΤΙΚΩΝ ΚΑΜΠΥΛΩΝ (IV)





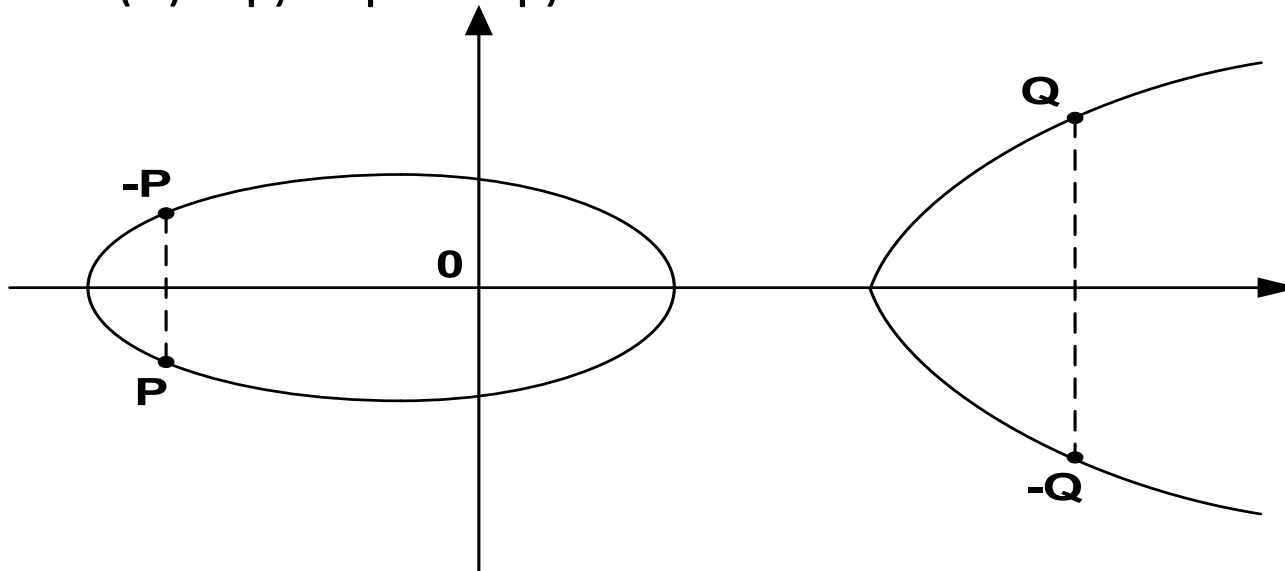
ΚΡΥΠΤΟΣΥΣΤΗΜΑ ΕΛΛΕΙΠΤΙΚΩΝ ΚΑΜΠΥΛΩΝ (V)

Για κάποιο συνδυασμό των a και b η ελλειπτική καμπύλη δεν έχει τρεις ρίζες. Αυτό συμβαίνει όταν $4a^3+27b^2=0$. Τότε η καμπύλη ονομάζεται **ιδιάζουσα (singular)**



ΠΡΟΣΘΕΣΗ ΣΗΜΕΙΩΝ...

- Η Ελλειπτική Καμπύλη είναι συμμετρική ως προς τον άξονα x
- Έτσι μπορούμε να ορίσουμε το αντίθετο σημείο $(-P)$ ενός σημείου (P) της καμπύλης

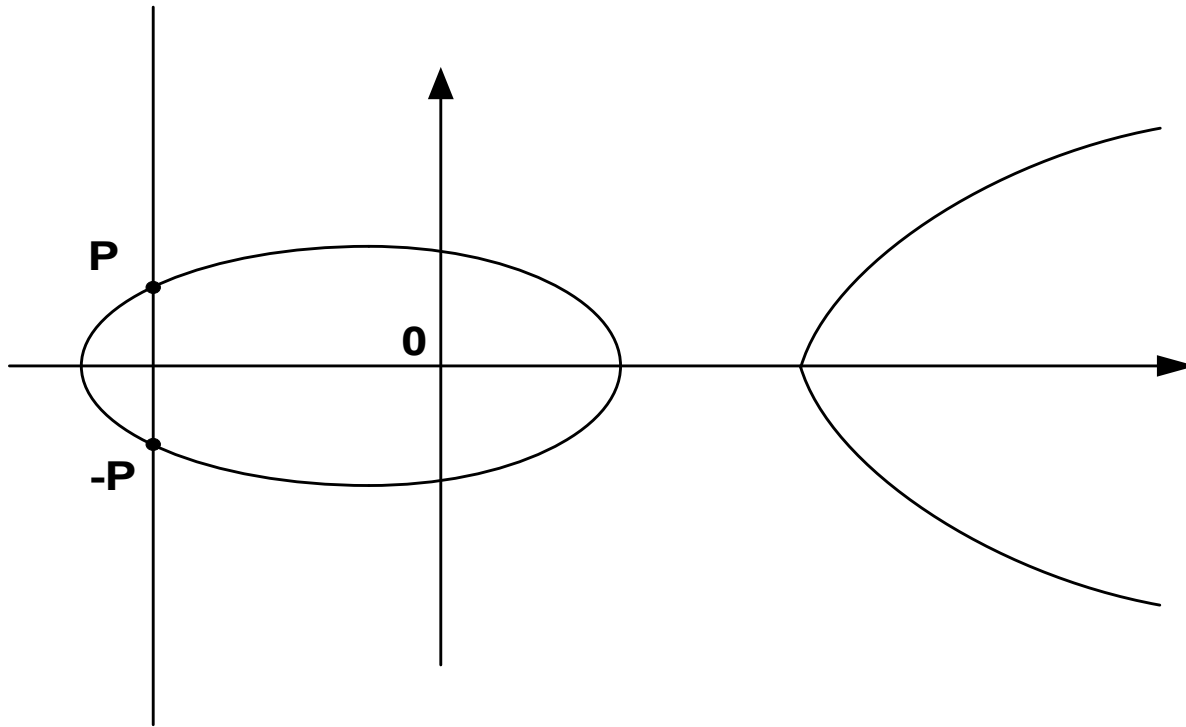


- Το σημείο $-P$ είναι συμμετρικό του P
- Άρα, αν $P=(x, y)$ τότε $-P=(x, -y)$

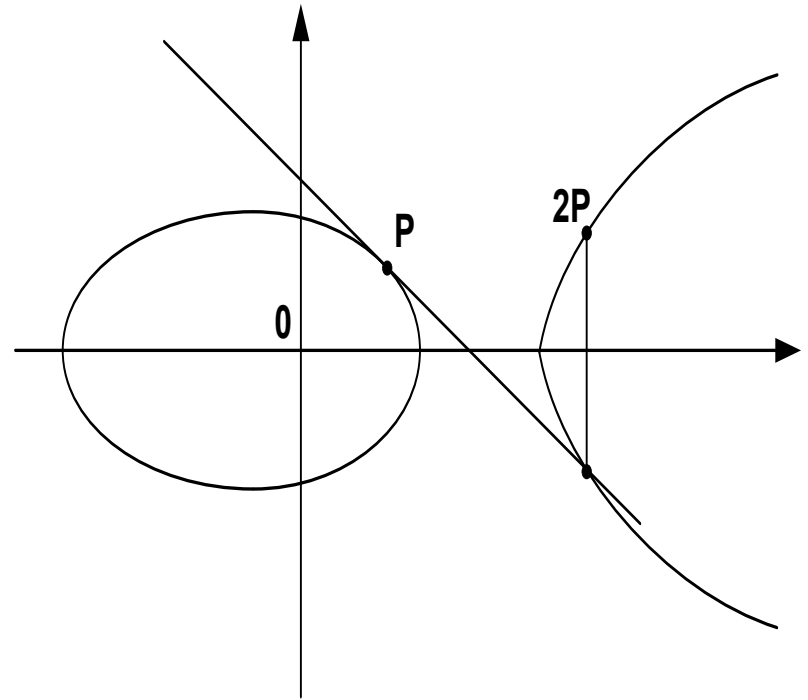
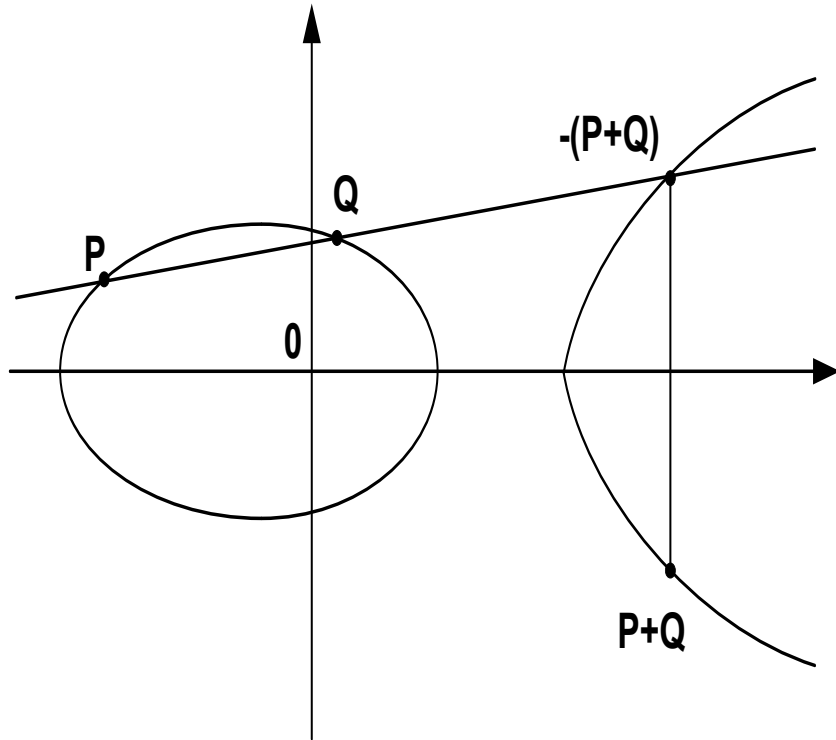
...ΠΡΟΣΘΕΣΗ ΣΗΜΕΙΩΝ...

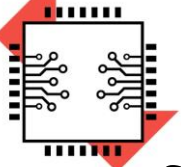
ECSA Lab

- Αν $P=(x, y)$ τότε $-P=(x,-y)$: Αντίστροφο σημείο
- Ισχύει $P + (-P) = O$ με $O(x, \infty)$ είναι το ουδέτερο σημείο
- Επίσης $P+O=O+P=P$



...ΠΡΟΣΘΕΣΗ ΣΗΜΕΙΩΝ...





...ΠΡΟΣΘΕΣΗ ΣΗΜΕΙΩΝ

- Για δύο σημεία καθώς και το αντίστροφο του αθροίσματός τους βρίσκονται πάνω στην ίδια ευθεία

- Έστω τα σημεία $P(x_1, y_1)$ και $Q(x_2, y_2)$. Η ευθεία που διέρχεται από αυτά έχει εξίσωση $y=\lambda x+c$ και κλίση $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

- Αντικαθιστούμε την ευθεία στην εξίσωση της καμπύλης και βρίσκουμε ότι οι συντεταγμένες του αθροίσματος των σημείων $P+Q=(x_3, y_3)$ έχουν εξισώσεις

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

- Αν $Q=-P=(x_1, -y_1)$ η κλίση γίνεται άπειρη και έχουμε το σημείο O .
- Αν $P=Q$ έχουμε τον διπλασιασμό του σημείου και η κλίση τότε είναι ίση με

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ ΟΡΙΣΜΕΝΕΣ ΣΤΟ modulo p

- Η ελλειπτική καμπύλη ορισμένη στο σώμα $\mathbf{Z}_p$ για κάποιον πρώτο ακέραιο $p > 3$ είναι το σύνολο των στοιχείων $(x, y) \in \mathbf{Z}_p \times \mathbf{Z}_p$ τα οποία ικανοποιούν την εξίσωση:

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

$$\text{όπου } a, b \in \mathbf{Z}_p \qquad 4a^3 + 27b^2 \not\equiv 0 \pmod{p}$$

ΠΡΟΣΘΕΣΗ ΣΤΟ ΣΩΜΑ Z_p

- Η πρόσθεση ορίζεται ακριβώς με τον ίδιο τρόπο όπως και στους πραγματικούς αριθμούς
 - Έστω δύο διαφορετικά σημεία $P=(x_1, y_1)$ και $Q=(x_2, y_2)$ της ελλειπτικής καμπύλης $y^2 \equiv x^3 + ax + b \pmod{p}$
 - Το $P+Q=(x_3, y_3)$ έχει συντεταγμένες

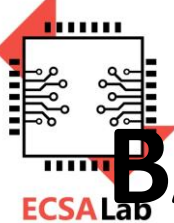
$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p}$$

$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}$$

$$\text{Όπου } \lambda = \begin{cases} \frac{(y_2 - y_1)}{(x_2 - x_1)} \pmod{p} & \text{για } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} \pmod{p} & \text{για } P = Q \end{cases}$$

ΤΟ ΠΡΩΤΟΚΟΛΛΟ ΤΩΝ DIFFIE – HELLMAN ΣΤΙΣ ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ

- Η Αλίκη και ο Βύρωνας επιλέγουν δημόσια μια καμπύλη
$$y^2 \equiv x^3 + ax + b \pmod{p}$$
και ένα στοιχείο της καμπύλης $A=(x_1, y_1)$.
- Μετά η Αλίκη επιλέγει έναν μυστικό αριθμό x_a , τέτοιον ώστε $1 < x_a < p$ και όμοια ο Βύρωνας έναν μυστικό αριθμό x_b , τέτοιον ώστε $1 < x_b < p$.
- Τέλος εκτελείται η ακολουθία
 - Αλίκη $\rightarrow$ Βύρωνας: $x_a A \pmod{p}$
 - Βύρωνας $\rightarrow$ Αλίκη: $x_b A \pmod{p}$
 - Βύρωνας: $(x_a A) x_b \pmod{p}$
 - Αλίκη: $(x_b A) x_a \pmod{p}$



ΒΑΘΜΩΤΟΣ ΠΟΛΛΑΠΛΑΣΙΑΣΜΟΣ (I)

- Θέλουμε να υπολογίσουμε τον βαθμωτό πολ/σμο ενός σημείου. Δηλαδή το nP για δοσμένο n .
- Πώς ????
- Με τον αλγόριθμο «Διπλασιασμού – και – Πρόσθεσης» ο οποίος είναι ανάλογος με τον αλγόριθμο «Επαναλαμβανόμενου τετραγωνισμού – και – Πολλαπλασιασμού» στους ακέραιους.

ΒΑΘΜΩΤΟΣ ΠΟΛΛΑΠΛΑΣΙΑΣΜΟΣ (II)

Έστω ένα σημείο P της ελλειπτικής καμπύλης και έστω ο ακέραιος n . Ζητείται το σημείο που αντιστοιχεί στο nP .

1) Είσοδος: n, P

2) Έστω $Q \leftarrow \mathbf{0}, i \leftarrow l+1$

3) Υπολογίζουμε τη δυαδική αναπαράσταση του n . Έστω $(c_0 c_1 c_2 \dots c_{l-1})$ η δυαδική λέξη μήκους l -bit όπου

$$n = \sum_{i=0}^{l-1} c_i 2^i$$

4) Επανάλαβε το βήμα έως ότου $i < 0$:

$Q \leftarrow 2Q$

Αν $c_i = 1$ τότε $Q \leftarrow Q + P$

$i \leftarrow i-1$

5) Έξοδος: Q

- **Παράδειγμα:** Έστω το σημείο P μιας ελλειπτικής καμπύλης. Ζητείται το $171P$.

Λύση: $(171)_{10} = (10101011)_2$

Ξεκινάμε από δεξιά bit διπλασιάζοντας σε κάθε βήμα και προσθέτουμε P όποτε το bit είναι ίσο με 1.

Έτσι έχουμε το σημείο:

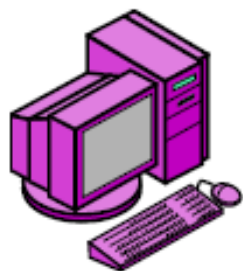
$$171P = 2(2(2(2(2(2(2P) + P)) + P)) + P) + P$$

ΔΙΑΝΟΜΗ ΚΛΕΙΔΙΟΥ: KEY DISTRIBUTION

- ☐ Κάποιο κλειδί μπορεί να επιλεγεί από την οντότητα A και να παραδοθεί με φυσικό τρόπο στην οντότητα B
- ☐ Μια τρίτη οντότητα (third party) μπορεί να επιλέξει ένα κλειδί και να το κοινοποιήσει με φυσικό τρόπο στην οντότητα A και στην οντότητα B
- ☐ Εάν οι A και B έχουν χρησιμοποιήσει στο παρελθόν μια τιμή κλειδιού, η μια οντότητα μπορεί να μεταδώσει το νέο κλειδί στην άλλη, κρυπτογραφώντας το με την προηγούμενη τιμή κλειδιού
- ☐ Εάν οι οντότητες A και B έχουν μια αποκαταστημένη διασύνδεση με μια τρίτη οντότητα, τότε η C μπορεί να μεταδώσει το κλειδί μέσω των κρυπτογραφημένων συνδέσεων (links) με την A και B

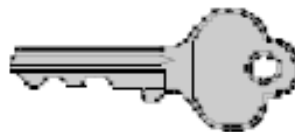
ΔΙΑΝΟΜΗ ΚΛΕΙΔΙΟΥ (KEY DISTRIBUTION)

ΑΡΧΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

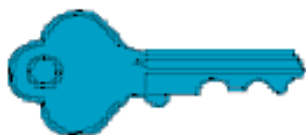


Αποστολέας Α

1. Δημιουργία
συμμετρικού κλειδιού



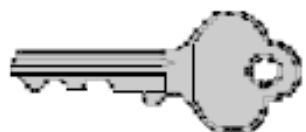
Παραλήπτης Β



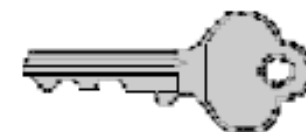
2. Κρυπτογράφηση
του κλειδιού με το
Δημόσιο Κλειδί του Β

3. Αποστολή του συμμετρικού
κλειδιού (κρυπτογραφημένου)

4. Αποκρυπτογράφηση
του συμμετρικού
κλειδιού, με χρήση του
Ιδιωτικού κλειδιού του Β



5. Χρήση του συμμετρικού κλειδιού
για κρυπτογράφηση του μηνύματος



ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΔΙΑΝΟΜΗ ΚΛΕΙΔΙΩΝ

(1/5)

Για τη λειτουργία αυτή, προσδιορίζονται δύο είδη κλειδιών:

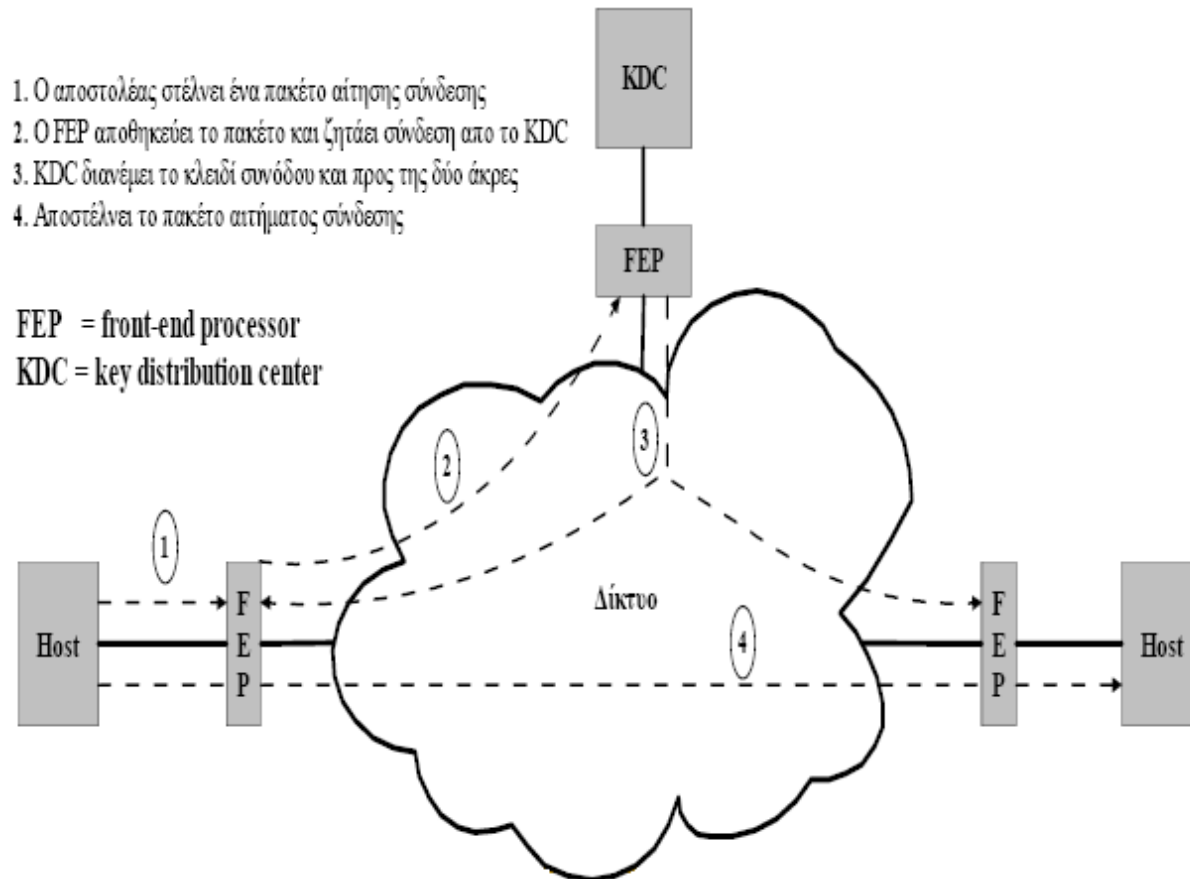
- **Κλειδί Συνόδου (Session Key):**
 - Τα δεδομένα κρυπτογραφούνται με κλειδιά συνόδου (session keys) μιας χρήσης (one time)
 - Όταν η μετάδοση ολοκληρωθεί το αντίστοιχο session key καταστρέφεται
- **Μόνιμο Κλειδί (Permanent ή Master Key):**
 - Χρησιμοποιείται από τις οντότητες για την διανομή κλειδιών συνόδων (session keys)

Η διαμόρφωση (configuration) περιλαμβάνει τα ακόλουθα στοιχεία:

- Κέντρο διανομής κλειδιού (key distribution center – KDC)
- Μετωπικός επεξεργαστής (front-end processor – FEP)

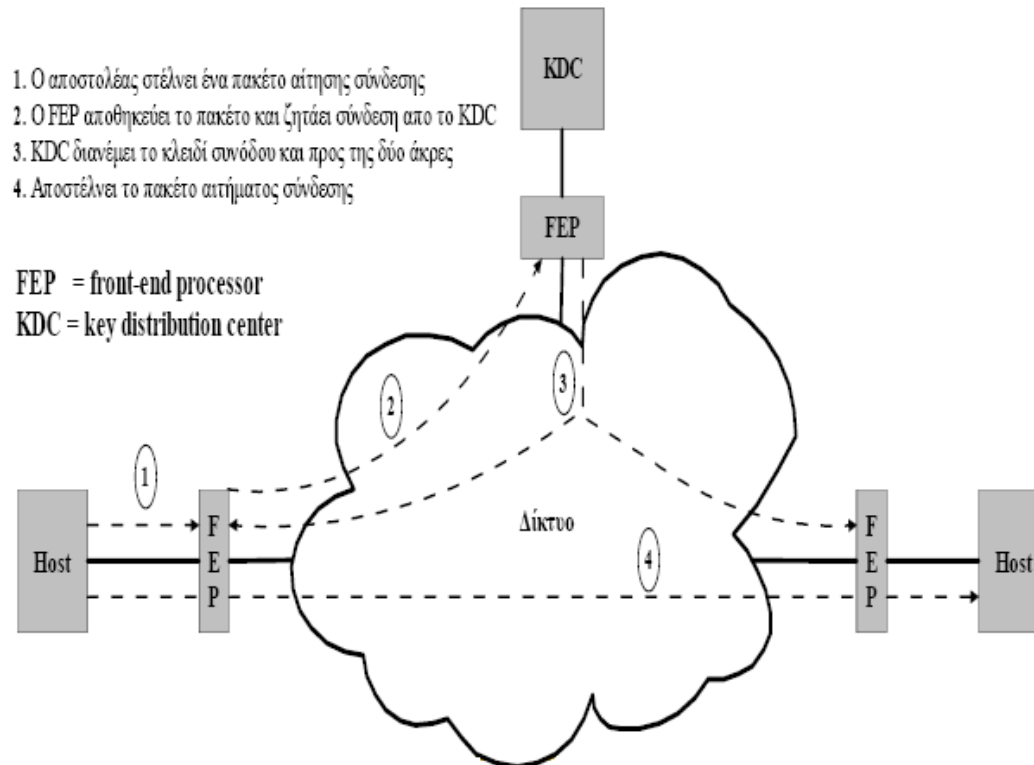
ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΔΙΑΝΟΜΗ ΚΛΕΙΔΙΩΝ (2/5)

- Βήμα 1. Αποστολή πακέτου αίτησης σύνδεσης (connection-request packet) στον μετωπικό επεξεργαστή



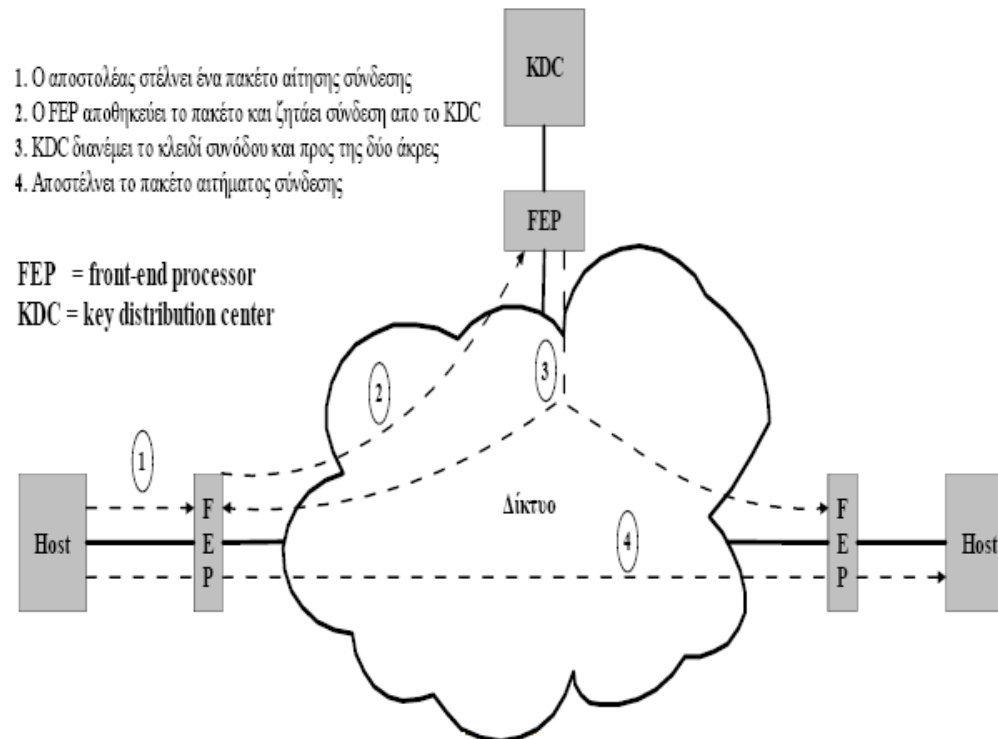
ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΔΙΑΝΟΜΗ ΚΛΕΙΔΙΩΝ (3/5)

- Βήμα 2. Ο FEP (μετωπικός επεξεργαστής) αποθηκεύει το πακέτο και αποστέλλει μια αίτηση στο KDC (κέντρο διανομής κλειδιού) για την επίτευξη της σύνδεσης



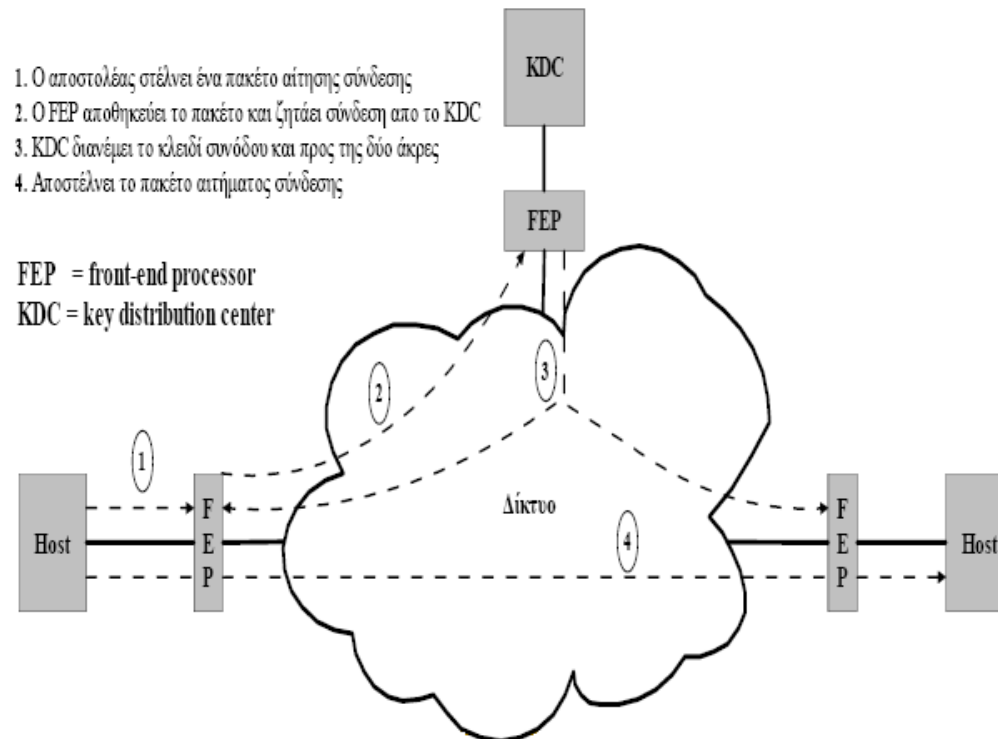
ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΔΙΑΝΟΜΗ ΚΛΕΙΔΙΩΝ (4/5)

- Βήμα 3. Η επικοινωνία μεταξύ του FEP (μετωπικός επεξεργαστής) και του KDC (κέντρο διανομής κλειδιού) κρυπτογραφείται χρησιμοποιώντας ένα κύριο κλειδί, που γνωρίζουν μόνο οι FEP και KDC.

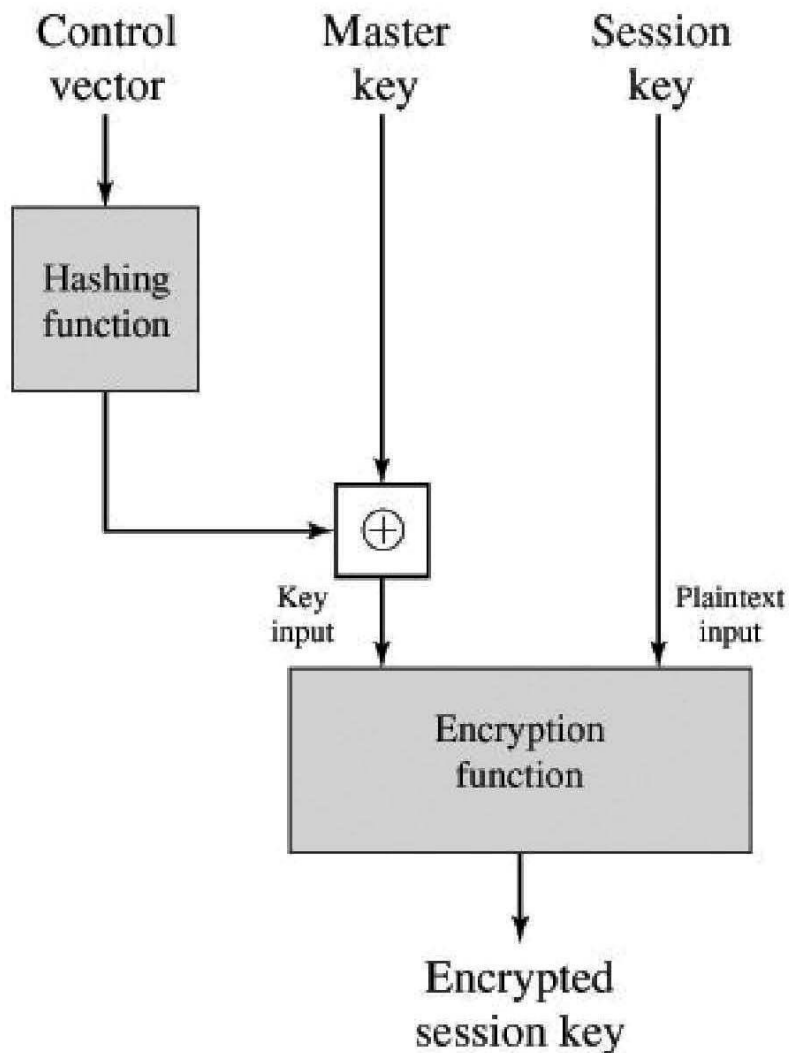


ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΔΙΑΝΟΜΗ ΚΛΕΙΔΙΩΝ (5/5)

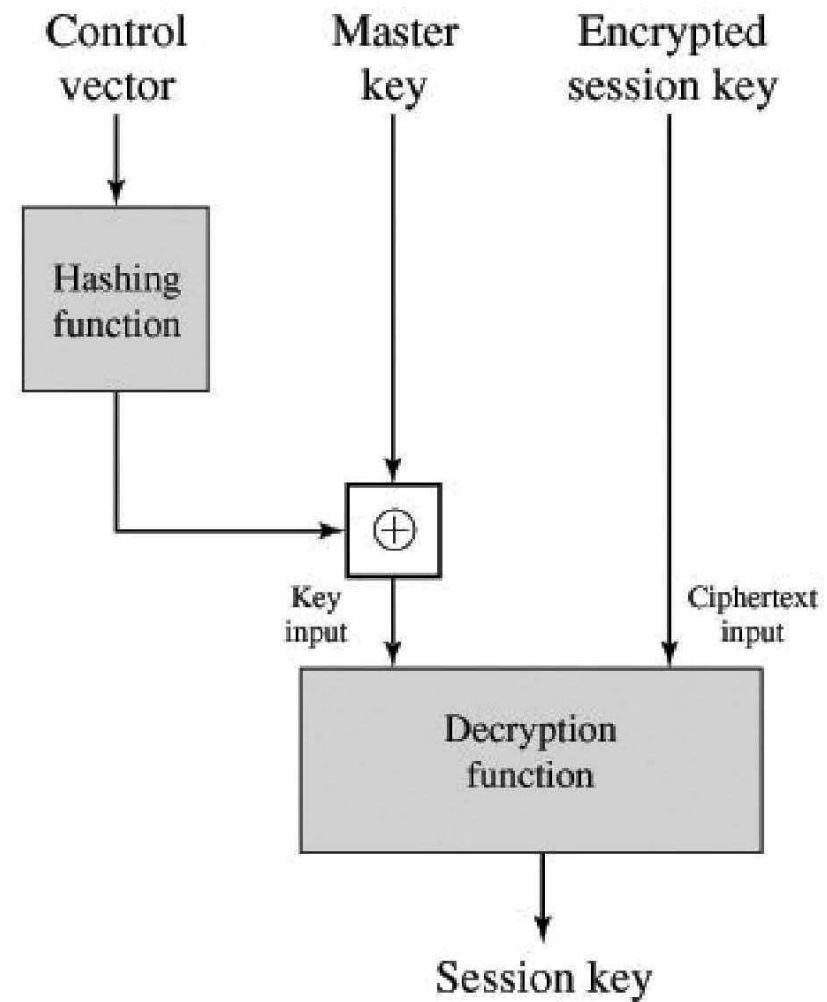
- Βήμα 4. Ο FEP έχει τη δυνατότητα να αποστείλει το πακέτο αιτήματος σύνδεσης και να πραγματοποιηθεί μια σύνδεση μεταξύ των δύο συστημάτων. Τα δεδομένα του χρήστη κρυπτογραφούνται από τους αντίστοιχους FEP χρησιμοποιώντας το κλειδί συνόδου μιας χρήσης



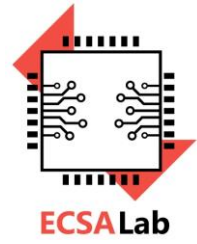
ΚΡΥΠΤΟΓΡΑΦΗΣΗ SESSION KEY: ΔΙΑΝΥΣΜΑ ΕΛΕΓΧΟΥ



(a) Control Vector Encryption



(b) Control Vector Decryption



Απορίες???