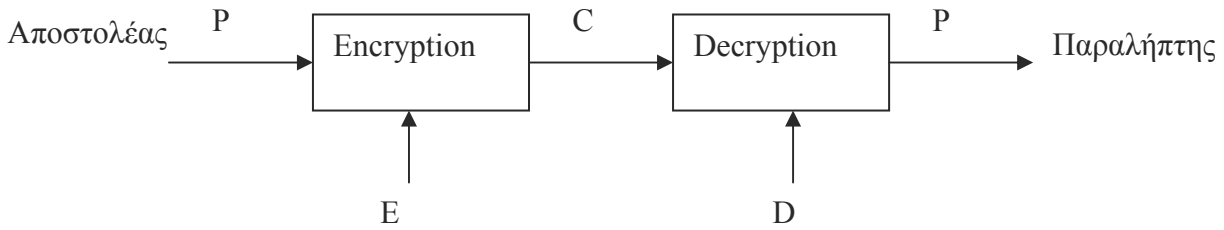
Κρυπτογραφία

Αλγόριθμοι Δημοσίου Κλειδιού
(ή ασύμμετροι αλγόριθμοι)

Κρυπτοσυστήματα Δημοσίου κλειδιού

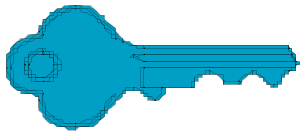


- Προτάθηκαν το 1976
- Κάθε συμμετέχων στο σύστημα κατέχει ένα ζευγάρι κλειδιών e και d, που το ένα αντιστρέφει το άλλο: d(e(m))=m
- Ένα από τα δύο κλειδιά είναι γνωστό σε όλους (το e) και λέγεται Δημόσιο Κλειδί. Το άλλο κλειδί το γνωρίζει μόνο ο κάτοχός του και ονομάζεται ιδιωτικό. Απαραίτητη προϋπόθεση είναι ότι η γνώση του e δεν οδηγεί σε προσδιορισμό του μυστικού κλειδιού d.

Τρόπος λειτουργίας συστημάτων δημοσίου κλειδιού

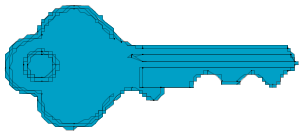
- Όταν ένα πρόσωπο A θέλει να στείλει ένα μήνυμα m σε ένα πρόσωπο B, το δημόσιο κλειδί κρυπτογράφησης του παραλήπτη B χρησιμοποιείται για τη δημιουργία του κρυπτογράμματος $E_e(m)$. Αφού το E_e είναι πλήρως διαθέσιμο σε όλους, ο οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα με προορισμό τον B. Ωστόσο, μόνο ο B, ο οποίος γνωρίζει το ιδιωτικό του κλεδί D_B μπορεί να ανακατασκευάσει το αρχικό μήνυμα, εφαρμόζοντας τον αντίστροφο μετασχηματισμό D_B $(E_B(m))$.

Σχηματική αναπαράσταση

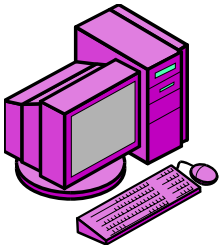


Κρυπτογράφηση με το δημόσιο κλειδί του Β

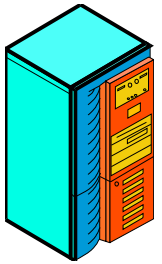
Κρυπτογραφημένο μήνυμα



Αποκρυπτογράφηση με το ιδιωτικό κλειδί του Β

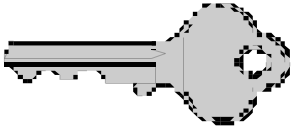


Χρήστης Α



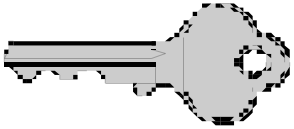
Χρήστης Β

Αποκρυπτογράφηση με το ιδιωτικό κλειδί του Α



Κρυπτογραφημένο μήνυμα

Κρυπτογράφηση με το δημόσιο κλειδί του Α



Μαθηματική Θεωρία

- Συνάρτηση μίας κατεύθυνσης (one-way) ονομάζεται κάποια συνάρτηση η οποία είναι εύκολο να υπολογιστεί, αλλά πολύ δύσκολο να αντιστραφεί. 'Καταπακτή' ('trapdoor') σε μία τέτοια συνάρτηση αποκαλείται οποιαδήποτε γνώση μας επιτρέπει να την αντιστρέψουμε.
- Η κρυπτογράφηση σε ένα σύστημα Δημοσίου Κλειδιού πρέπει να είναι μία 'one-way' συνάρτηση η οποία πρέπει να έχει ένα 'trapdoor' (που στην ουσία αντιστοιχεί στο ιδιωτικό κλειδί αποκρυπτογράφησης).
- Το 'trapdoor' πρέπει να το γνωρίζει μόνο ο παραλήπτης.

Στοιχεία Θεωρίας Πολυπλοκότητας

- Προβλήματα τα οποία μπορούν να επιλυθούν σε πολυωνυμικό χρόνο ανήκουν στην κλάση P
- Προβλήματα των οποίων μία καταφατική απάντηση μπορεί να επιβεβαιωθεί σε πολυωνυμικό χρόνο, δοθείσας κάποιας επιπρόσθετης πληροφορίας, ανήκουν στην κλάση NP
- Προβλήματα των οποίων μία αρνητική απάντηση μπορεί να επιβεβαιωθεί σε πολυωνυμικό χρόνο, δοθείσας κάποιας επιπρόσθετης πληροφορίας, ανήκουν στην κλάση co-NP
- Τα πιο δύσκολα NP προβλήματα ονομάζονται NP-complete.

Στοιχεία Θεωρίας Πολυπλοκότητας

- Ένα NP πρόβλημα χαρακτηρίζεται από το ότι δεν έχει βρεθεί πολυωνυμικός αλγόριθμος που να το επιλύει. Αντίστοιχα, για όσα προβλήματα υπάρχει λύση που τρέχει σε πολυωνυμικό χρόνο, αυτά υπάγονται στην κλάση P.
- Ισχύει $P \subseteq NP$
- Παρόλο που πιστεύεται ότι $NP \neq P$, εν τούτοις δεν έχει αποδειχτεί
- Παράδειγμα: η ανάλυση ενός αριθμού στους πρώτους του παράγοντες είναι NP πρόβλημα
- Συναρτήσεις μίας κατεύθυνσης στην πράξη θεωρούνται αυτές που εμφανίζονται στα NP προβλήματα. Όλοι λοιπόν οι αλγόριθμοι Δημοσίου Κλειδιού βασίζονται σε NP προβλήματα – η δυσκολία επίλυσης των οποίων καθιστά τους αλγορίθμους ασφαλείς.

Παραδείγματα συστημάτων Δημοσίου Κλειδιού

- RSA (αναπτύσσεται στο εργαστηριακό μάθημα)
- El Gamal (αναπτύσσεται στο εργαστηριακό μάθημα)
- Κρυπτοσύστημα Rabin (θα αναπτυχθεί παρακάτω)
- McEliece κρυπτοσύστημα
- Knapsak αλγόριθμοι
- Elliptic Curve κρυπτοσύστημα (ελλειπτικών καμπυλών)
- Και άλλοι….

Χρήσιμα Μαθηματικά Εργαλεία – Θεώρημα Κινεζικού Υπολοίπου (Chinese Remainder Theorem (CRT))

- Επειδή η αποκρυπτογράφηση στο σύστημα Rabin που θα δούμε στη συνέχεια βασίζεται στο Θεώρημα Κινεζικού Υπολοίπου (CRT), το εν λόγω θεώρημα θα αναπτυχθεί ανεξάρτητα στις επόμενες τρεις διαφάνειες.
- Έστω $m_1, \ldots, m_r$ ακέραιοι αριθμοί, πρώτοι μεταξύ τους, και έστω επίσης $a_1, \ldots, a_r$ ακέραιοι αριθμοί.

  Τότε το σύστημα ισοδυναμιών:

  $$x \equiv a_i \bmod m_i \ , \ i = 1, \ldots, r$$

  έχει *μοναδική* λύση modulo $M = m_1 \, x \ldots x \, m_r$, η οποία είναι

  $$x = \sum a_i M_i y_i \bmod M,$$

  όπου $M_i = M/m_i$ και $y_i = M_i^{-1} \bmod m_i$, $i = 1, \ldots, r$

Παράδειγμα για το Θεώρημα Κινεζικού Υπολοίπου

- Έστω το ακόλουθο σύστημα ισοδυναμιών:

$$x \equiv 1 \bmod 3$$
$$x \equiv 2 \bmod 4$$
$$x \equiv 3 \bmod 5$$

- Αναζητούμε τη λύση του συστήματος – δηλαδή, έναν αριθμό x που ικανοποιεί και τις 3 παραπάνω σχέσεις.
- Επειδή τα 3,4,5 είναι πρώτοι μεταξύ τους, το σύστημα αυτό έχει μοναδική λύση mod 60 ($60 = 3 \cdot 4 \cdot 5$).
- Εργαζόμαστε λοιπόν ως εξής:
  - $M_1 = 3 \cdot 4 \cdot 5 / 3 = 20$
  - $M_2 = 3 \cdot 4 \cdot 5 / 4 = 15$
  - $M_3 = 3 \cdot 4 \cdot 5 / 5 = 12$

Παράδειγμα για το Θεώρημα Κινεζικού Υπολοίπου (συνέχεια)

- Χρειαζόμαστε επίσης και τα αντίστροφα των M_1, M_2, M_3.
- Για τον αντίστροφο του M_1, αναζητούμε y_1 τέτοιο ώστε $M_1 y_1 \equiv 1 \bmod 3$. Με δοκιμές βρίσκουμε ότι $y_1=2$.
- Αντίστοιχα, οι αντίστροφοι των M_2, M_3 υπολογίζονται ότι είναι ίσοι με $y_2=3$, $y_3=3$ αντίστοιχα.
- Συνεπώς η λύση του αρχικού συστήματος είναι:
- $x \equiv 1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \bmod 60 \equiv$
- $\equiv 40 + 90 + 108 \bmod 60 \equiv 40 + 30 + 48 \bmod 60 \equiv$
- $\equiv 118 \bmod 60 \equiv 58 \bmod 60$

Αλγόριθμος Rabin

- Ένας χρήστης Α επιλέγει δύο τυχαίους πολύ μεγάλους πρώτους αριθμούς p, q και υπολογίζει το γινόμενό τους N
- Το δημόσιο κλειδί του Α είναι το N, και το ιδιωτικό τα p, q.
- Για την κρυπτογράφηση του μηνύματος **m** που θέλει να στείλει κάποιος χρήστης στον Α, απλά το υψώνει στο τετράγωνο mod N:

$$\mathbf{c \equiv m^2 \ (mod\ N)}$$

Αρχικό μήνυμα *κρυπτόγραμμα*

- Στην ουσία, η συνάρτηση $f(x) \equiv x^2 \bmod N$ είναι μίας κατεύθυνσης (για πολύ μεγάλο N): κάποιος που γνωρίζει το x μπορεί να υπολογίσει το f(x), αλλά από την άλλη κάποιος που γνωρίζει το f(x) δεν είναι εύκολο να βρει το x.
  - Όμως, όπως θα δούμε παρακάτω, αν κάποιος γνωρίζει είτε το p είτε το q μπορεί να εξάγει το x από το f(x) (τα p και q λοιπόν είναι «καταπακτές» (trapdoors). Άρα, μόνο ο Α μπορεί να αποκρυπτογραφήσει το κρυπτόγραμμα c που λαμβάνει και να ανακτήσει το αρχικό μήνυμα m.

Αποκρυπτογράφηση Rabin

- Ειδική περίπτωση: τα p, q επιλέγονται με τέτοιον τρόπο ώστε να ισχύει p,q ≡ 3 mod 4 (αυτό γίνεται για λόγους απλότητας – στην πράξη τα p, q μπορεί να είναι οποιαδήποτε, αλλά τότε ο αλγόριθμος αποκρυπτογράφησης γίνεται πιο σύνθετος).
- Έστω ότι ο παραλήπτης θέλει να αποκρυπτογραφήσει το $y \equiv x^2 \bmod N$. Όταν ισχύει $p,q \equiv 3 \bmod 4$, υπάρχει ένας απλός τρόπος υπολογισμού του x: προσέξτε ότι

$$(\pm y^{(p+1)/4})^2 \equiv y^{(p+1)/2} \equiv y^{(p-1)/2} y \equiv y \bmod p$$

μια που ισχύει λόγω του θεωρήματος του Euler (το οποίο είδαμε και στον RSA)

$$y^{(p-1)/2} \bmod(\mathrm{p}) \equiv x^{p-1} \bmod(p) \equiv 1 \bmod(p)$$

(προσέξτε ότι φ(p)=p-1)

Αποκρυπτογράφηση Rabin (συνέχεια)

- Από την προηγούμενη ανάλυση έπεται ότι ο αριθμός:

$$\pm y^{(p+1)/4} \bmod p$$

είναι μια τετραγωνική ρίζα του *y* modulo *p.*

- Μια παρόμοια ανάλυση μπορεί να γίνει και για τον άλλον πρώτο αριθμό q.
- Βρίσκουμε λοιπόν τα τετραγωνικά υπόλοιπα modulo *p* και modulo *q*. Έτσι, μπορούμε να βρούμε το ζητούμενο τετραγωνικό υπόλοιπο modulo N με το θεώρημα του Κινεζικού υπολοίπου

Παράδειγμα κρυπτογράφησης Rabin

Έστω p=7 και q=11 (παρατηρήστε ότι p,q≡3 mod 4.)

Τότε N = 77.

Έστω ότι ο χρήστης λαμβάνει ως κρυπτόγραμμα τον αριθμό 23. Τότε εργάζεται ως εξής:

$$\pm 23^{(7+1)/4} \equiv \pm 2^2 \equiv \pm 4 \bmod 7$$

$$\pm 23^{(11+1)/4} \equiv \pm 1^3 \equiv \pm 1 \bmod 11$$

Παράδειγμα κρυπτογράφησης Rabin (συνέχεια)

Εφαρμογή του Θεωρήματος του Κινεζικού Υπολοίπου:

1) $x \equiv 4 \bmod 7$

$x \equiv 1 \bmod 11$

Έχουμε $M_1=11$, $M_2=7$.

Για τον αντίστροφο y_1 του M_1 δοκιμάζουμε να λύσουμε τη σχέση

$11y_1 \equiv 1 \bmod 7$ όπου με δοκιμές βρίσκουμε $y_1=2$.

Για τον αντίστροφο y_2 του M_2 δοκιμάζουμε να λύσουμε τη σχέση
$7y_2 \equiv 1 \bmod 11$ όπου με δοκιμές βρίσκουμε $y_2=8$.

Άρα η λύση του παραπάνω συστήματος είναι $(4 \cdot 11 \cdot 2 + 1 \cdot 7 \cdot 8) \bmod 77 \equiv$
$\equiv (88+56) \bmod 77 \equiv 144 \bmod 77 \equiv 67 \bmod 77$

Παράδειγμα κρυπτογράφησης Rabin (συνέχεια)

2) $x \equiv -4 \bmod 7$

$x \equiv 1 \bmod 11$

Όλοι οι απαραίτητοι υπολογισμοί έχουν γίνει από πριν, άρα η λύση του παραπάνω συστήματος είναι $(-4 \cdot 11 \cdot 2 + 1 \cdot 7 \cdot 8) \bmod 77 \equiv$
$\equiv (-88+56) \bmod 77 \equiv -32 \bmod 77 \equiv 45 \bmod 77$.

3) $x \equiv 4 \bmod 7$

$x \equiv -1 \bmod 11$

Η λύση του παραπάνω συστήματος είναι $(4 \cdot 11 \cdot 2 - 1 \cdot 7 \cdot 8) \bmod 77 \equiv$
$\equiv (88-56) \bmod 77 \equiv 32 \bmod 77$

4) $x \equiv -4 \bmod 7$

$x \equiv -1 \bmod 11$

Η λύση του παραπάνω συστήματος είναι $(-4 \cdot 11 \cdot 2 - 1 \cdot 7 \cdot 8) \bmod 77 \equiv$
$\equiv (-88-56) \bmod 77 \equiv -144 \bmod 77 \equiv 10 \bmod 77$

Συνεπώς τα 4 πιθανά μηνύματα (ένα εκ των οποίων εστάλη) είναι τα $\pm 10 \bmod 77,\ \pm 32 \bmod 77$

Σχόλια για τον αλγόριθμο Rabin

- Βρίσκουμε πάντα 4 πιθανά μηνύματα, για δοθέν κρυπτόγραμμα. Αυτό είναι μειονέκτημα (το ιδανικό θα ήταν να βρίσκαμε πάντα ακριβώς το αρχικό μήνυμα). Μια τυπική τεχνική για να αντιμετωπιστεί αυτό το πρόβλημα είναι η εξής:
  - Εισαγωγή περισσότερων πλεοναστικών ψηφίων στο μήνυμα που αποστέλλεται, με στόχο να βοηθήσουν στη σωστή αποκρυπτογράφηση. Για παράδειγμα, το μήνυμα που στέλνεται μπορεί περιέχει ένα διπλότυπο του εαυτού του (δηλαδή, αντί να στείλουμε το 45, να στέλνουμε το 4545). Έτσι ο παραλήπτης μπορεί πια να αποφασίσει, από τα 4 λαμβανόμενα μηνύματα, ποιο είναι αυτό που πραγματικά εστάλη.

Ασφάλεια του αλγορίθμου Rabin

- Η ασφάλεια του αλγορίθμου έγκειται σε δύο προβλήματα που ανήκουν στο NP:
  - Στο πρόβλημα του να βρει κανείς το τετραγωνικό υπόλοιπο modulo n (δηλαδή, το να ξέρει κανείς το $x^2 \bmod n$ δεν του αρκεί για να βρει το x).
  - Για μεγάλα p,q, ο οποιοσδήποτε γνωρίζει το n δεν μπορεί να βρει τα p,q (η παραγοντοποίηση ενός αριθμού σε πρώτους παράγοντες είναι υπολογιστικά δύσκολο πρόβλημα (ανήκει στην κλάση NP),

Γενικά πλεονεκτήματα των συστημάτων Δημοσίου Κλειδιού

- Το ζεύγος δημόσιο κλειδί – ιδιωτικό κλειδί μπορεί να μένει το ίδιο για μεγάλα χρονικά διαστήματα (π.χ. για χρόνια) – στα συστήματα συμμετρικού κλειδιού αντιθέτως, το κλειδί πρέπει να αλλάζει συχνά
- Σε ένα μεγάλο δίκτυο, ο αριθμός των κλειδιών που χρειάζονται είναι μικρότερος από ό,τι αν χρησιμοποιούνταν συμμετρική κρυπτογράφηση (στη συμμετρική κρυπτογράφηση, χρειάζεται ένα ζευγάρι κλειδιών για κάθε χρήστη).

Γενικά μειονεκτήματα των συστημάτων Δημοσίου Κλειδιού

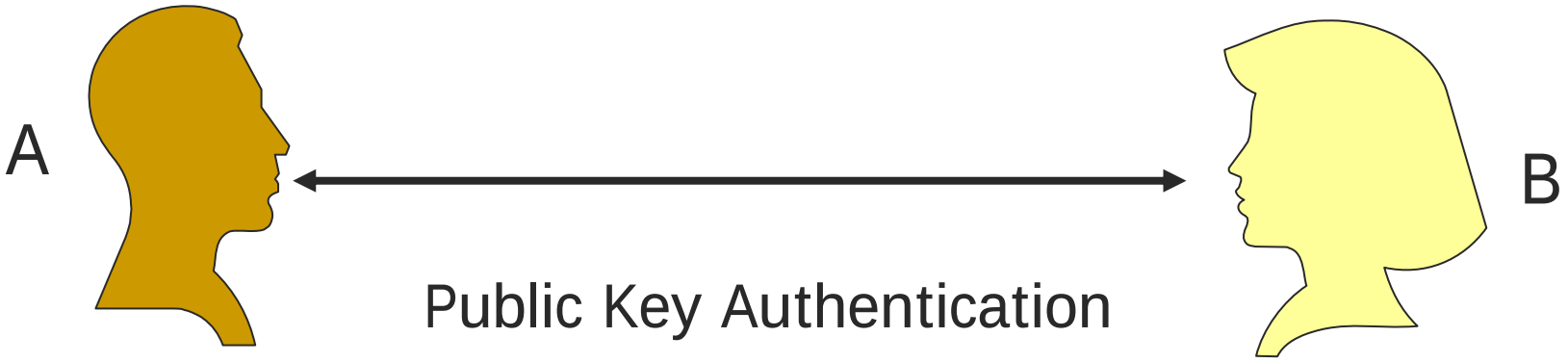
- Η απόδοση (throughput) είναι σημαντικά μικρότερη, συγκριτικά με τους καλύτερους block ciphers
- Το μήκος των κλειδιών είναι πιο μεγάλο
- Κανένας αλγόριθμος δεν έχει αποδειχτεί ότι είναι απόλυτα ασφαλής - η ασφάλειά τους στηρίζεται σε γνωστά NP προβλήματα. Αν βρεθεί πολυωνυμική (δηλαδή, με απλά λόγια, γρήγορη) λύση για κάποιο από αυτά τα προβλήματα, η ασφάλεια καταρρέει (κάτι τέτοιο θα σήμαινε ότι οποιοσδήποτε θα μπορούσε να ανακτήσει το ιδιωτικό κλειδί).
  - Πάντως, θα πρέπει να σημειωθεί ότι ούτε οι αλγόριθμοι συμμετρικού κλειδιού (stream ciphers, block ciphers) είναι εγγυημένα ασφαλείς

Συνδυασμός συστημάτων Δημοσίου και Συμμετρικού Κλειδιού

- Όχι ανταγωνιστικά – χρησιμοποιούνται μαζί
  - Το δημόσιο κλειδί διαμοιράζεται εύκολα, αλλά μπορεί να χρησιμοποιηθεί μόνο σε μικρά μηνύματα
  - Το συμμετρικό κλειδί διανέμεται δύσκολα (πρόβλημα εύρεσης ασφαλούς «καναλιού» μετάδοσής του), αλλά μπορεί να χρησιμοποιηθεί και σε μεγάλα μηνύματα
  - Έχουν συμπληρωματικά προτερήματα και ελαττώματα

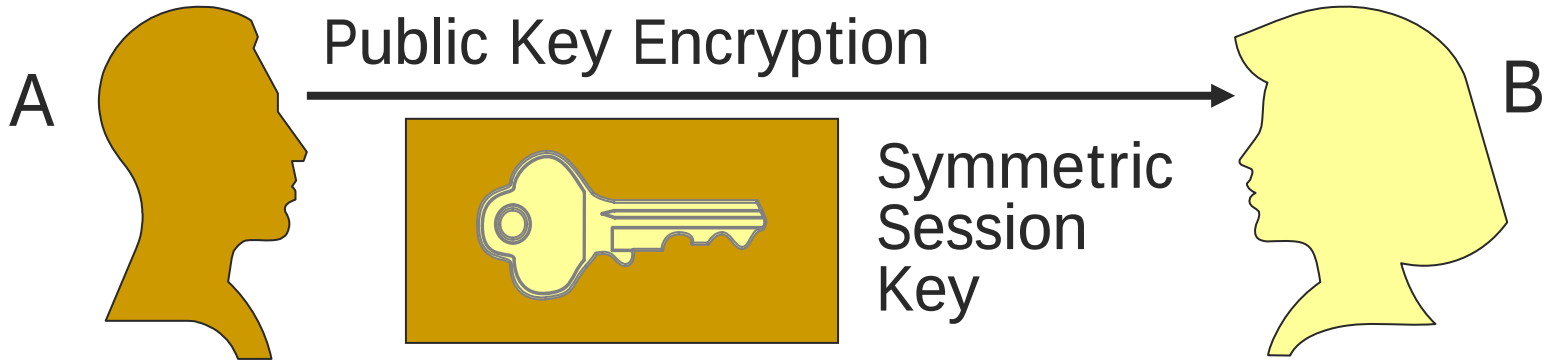
Συνδυασμός Συμμετρικού – Δημοσίου Κλειδιού

- Συχνά, η επικοινωνία ξεκινά με πιστοποίηση ταυτότητας, με χρήση αλγορίθμου Δημοσίου κλειδιού



Συνδυασμός Συμμετρικού – Δημοσίου Κλειδιού (ΙΙ)

- Στη συνέχεια, ο καθένας παράγει ένα συμμετρικό κλειδί
- Κρυπτογραφεί το συμμετρικό του κλειδί με το δημόσιο κλειδί του άλλου και του το στέλνει
  - Έτσι, και οι δύο έχουν το συμμετρικό κλειδί για την επικοινωνία με τον άλλο



Συνδυασμός Συμμετρικού – Δημοσίου Κλειδιού (III)

- Τελικά, επικοινωνεί ο ένας με τον άλλον με το συμμετρικό κλειδί
- Με άλλα λόγια, η κρυπτογραφία δημόσιου κλειδιού έλυσε το πρόβλημα της εύρεσης ασφαλούς καναλιού, για την ανταλλαγή των κλειδιών