

# Μοντέλα και Αποδείξεις Ασφάλειας στην Κρυπτογραφία - Ανταλλαγή Κλειδιού Diffie Hellman

---

Παναγιώτης Γροντάς - Άρης Παγουρτζής

21/11/2023

ΕΜΠ - Κρυπτογραφία

# Ερωτήματα

- Τι σημαίνει ότι ένα σύστημα είναι ασφαλές;
- Πώς αποδεικνύεται;



## Μειονέκτημα

Ασφαλές: προστασία  $\forall$  επίθεση

Μη-Ασφαλές:  $\exists$  μία επιτυχής επίθεση

Σύγχρονη Κρυπτογραφία: Αυστηροί Ορισμοί και Αποδείξεις

# Ορισμοί

---

- $CS = (M, K, C, KGen, Enc, Dec)$
- $M$ : Σύνολο Μηνυμάτων
- $K$ : Σύνολο Κλειδιών
- $C$ : Σύνολο Κρυπτοκειμένων

- $KGen(1^\lambda) = (key_{Enc}, key_{Dec}) \in K^2$ 
  - Πιθανοτικός Αλγόριθμος
  - Το κλειδί συνήθως επιλέγεται *ομοιόμορφα* από το  $K$
  - $\lambda$  : Παράμετρος ασφάλειας - πλήθος bits του κλειδιού
    - Συμβολισμός στο μοναδιαίο ( $\lambda$  '1'): Χαρακτηρισμός ως προς το μέγεθος της εισόδου, όχι ως προς το μέγεθος της αναπαράστασής της
    - Πχ. για ασφάλεια 80 bits θέλουμε το κλειδί να έχει 80 δυαδικά ψηφία και όχι  $\log_2 80 = 7$  ή  $\log_{10} 80 = 2$
    - Σημασία για χρόνο παραγωγής κλειδιών, εκτέλεσης κρυπτογράφησης, υπολογιστικής προσπάθειας - πιθανότητας επιτυχίας 'σπασίματος'

## Κρυπτογράφηση

$$\text{Enc}(\text{key}_{\text{enc}}, m) = c \in \mathcal{C}$$

- Ντετερμινιστικός Αλγόριθμος: Κάθε μήνυμα αντιστοιχεί σε ένα κρυπτοκείμενο
- Πιθανοτικός Αλγόριθμος: Κάθε μήνυμα αντιστοιχεί σε ένα σύνολο πιθανών κρυπτοκειμένων

## Αποκρυπτογράφηση

$$\text{Dec}(\text{key}_{\text{dec}}, c) = m$$

## Ορθότητα

$$\text{Dec}(\text{key}_{\text{dec}}, \text{Enc}(\text{key}_{\text{enc}}, m)) = m, \forall m \in \mathcal{M}$$

- Συμμετρικό Κρυπτοσύστημα  $key_{enc} = key_{dec}$
- Ασύμμετρο Κρυπτοσύστημα  $key_{enc} \neq key_{dec}$ 
  - Κρυπτογραφία Δημοσίου Κλειδιού
  - Το  $key_{enc}$  μπορεί να δημοσιοποιηθεί για την εύκολη ανταλλαγή μηνυμάτων
  - Το  $key_{dec}$  είναι μυστικό

- Στόχος: Να παραβιάσει την ασφάλεια.
- Δηλαδή, για το κρυπτοκείμενο  $c$ :
  - Να μάθει το κλειδί  $k$ ;
    - Θέλουμε να προστατεύσουμε το μήνυμα
    - Τετριμμένα  $\text{Enc}(k, m) = m$  είναι αδύνατο να σπάσει, αλλά τι ασφάλεια παρέχει;
  - Να μάθει ολόκληρο το αρχικό μήνυμα  $m$ ;
    - Αν μάθει το 90%;
  - Να μάθει κάποια συνάρτηση του  $m$ ;
    - Ναι αλλά ποια;
- Συμπέρασμα: Χρειάζονται ακριβείς ορισμοί
  - Για τις δυνατότητες και τα μέσα του αντιπάλου.
  - Για τον τρόπο αλληλεπίδρασής του με το σύστημα.
  - Για το κριτήριο επιτυχίας - 'σπάσιμο'.



## Είδη επιθέσεων

---

# Επίθεση Μόνο Κρυπτοκειμένου - Ciphertext Only Attack (COA)

- Παθητικός Αντίπαλος (Eve)
- Πολύ εύκολη: Χρειάζεται απλά πρόσβαση στο κανάλι επικοινωνίας

# Επίθεση Γνωστού Μηνύματος - Known Plaintext Attack (ΚΡΑ)

- Παθητικός Αντίπαλος
- Γνωρίζει ζεύγη μηνυμάτων - κρυπτοκειμένων
- Τετριμμένο σενάριο για ασύμμετρα, γιατί:
  - Ο  $\mathcal{A}$  έχει το δημόσιο κλειδί
  - Μπορεί να κατασκευάσει μόνος του όσα ζεύγη θέλει
- Ρεαλιστικό σενάριο και για συμμετρικά, γιατί:
  - Ακόμα και τα κρυπτογραφημένα πρωτόκολλα περιέχουν μη απόρρητα μηνύματα (handshakes, ack)
  - Ιστορικό παράδειγμα: Κρυπτοκείμενα πρόγνωσης καιρού στη μηχανή Enigma
  - Κρυπτογραφημένα μηνύματα γίνονται κάποια στιγμή διαθέσιμα

# Επίθεση Επιλεγμένου Μηνύματος - Chosen Plaintext Attack (CPA)

- *Ενεργός Αντίπαλος (Mallorie)*
- Γνωρίζει ζεύγη μηνυμάτων - κρυπτοκειμένων
- *Μπορεί να ζητήσει την κρυπτογράφηση μηνυμάτων της επιλογής του (Μαντείο Κρυπτογράφησης)*
- Ιστορικό Παράδειγμα: Σπάσιμο κρυπτοσυστήματος JN-25b στη ναυμαχία του Midway (Ιούνιος 1942)
  - Υποψία ότι  $\text{Enc}(\text{"Midway"}) = \text{"AF"}$
  - Αποστολή Πλαστών Μηνυμάτων για επισκευή του συστήματος υδροδότησης του 'Midway'
  - Συλλογή Επικοινωνιών Με Κρυπτοκείμενα 'AF'
  - Συσχέτιση με παλιότερες επικοινωνίες

# Επίθεση Επιλεγμένου Κρυπτοκειμένου

## Chosen Ciphertext Attack (CCA)

- Ενεργός Αντίπαλος
- Γνωρίζει ζεύγη μηνυμάτων - κρυπτοκειμένων
- Μπορεί να ζητήσει την κρυπτογράφηση μηνυμάτων της επιλογής του (Μαντείο Κρυπτογράφησης)
- Μπορεί να επιτύχει την αποκρυπτογράφηση μηνυμάτων της επιλογής του (Μαντείο Αποκρυπτογράφησης)
- Διαισθήση: Ο αντίπαλος μπορεί να βγάλει έμμεσα συμπεράσματα από αντιδράσεις σε κρυπτογραφημένα μηνύματα
  - Απόρριψη κρυπτογραφημένων 'σκουπιδιών' από το πρωτόκολλο (Bleichenbacher RSA PKCS1 attack)
  - Ενέργεια στον πραγματικό κόσμο (πχ. αγορά μετοχών)

# Μοντέλα Ασφάλειας

---

# Οι κανόνες του Kerchoffs (1883)

Οι πρώτες προσπάθειες ορισμού ασφάλειας  
κρυπτοσυστημάτων και προστασίας

## Αρχή 2

Ο αλγόριθμος(από)κρυπτογράφησης δεν πρέπει να είναι  
μυστικός. Πρέπει να μπορεί να πέσει στα χέρια του  $\mathcal{A}$  χωρίς να  
δημιουργήσει κανένα πρόβλημα. Αντίθετα το κλειδί μόνο  
πρέπει να είναι μυστικό.

Λόγοι:

- Το κλειδί διανέμεται πιο εύκολα από τους αλγόριθμους  
(μικρότερο μέγεθος, απλούστερη δομή)
- Το κλειδί είναι πιο εύκολο να αλλαχθεί αν διαρρεύσει
- Πιο πρακτική χρήση για περισσότερους από έναν  
συμμετέχοντες
- Ανοικτό κρυπτοσύστημα: Εύκολη μελέτη

## Οι κανόνες του Kerchoffs (1883) - (2)

Παρατηρήσεις:

Αν και έχουν παράδοση ακόμα και σήμερα δεν εφαρμόζονται πλήρως

- (Μεγάλες) εταιρίες δημιουργούν και χρησιμοποιούν δικούς τους μυστικούς αλγόριθμους/πρωτόκολλα
- Crypto Snake Oil (Bruce Schneier)



## Αρχή 1

Το κρυπτοσύστημα θα πρέπει να είναι *πρακτικά* απρόσβλητο, αν δεν γίνεται θεωρητικά

- Διάρκεια Κρυπτανάλυσης > Διάρκεια Ζωής Μηνύματος
- Μικρή Πιθανότητα Επιτυχίας
- Υπολογιστική Ασφάλεια

Εμπειρική αρχή - δεν αντιστοιχίζονται σε κάτι πρακτικό

## Ιδέα

Μαθηματική (Λογική) απόδειξη ότι το κρυπτοσύστημα έχει κάποιες ιδιότητες ασφάλειας.

Παράδειγμα: Τέλεια μυστικότητα (Shannon)

Μπορεί να εφαρμοστεί στην κρυπτογραφία δημοσίου κλειδιού;  
Γιατί;

Επαναχρησιμοποίηση δημοσίου κλειδιού

# Σημασιολογική Ασφάλεια

Βασική ιδέα (Goldwasser, Micali):

Χαλαρώνουμε τις απαιτήσεις ασφάλειας για να οδηγηθούμε σε έναν πρακτικό ορισμό

Λαμβάνουμε υπ' όψιν:

- την υπολογιστική ισχύ του  $\mathcal{A}$
- την πιθανότητα επιτυχίας
- το είδος των επιθέσεων

## Διαίσθηση

Ένας υπολογιστικά περιορισμένος  $\mathcal{A}$  δεν μπορεί να μάθει τίποτε χρήσιμο από το κρυπτοκείμενο παρά μόνο με αμελητέα πιθανότητα

## Ορισμός

Ένα κρυπτοσύστημα είναι  $(\tau, \epsilon)$  ασφαλές αν οποιοσδήποτε  $\mathcal{A}$  σε χρόνο (πλήθος λειτουργιών) το πολύ  $\tau$ , δεν μπορεί να το σπάσει με πιθανότητα καλύτερη από  $\epsilon$

Κάθε κρυπτοσύστημα με μήκος κλειδιού  $\lambda$  bits έχει ασφάλεια στην καλύτερη περίπτωση  $(\tau, \frac{\tau}{2^\lambda})$

## Επίθεση Brute Force

Με  $\tau = 2^\lambda$  λειτουργίες το κρυπτοσύστημα θα σπάσει. Θα θέλαμε να είναι το καλύτερο δυνατό που μπορεί να γίνει.

## Πρακτικά

Για συμμετρικά κρυπτοσυστήματα σήμερα με βραχυχρόνιες απαιτήσεις ασφάλειας  $2^{80} < \tau < 2^{100}$  και  $\epsilon = 2^{-64}$

Για μακροχρόνιες απαιτήσεις ασφαλείας:  $\tau = 2^{128}$

Κβαντικοί υπολογιστές  $\tau = 2^{256}$  (Αλγόριθμος αναζήτησης

## Ρητή Προσέγγιση (2)

### Κάποιοι αριθμοί

Distributed.net RC5 brute force cracking

- 56bits - 250 μέρες - 1997
- 64bits - 5 χρόνια - 2002
- 72bits - δεν έχει σπάσει ακόμα (μετά 15 χρόνια είχε εξερευνηθεί το 5% του  $K$ )
- Bitcoin miners: Υπολογισμός περίπου  $2^{93}$  hashes όλο το 2022
- $2^{88}$  αριθμός δευτερολέπτων από το Big - Bang

Δεν χρησιμοποιείται γιατί:

- Δεν λαμβάνει υπ' όψιν το υπολογιστικό μοντέλο (παράλληλοι υπολογιστές, εξειδικευμένο HW κτλ.)

## Ορισμός

Ένα κρυπτοσύστημα είναι ασφαλές αν οποιοσδήποτε περιορισμένος  $\mathcal{A}$  έχει αμελητέα πιθανότητα να το σπάσει (σε σχέση με την παράμετρο ασφάλειας)

Παρατηρήσεις:

- περιορισμένος = Probabilistic Polynomial Time
- Ισχύει για μεγάλες τιμές του  $\lambda$
- Συνέπεια του  $|K| < |M|$
- Επιτρέπει προσαρμογή της ασφάλειας με αλλαγή του μήκους του κλειδιού

- Ο  $\mathcal{A}$  θέλει να υπολογίσει το κατηγορήμα  $q : \mathcal{M} \rightarrow \{0, 1\}$
- Γενικά:  $\Pr_{m \in \mathcal{M}}[q(m) = 0] = \Pr_{m \in \mathcal{M}}[q(m) = 1] = \frac{1}{2}$
- Το μήκος των κρυπτοκειμένων είναι το ίδιο (δεν διαρρέει πληροφορία)

**Το πλεονέκτημα του  $\mathcal{A}$**

$$\text{Adv}_q^{\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(c) = q(\text{Dec}(\text{key}, c))] - \frac{1}{2}|$$

Αν ο  $\mathcal{A}$  μαντέψει στην τύχη έχει  $\text{Adv}_q(\mathcal{A}) = 0$

## Ορισμός

Ένα κρυπτοσύστημα  $\mathcal{CS}$  είναι σημασιολογικά ασφαλές όταν  $\forall$  PPT  $\mathcal{A}$ ,  $\forall q$ :

$$\text{Adv}_q^{\mathcal{A}}(\lambda) = \text{negl}(\lambda)$$

## Αμελητέα συνάρτηση

Οποιαδήποτε συνάρτηση  $f$  για την οποία για κάθε πολυώνυμο  $p$  υπάρχει  $n_0$  ώστε  $\forall n \geq n_0 : f(n) < \frac{1}{p(n)}$

Δηλαδή: Μεγαλώνει με πιο αργό ρυθμό από αντίστροφο πολυώνυμο

Παραδείγματα αμελητέων συναρτήσεων:  $2^{-n}, 2^{-\sqrt{n}}$



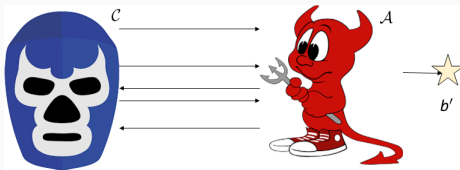
### Παρατηρήσεις

- Ο τυπικός ορισμός ενσωματώνει την παράμετρο ασφαλείας
- Δύσχρηστος ορισμός - δεν ορίζουμε τι ξέρει ο  $\mathcal{A}$  και τι διαδικασία ακολουθεί για το 'σπάσιμο'
- Ανάγκη εύρεση κατηγορήματος - που δεν ικανοποιεί τον ορισμό.

# Μη Διακρισιμότητα (Indistinguishability)

Οντότητα (challenger - αναπαριστά το κρυπτοσύστημα)

Παίγνιο Μη Διακρισιμότητας μεταξύ των  $\mathcal{A}$ ,  $\mathcal{C}$



- Ανταλλαγή Μηνυμάτων μεταξύ  $\mathcal{A}$ ,  $\mathcal{C}$
- $\mathcal{A}$  Παράγει δύο μηνύματα  $m_0, m_1$
- $\mathcal{C}$ : Διαλέγει ένα τυχαίο bit  $b \leftarrow \$ \{0, 1\}$
- $\mathcal{C}$ : Παράγει και απαντά με το  $c_b = \text{Enc}(m_b)$
- $\mathcal{A}$  Μαντεύει ένα bit  $b'$
- Κερδίζει αν μαντέψει την επιλογή του  $\mathcal{C}$

## Μη Διακρισιμότητα (Indistinguishability) - (2)

Δηλαδή:

$$IND - Game(\mathcal{A}) = \begin{cases} 1, b' = b \\ 0, \text{αλλιώς} \end{cases}$$

**Πλεονέκτημα**

$$\text{Adv}_{IND}^{\mathcal{A}}(\lambda) = |\Pr[IND - Game(\mathcal{A}) = 1] - \frac{1}{2}|$$

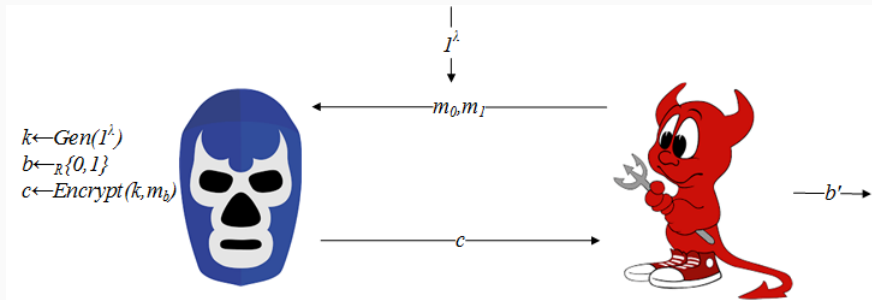
**Ορισμός**

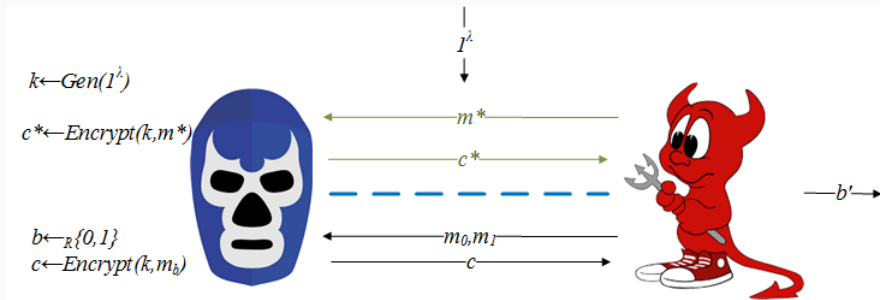
Ένα κρυπτοσύστημα διαθέτει την ιδιότητα της μη διακρισιμότητας όταν  $\forall$  PPT  $\mathcal{A}$ :

$$\text{Adv}_{IND}^{\mathcal{A}}(\lambda) = \text{negl}(\lambda)$$

**Θεώρημα**

Σημασιολογική Ασφάλεια  $\Leftrightarrow$  Μη-Διακρισιμότητα



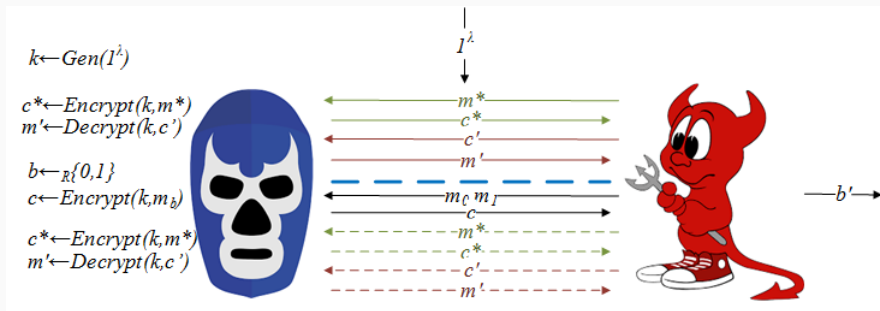


## Θεώρημα

Ένα κρυπτοσύστημα με ντετερμινιστικό αλγόριθμο κρυπτογράφησης δεν μπορεί να έχει την ιδιότητα IND-CPA.

Απόδειξη

- Ο  $\mathcal{A}$  θέτει  $m^* = m_0$  και λαμβάνει την κρυπτογράφηση  $c^*$
- Η απάντηση του είναι  $b' = \begin{cases} 0, c^* = c \\ 1, \text{αλλιώς} \end{cases}$
- Ο  $\mathcal{A}$  κερδίζει πάντα  $\Pr[\text{IND} - \text{CPA}(\mathcal{A}) = 1] = 1$



- Παραλλαγή IND-CCA2: Επιτρέπεται χρήση του μαντείου αποκρυπτογράφησης μετά το  $c$  (adaptive IND-CCA)
- Παραλλαγή IND-CCA1: αλλιώς ( $\mathcal{A}$  έχει μάθει ανεξάρτητες απο-κρυπτογραφήσεις)
- Στο παίγνιο IND-CCA2 ο  $\mathcal{A}$  δεν μπορεί να ρωτήσει τον  $C$  για την αποκρυπτογράφηση του  $c$
- Μπορεί όμως να:
  - Μετατρέψει το  $c$  σε  $\hat{c}$
  - Ζητήσει την αποκρυπτογράφηση του  $\hat{c}$  σε  $\hat{m}$
  - Να μετατρέψει το  $\hat{m}$  σε  $m$ , κερδίζοντας με πιθανότητα 1



Χειρισμός κρυπτοκειμένων χωρίς αποκρυπτογράφηση

## **Malleable (εύπλαστο) Κρυπτοσύστημα**

Επιτρέπει στον  $\mathcal{A}$  να φτιάξει, γνωρίζοντας μόνο το κρυπτοκείμενο  $c = \text{Enc}(m)$ , ένα έγκυρο κρυπτοκείμενο  $c' = \text{Enc}(f(m))$ , για κάποια, συνήθως πολυωνυμικά αντιστρέψιμη, συνάρτηση  $f$  γνωστή σε αυτόν.

Κάποιες φορές είναι επιθυμητή και κάποιες όχι.

- Ομομορφικά Κρυπτοσυστήματα: Αποτίμηση μερικών πράξεων στα κρυπτοκείμενα (ηλ. ψηφοφορίες)
- Πλήρως Ομομορφικά Κρυπτοσυστήματα (Gentry 2010): Αποτίμηση οποιουδήποτε κυκλώματος στα κρυπτοκείμενα
- Δεν μπορούν να είναι IND-CCA2, ... αλλά είναι πολύ χρήσιμα

## **Σημαντική ιδιότητα**

Non-malleability  $\Leftrightarrow$  IND-CCA2

# Αποδείξεις Ασφάλειας

---

## Γενική Μορφή

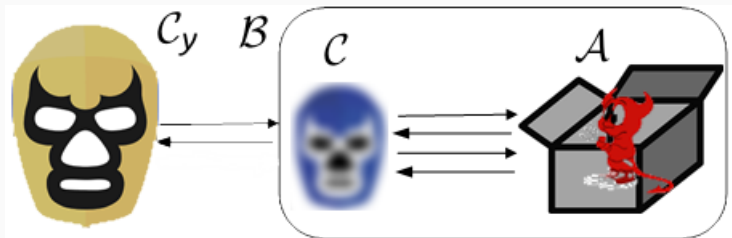
Αν ισχύει η υπόθεση  $\mathcal{V}$ , τότε το κρυπτοσύστημα  $\mathcal{CS}$  είναι ασφαλές (υπό συγκεκριμένο ορισμό).

## Αντιθετοαντιστροφή

Αν το  $\mathcal{CS}$  ΔΕΝ είναι ασφαλές (υπό συγκεκριμένο ορισμό), τότε δεν ισχύει η  $\mathcal{V}$ .

$\mathcal{V}$ : Δυσκολία παραγοντοποίησης, δυσκολία εύρεσης διακριτού λογαρίθμου κλπ.

- $\mathcal{CS}$  μη ασφαλές  $\Rightarrow \exists$  PPT  $\mathcal{A}$  ο οποίος παραβιάζει τον ορισμό ασφάλειας
- Κατασκευάζουμε PPT αλγόριθμο  $\mathcal{B}$ , ο οποίος αλληλεπιδρά με τον  $\mathcal{C}_Y$  ο οποίος προσπαθεί να 'υπερασπιστεί' την  $Y$
- Ο  $\mathcal{B}$  για να καταρρίψει την  $Y$  χρησιμοποιεί εσωτερικά σαν υπορουτίνα τον  $\mathcal{A}$  (black box access) παριστάνοντας τον  $\mathcal{C}$  στο παίγνιο μη διακρισιμότητας του  $\mathcal{CS}$



## Κανόνες Ορθότητας

- Προσομοίωση: Ο  $\mathcal{A}$  δεν θα πρέπει να ξεχωρίζει τον challenger του  $\mathcal{B}$  από τον κανονικό challenger.
- Πιθανότητα επιτυχίας: Αν ο  $\mathcal{A}$  έχει μη αμελητέα πιθανότητα επιτυχίας τότε και ο  $\mathcal{B}$  θα πρέπει να έχει μη αμελητέα πιθανότητα
- Πολυπλοκότητα: Ο  $\mathcal{B}$  θα πρέπει να είναι PPT. Αυτό πρακτικά σημαίνει ότι όποια επιπλέον εσωτερική επεξεργασία πρέπει να είναι πολυωνυμική
- Πρέπει να είναι όσο πιο tight γίνεται ( $t_{\mathcal{B}} \approx t_{\mathcal{A}}$  και  $\epsilon_{\mathcal{B}} \approx \epsilon_{\mathcal{A}}$ )

## Κρυπτογραφικές Αναγωγές

- Παρέχουν σχετικές εγγυήσεις (Δύσκολο Πρόβλημα, Μοντέλο Ασφάλειας)
- Δίνουν ευκαιρία να ορίσουμε καλύτερα το κρυπτοσύστημα/πρωτόκολλο
- Πρακτική Χρησιμότητα: Ρύθμιση Παραμέτρου Ασφάλειας
- Συγκέντρωση Κρυπταναλυτικών Προσπαθειών στο Πρόβλημα Αναγωγής και όχι σε κάθε κρυπτοσύστημα ξεχωριστά
- Πιο σημαντικές όσο πιο πολύπλοκο γίνεται το πρωτόκολλο
- Αποδεικνύουν την ασφάλεια του μοντέλου, αλλά:
  - Πόσο αναπαριστά το μοντέλο την πραγματικότητα περίπτωση KRACK attack on WPA2
  - Δεν σημαίνει ότι οποιαδήποτε υλοποίηση θα είναι ασφαλής

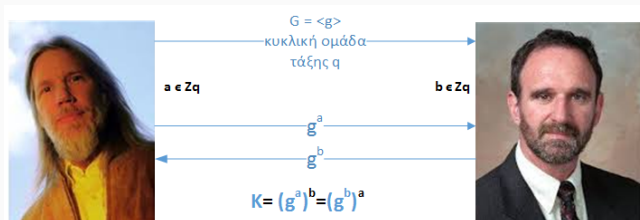
# Ανταλλαγή Κλειδιού Diffie Hellman

---



# Το πρωτόκολλο DHKE

Αντί για Alice και Bob...



Πρωτόκολλο Δημιουργίας Κλειδιού

**Απαιτήσεις:**

Συνήθως:  $\mathbb{G}$  υποομάδα τάξης πρώτου του  $\mathbb{Z}_p^*$  (με  $p$  πρώτο) ή  
ελλειπτικές καμπύλες

Εφαρμογές: SSL, TLS, IPSEC

## DLP - Το πρόβλημα του Διακριτού Λογάριθμου

Δίνεται μια κυκλική ομάδα  $\mathbb{G} = \langle g \rangle$  τάξης  $q$  και ένα τυχαίο στοιχείο  $y \in \mathbb{G}$

Να υπολογιστεί  $x \in \mathbb{Z}_q$  ώστε  $g^x = y$   
δηλ. το  $\log_g y \in \mathbb{Z}_q$

Αγνοούμε δεδομένα στο πρωτόκολλο DHKE

## CDHP - Το υπολογιστικό πρόβλημα Diffie Hellman

Δίνεται μια κυκλική ομάδα  $\mathbb{G} = \langle g \rangle$ , δύο στοιχεία

$$y_1 = g^{x_1}, y_2 = g^{x_2}$$

Να υπολογιστεί το  $g^{x_1 \cdot x_2}$

Μπορούμε να δοκιμάζουμε στοιχεία

## DDHP - Το πρόβλημα απόφασης Diffie Hellman

Δίνεται μια κυκλική ομάδα  $\mathbb{G} = \langle g \rangle$ , δύο στοιχεία

$y_1 = g^{x_1}, y_2 = g^{x_2}$  και κάποιο  $y \in \mathbb{G}$

Να εξεταστεί αν  $y = g^{x_1 \cdot x_2}$

ή ισοδύναμα

## DDHP - Το πρόβλημα απόφασης Diffie Hellman

Δίνεται μια κυκλική ομάδα  $\mathbb{G} = \langle g \rangle$ , δύο στοιχεία

$y_1 = g^{x_1}, y_2 = g^{x_2}$  και κάποιο  $y \in \mathbb{G}$

Μπορούμε να ξεχωρίσουμε τις τριάδες  $(g^{x_1}, g^{x_2}, g^{x_1 x_2})$  και  $(g^{x_1}, g^{x_2}, y)$ ;

## $CDHP \leq DLP$

Αν μπορούμε να λύσουμε το  $DLP$ , τότε μπορούμε να υπολογίζουμε τα  $x_1, x_2$  από τα  $y_1, y_2$  και στην συνέχεια το  $g^{x_1 \cdot x_2}$

## $DDHP \leq CDHP$

Αν μπορούμε να λύσουμε το  $CDHP$ , υπολογίζουμε το  $g^{x_1 \cdot x_2}$  και ελέγχουμε ισότητα με το  $y$

Δηλαδή:  $DDHP \leq CDHP \leq DLP$

Δεν γνωρίζουμε αν ισχύει η αντίστροφη σειρά - ισοδυναμία

**Όμως:** Υπάρχουν ομάδες όπου το  $DDHP$  έχει αποδειχθεί εύκολο, ενώ  $CDHP$  δεν έχει αποδειχθεί εύκολο

**Μάλλον:**  $DDHP < CDHP$

# DDH σε μορφή παιγνίου μη διακρισιμότητας

Κοινή είσοδος: παράμετρος ασφάλειας  $\lambda$ .

Λειτουργίες  $\mathcal{C}$

- Παραγωγή:  $\mathbb{G} = \langle g \rangle$  τάξης πρώτου  $q$ .
- Επιλογή  $x_1, x_2 \in \mathbb{Z}_q, y \leftarrow \$ \mathbb{G}$
- Υπολογισμός  $g^{x_1}, g^{x_2}, g^{x_1 x_2}$
- Επιλογή τυχαίου bit  $b \in \{0, 1\}$
- Αν  $b = 0$  τότε αποστολή  $\mathbb{G}, g^{x_1}, g^{x_2}, y' = g^{x_1 x_2}$  στον  $\mathcal{A}$
- Αν  $b = 1$  τότε αποστολή  $\mathbb{G}, g^{x_1}, g^{x_2}, y' = y$  στον  $\mathcal{A}$

Ο  $\mathcal{A}$  υπολογίζει  $b'$ .

Αν  $b' \neq b$  τότε το αποτέλεσμα του παιχνιδιού είναι **Failure**, αλλιώς **Success**

Πλεονέκτημα  $\mathcal{A}$

$$\text{Adv}_{\mathcal{A}}^{\text{ddh}}(\lambda) = |\Pr[\mathcal{A}(\mathbb{G}, g^{x_1}, g^{x_2}, g^{x_1 x_2}) = 1] - \Pr[\mathcal{A}(\mathbb{G}, g^{x_1}, g^{x_2}, y) = 1]|$$

Η υπόθεση DDH ισχύει αν  $\forall$  PPT  $\mathcal{A}$ :  $\text{Adv}_{\mathcal{A}}^{\text{ddh}}(\lambda) \leq \text{negl}(\lambda)$

## Διαίσθηση

Ο  $\mathcal{A}$  δεν μπορεί να διακρίνει το κλειδί από ένα τυχαίο στοιχείο της ομάδας στην οποία ανήκει

## Ισοδύναμα

Ο  $\mathcal{A}$  δεν αποκτά καμία χρήσιμη πληροφορία για το κλειδί που δημιουργείται.

Μοντέλο ασφάλειας: **παθητικός αντίπαλος**

# Παιχνίδι ανταλλαγής κλειδιού $KEG_{\mathcal{A},\Pi}(\lambda)$

Κοινή είσοδος:  $\lambda$ . Λειτουργίες  $\mathcal{C}$ :

- Δημιουργεί ομάδα  $\mathbb{G}$
- Εκτελεί το πρωτόκολλο  $\Pi(1^\lambda)$
- Παράγεται:  $(\tau, k)$ 
  - $\tau$  transcript: Τα μηνύματα που ανταλλάσσονται (δημόσια)
  - $k$ : Το κλειδί που παράγεται
- Επιλογή τυχαίου  $b \in \{0, 1\}$
- Αν  $b = 1$  επιλογή τυχαίου  $k'$  και αποστολή  $(\tau, k')$  στον  $\mathcal{A}$
- Αν  $b = 0$  αποστολή  $(\tau, k)$  στον  $\mathcal{A}$

Ο  $\mathcal{A}$  υπολογίζει  $b'$ . Αν  $b' \neq b$  τότε το αποτέλεσμα του παιχνιδιού είναι *Failure* (ήττα  $\mathcal{A}$ ), αλλιώς *Success* (νίκη  $\mathcal{A}$ )



Πλεονέκτημα  $\mathcal{A}$ :

$$\text{Adv}_{\mathcal{A}, \Pi}^{\text{keg}}(\lambda) = |\Pr[\text{KEG}_{\mathcal{A}, \Pi}(\lambda) = \text{Success}] - \frac{1}{2}|$$

Ένα πρωτόκολλο ανταλλαγής κλειδιού  $\Pi$  είναι ασφαλές, αν κάθε PPT παθητικός αντίπαλος  $\mathcal{A}$  έχει αμελητέο πλεονέκτημα ως προς την παράμετρο ασφάλειας να επιτύχει στο KEG

$$\text{Adv}_{\mathcal{A}, \Pi}^{\text{keg}}(\lambda) \leq \text{negl}(\lambda)$$

Δυσκολία DLP, CDHP αναγκαίες, αλλά όχι ικανές συνθήκες.

Αν το DDHP είναι δύσκολο, τότε το πρωτόκολλο είναι ασφαλές (απέναντι σε παθητικό αντίπαλο)

**Απόδειξη - Σχεδιάγραμμα** DHKE μη ασφαλές:  $\exists \mathcal{A}$  ώστε

$$\text{Adv}_{\mathcal{A}, \text{DHKE}}^{\text{key}}(\lambda) > \text{negl}(\lambda)$$

Θα κατασκευάσουμε αντίπαλο PPT  $\mathcal{B}$  ως προς την υπόθεση  $\text{DDH}$ :

- Όταν λάβει το μήνυμα από τον  $\mathcal{C}_{\text{DDH}}$  το προωθεί στον  $\mathcal{A}$
- Μορφή μηνύματος  $(\tau, k') = ((\mathbb{G}, g^{x_1}, g^{x_2}), y')$
- Όταν ο  $\mathcal{A}$  απαντήσει, προωθεί το  $b'$ .

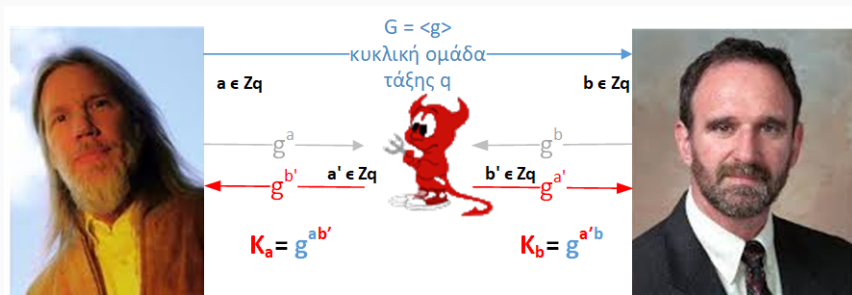
## Απόδειξη ασφάλειας DHKE (2)

$$\begin{aligned} & \Pr[KEG_{\mathcal{A}, DHKE}(\lambda) = \textit{Success}] \\ &= \frac{1}{2} \Pr[KEG_{\mathcal{A}, DHKE}(\lambda) = \textit{Success} | b = 1] + \frac{1}{2} \Pr[KEG_{\mathcal{A}, DHKE}(\lambda) = \textit{Success} | b = 0] \\ &= \frac{1}{2} \Pr[\mathcal{B}(\mathbb{G}, g^{x_1}, g^{x_2}, y) = 1] + \frac{1}{2} \Pr[\mathcal{B}(\mathbb{G}, g^{x_1}, g^{x_2}, g^{x_1 x_2}) = 0] \\ &= \frac{1}{2} \Pr[\mathcal{B}(\mathbb{G}, g^{x_1}, g^{x_2}, y) = 1] + \frac{1}{2} (1 - \Pr[\mathcal{B}(\mathbb{G}, g^{x_1}, g^{x_2}, g^{x_1 x_2}) = 1]) \\ &= \frac{1}{2} + \frac{1}{2} (\Pr[\mathcal{B}(\mathbb{G}, g^{x_1}, g^{x_2}, y) = 1] - \Pr[\mathcal{B}(\mathbb{G}, g^{x_1}, g^{x_2}, g^{x_1 x_2}) = 1]) \\ &\leq \frac{1}{2} + \frac{1}{2} |\Pr[\mathcal{B}(\mathbb{G}, g^{x_1}, g^{x_2}, y) = 1] - \Pr[\mathcal{B}(\mathbb{G}, g^{x_1}, g^{x_2}, g^{x_1 x_2}) = 1]| \\ &\leq \frac{1}{2} + \frac{1}{2} \text{Adv}_{\mathcal{B}}^{\text{ddh}}(\lambda) \leq \frac{1}{2} + \frac{1}{2} \text{negl}(\lambda) \end{aligned}$$

ΑΤΟΠΟ

# Ενεργοί Αντίπαλοι

## Η σημασία του μοντέλου ασφάλειας - Man In The Middle Attacks



Πώς είμαι σίγουρος ότι μιλάω με αυτόν που νομίζω ότι μιλάω;  
Λύση: ψηφιακές υπογραφές - ψηφιακό πιστοποιητικό (εγγύηση  
'έμπιστου' τρίτου)

## Superfish (02/2015)

- Προεγκατεστημένο λογισμικό Visual Discovery: προσπάθεια για εμφάνιση διαφημίσεων όχι με βάση κείμενο αλλά με βάση εικόνες
- Παρακολούθηση δικτυακής κίνησης και μέσω https
- Λογισμικό proxy που λειτουργεί ως MiTM
- Εγκατάσταση και (self signed) ψηφιακού πιστοποιητικού

Και άλλες ανάλογες περιπτώσεις: πχ. **DELL - 10/2015**