# 1 Κρυπτογράφηση Δημοσίου Κλειδιού

Στην Ενότητα **??** ορίσαμε το συμμετρικό κρυπτοσυστήματα σαν αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης που μοιράζονται κοινό πεδίο ορισμού του κλειδιού. Σε ένα μή συμμετρικό κρυπτοσύστημα υπάρχουν δύο διακριτά πεδία ορισμού κλειδιών.

**Definition 1.0.1.** Ένα ***μη συμμετρικό κρυπτοσύστημα (asymmetric cryptosystem)*** αποτελείται από τα εξής στοιχεία.

- Ένα πεδίο ορισμού απλού μύνημάτων $\mathcal{M} = \{\mathcal{M}_\lambda\}_{\lambda\in\mathbb{N}}$
- Ένα πεδίο ορισμού κρυπτογραφημένων μηνυμάτων $\mathcal{C} = \{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$
- Ένα πεδίο ορισμού δημοσίου κλειδιού$\mathcal{P} = \{\mathcal{P}_\lambda\}_{\lambda\in\mathbb{N}}$ και μυστικού κλειδιού $\mathcal{S} = \{\mathcal{S}_\lambda\}_{\lambda\in\mathbb{N}}$
- Έναν αποδοτικό αλγόριθμο κρυπτογράφησης $\mathcal{E}\colon \mathcal{K}_p \times \mathcal{M} \longrightarrow \mathcal{C}$ που ικνοποιεί $\lambda$: $\mathcal{E}(\mathcal{P}_\lambda \times \mathcal{M}_\lambda) \subseteq \mathcal{C}_\lambda$
- Έναν αποδοτικό αλγόριθμο αποκρυπτογράφησης $\mathcal{D}\colon \mathcal{K}_s \times \mathcal{C} \longrightarrow \mathcal{M}$ που ικνοποιεί $\lambda$: $\mathcal{D}(\mathcal{S}_\lambda \times \mathcal{C}_\lambda) \subseteq \mathcal{M}_\lambda$
- Έναν αποδοτικό αλγόριθμο παραγωγης κλειδιού $\mathcal{G}\colon \mathbb{N} \longrightarrow \mathcal{P} \times \mathcal{S}$ που ικνοποιεί $\lambda$: $\mathcal{G}(1^\lambda)$.

Επιπλέον, ένα μη συμμετρικό κρυπτοσύστημα πρέπει να ικνοποιεί την ***ιδιότητα της ακρίβεας*** δηλαδή

- για κάθε $M \in \mathcal{M}$ και $\langle pk, sk\rangle \in \mathcal{K}_p \times \mathcal{K}_s$, ισχύει $\mathcal{D}(sk, \mathcal{E}(pk, M)) = M$.

## 1.1 Ασφάλεια AON-CPA

Το AON-CPA είναι ένα από τα ασθενέστερα μοντέλα ασφαλείας για την μη συμμετρική κρυπτογράφηση δημοσίου κλειδιού. Το AON αναφέρεται στο στόχο του αντιπάλου "all-or-nothing", όπου ο επιτιθέμενος επιχειρεί να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο για να αποκτήσει το απλό μύνημα. Το CPA αντιστοιχεί στην ικανότητα του αντιπάλου για μια επίθεση επιλεγμένου απλού μηνύματος. Σε μια επίθεση επιλεγμένου απλού μηνύματος υποθέτουμε ότι ο επιτιθέμενος μπορεί να αποκτήσει κρυπτογραφημένα μηνύματα της επιλογής του. Χρησιμοποιώντας τα ζεύγη μηνύματος κρυπτογραφημένου και απλού, μπορεί να εξασθενήσει το σύστημα και να πειραματιστεί με τον μηχανισμό κρυπτογράφησης δημοσίου κλειδιού.

**Definition 1.1.1.** Ένα σύστημα κρυπτογράφησης δημοσίου κλειδιού είναι AON-CPA ασφαλές αν το

$$\text{Prob}[\mathcal{A}(pk, c) = M\colon \langle pk, sk\rangle \leftarrow \mathcal{G}(1^\lambda),\ c \leftarrow \mathcal{E}(pk, M),\ M \xleftarrow{\text{r}} \mathcal{M}_\lambda]$$

είναι αμελητέο στο $\lambda$ για κάθε αντίπαλο $\mathcal{A}$.

Το μοντέλο αυτό είναι ασθενές επειδή υποθέτει πως ο αντίπαλος θέλει ανακτήσει ολόκληρο το κείμενο. Επιπλέον το κείμενο αυτό είναι τυχαίο. Το AON-CPA δεν απαγορεύει στον επιτιθέμενο μερική πληροφορία.

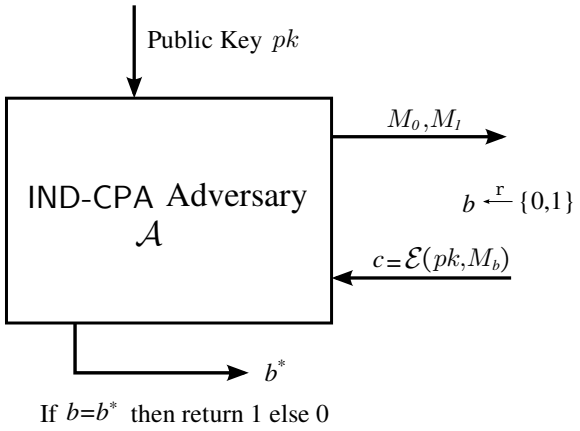
## 1.2 Ασφάλεια IND-CPA

Ένα ισχυρότερο μοντέλο ασφαλίας είναι το IND-CPA. Ένας αντίπαλο επιτρέπεται να υποβάλει δύο απλά μηνύματα στο μαντείο κρυπτογράφησης, το οποίο επιστρέφει το κρυπτογράφημα ενός από τα δύο τυχαία. Τότε ο αντίπαλος μπορεί να ξεχωρήσει ποιο από τα δύο μηνύματα του επιστράφηκε. Ο στόχος του αντιπάλου IND δηλώνει την μη διαχωρισιμότητα (indistinguishablility). Αυτό μπορεί να μοντελοποιηθεί ως το ακόλουθο παιχνίδι, $\text{Game}^{\mathcal{A}}_{\mathsf{IND\text{-}CPA}}(1^\lambda)$.

1. $\langle pk, sk\rangle \leftarrow \mathcal{G}(1^\lambda)$
2. $\langle \mathsf{aux}, M_0, M_1\rangle \leftarrow \mathcal{A}(\mathsf{play}, pk)$ for $M_0 \neq M_1$

3. $b \xleftarrow{r} \{0,1\}$
4. $c \leftarrow \mathcal{E}(pk, M_b)$
5. $b^* \leftarrow \mathcal{A}(\mathsf{guess}, \mathsf{aux}, c)$
6. If $b = b^*$ output 1; otherwise 0.

Το σχήμα 1 παρουσιάζει αυτό το παιχνίδι.




Σχήμα 1: Η επίθεση IND-CPA . Αν $b = b^*$, λέμε πως ο αντίπαλος κερδίζει το παιχνίδι.

**Definition 1.2.1.** Ένα σύστημα κρυπτογραφησης δημοσίου κλειδιού είναι IND-CPA ασφαλές αν για κάθε PPT αντίπαλο $\mathcal{A}$,

$$\text{Prob}[\text{Game}^{\mathcal{A}}_{\mathsf{IND\text{-}CPA}}(1^\lambda) = 1] \leq \frac{1}{2} + \text{negl}(\lambda).$$

**Example.** Το σχήμα κρυπτογράφησης RSA οπως παρουσιάζεται κάτω, δεν είναι IND-CPA ασφαλές. Στην πραγματικότητα, όλα τα ντετερμινιστικά κρυπτοσυστήματα δημοσίου κλειδιού αποτυγχανουν στο μοντέλο ασφαλείας IND-CPA.

$\mathcal{G}(1^\lambda)$ : $\langle pk, sk\rangle \leftarrow \mathcal{G}(1^\lambda)$
$pk = (n, e)$
$sk = d$

$\mathcal{E}(pk, M)$ : $M \in \{0,1\}^\lambda$
υπολογίζουμε το $c = M^e \bmod n$
επιστρέφουμε το $c$

$\mathcal{D}(sk, c)$ : $M = c^d \bmod n$
επιστρέφουμε $M$

Η κρυπτογράφηση RSA αποτυγχάνει στο μοντέλο ασφαλείας IND-CPA επειδή ένα φιξαρισμένο μήνυμα κρυπτογραφειται πάντα με το ιδιο κρυπτογράφημα. Αφού ο αντίπαλος έχει πρόσβαση στον αλγόριθμο κρυπτογράφησης έχει την δυνατότητα να βλέπει κρυπτογραφήματα των μηνυμάτων του ανεξάρτητα από το σύστημα. Όταν το μαντείο επιστρέφει ένα από τα κρυπτογραφημένα μυνήματα, ο αντίπαλος μπορεί να αναφερθεί στους υπολογισμούς του για να προσδιορίσει πιο μύνημα του δόθηκε. Αυτό συνεπάγεται ότι ένα σχήμα για είναι ασφαλές στο μοντέλο IND-CPA θα πρέπει να είναι ένα πιθανοτικό πρωτόκολλο.

Μπορούμε να τροποποιήσουμε τη συνάρτηση RSA για να τη δούμε σαν ένα πιθανοτικό σχήμα.

$\mathcal{G}(1^\lambda)$ : $\langle pk, sk\rangle \leftarrow \mathcal{G}(1^\lambda)$
$pk = (n, e)$
$sk = d$

$\mathcal{E}(pk, M)$ : $M \in \{0,1\}^{\lambda-\lambda_0}$
$r \in \{0,1\}^{\lambda_0}$
$M' = \mathsf{bit2integer}(r\|M)$
υπολόγίζουμε το $c = M'^e \bmod n$
επιστρέφουμε το $c$

$\mathcal{D}(sk, c)$ : $M' = c^d \bmod n$
$(r\|M) = \mathsf{integer2bit}(M')$
επιστρέφουμε το $M$

Εισάγοντας την τυχαιότητα $r$, το πρωτόκολλο δεν κρυπτογραφεί ένα μήνυμα με τον ίδιο τρόπο κάθε φορά. Αυτή η τροποποίηση παρακάμπτει το πρόβλημα του ντετερμινιστικού μοντέλου. Ωστόσο είναι ακόμα αβέβαιο αν αυτή η πιθανοτική εκδοχή ευάλωτη στην επίθεση IND-CPA.

## 1.3 Κρυπτογράφηση ElGamal

Η κρυπτογράφηση ElGamal είναι ένα ς αλγόριθμος κρυπτογράφησης μη συμμετρικού κλειδιού που είναι αποδεδειγμένα ασφαλής στο μοντέλο IND-CPA. Βασίζεται στην ανταλλαγή κλειδιού Diffie-Hellman, οπότε ορίζεται σε μια κυκλική ομάδα $\langle g\rangle$ ενός πρώτου τάξης $m$.

$\mathcal{G}(1^\lambda)$ : $\langle pk, sk\rangle \leftarrow \mathcal{G}(1^\lambda)$
$x \xleftarrow{r} \mathbb{Z}_m, h = g^x \bmod p$
$pk = \langle\langle p, m, g\rangle, h\rangle$
$sk = x$

$\mathcal{E}(pk, M)$ : $M \in \langle g\rangle$
$r \xleftarrow{r} \mathbb{Z}_m$
υπολογίζουμε τα $G = g^r \bmod p$, $H = h^r M \bmod p$
επιστρέφουμε το $\langle G, H\rangle$

$\mathcal{D}(sk, G, H)$ : υπολογίζουμε το $M = H/G^x \bmod p$
επιστρέφουμε το $M$

Μπορούμε να αποδείξουμε ότι αυτό είναι ασφαλές στο IND-CPA μοντέλο υπό την υπόθεση DDH. Δεδομένου ενός PPT IND-CPA αντιπάλου $\mathcal{B}$ τέτοιου ώστε

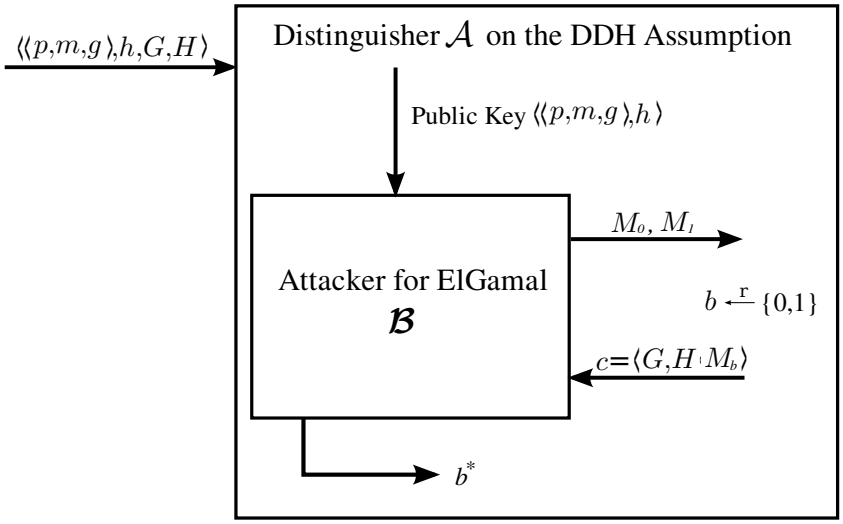
$$\text{Prob}[\text{Game}^{\mathcal{B}}_{\mathsf{IND\text{-}CPA}}(1^\lambda) = 1] \geq \frac{1}{2} + \alpha$$

για μη αμελητεα $\alpha$, θα κατασκευάσουμε έναν PPT αλγόριθμο $\mathcal{A}$ που μπορεί να διαχωρήσει το σύνολο μεταβλητών DDH από ένα τυχαίο.
Αλγόριθμος $\mathcal{A}(\langle p, m, g\rangle, h, G, H)$:

1. $\langle \mathsf{aux}, M_0, M_1\rangle \leftarrow \mathcal{B}(\mathsf{play}, pk, h)$ όπου $pk = \langle p, m, g\rangle$
2. $b \xleftarrow{r} \{0,1\}$

3. $c \leftarrow \langle G, H \cdot M_b \rangle$
4. $b^* \leftarrow \mathcal{B}(\mathsf{guess}, \mathsf{aux}, c)$
5. If $b = b^*$ επιστρέφουμε 1, διαφορετικά 0.

Το σχήμα 2 παρουσιάζει πως ο $\mathcal{A}$ χρησιμοποιεί τον επιτιθέμενο $\mathcal{B}$ για να σπάσει την υπόθεση DDH.




Σχήμα 2: Αν κάποιος επιτιθέμενος $\mathcal{B}$ κωδικοποιηεί ένα μήνυμα στο ElGamal με μη αμεληταία πιθανότητα, μπορούμε να κατασκευάσουμε έναν PPT αλγόριθμο διαχώρησης $\mathcal{A}$ που σπάει την υπόθεση DDH. Αν $b = b^*$, ο $\mathcal{A}$ είναι επιτυχής.

Έστω $v = \langle \langle p, m, g \rangle, g^x, g^y, g^{xy} \rangle$ να είναι το σύνολο μεταβλητώνDDH . Τότε ισχύει

$$\Pr_{v \leftarrow \langle \langle p,m,g \rangle, g^x, g^y, g^{xy} \rangle}[\mathcal{A}(v) = 1] = \text{Prob}[\text{Game}^{\mathcal{B}}_{\mathsf{IND\text{-}CPA}}(1^\lambda) = 1] \geq \frac{1}{2} + \alpha.$$

Αν το $v$ είναι ένα τυχαίο σύνολο, τότε $v = \langle \langle p, m, g \rangle, g^x, g^y, g^z \rangle$. Για κάθε $w \in \langle g \rangle$, μπορούμε να βρούμε ένα μοναδικό $z$ τέτοιο ώστε $w = g^z M_b$ or $z = \log_g(w/M_b)$. Γι' αυτό καμία πληροοφορία για το $b$ περνάει στον αντίπαλο. Αφού το $b^*$ είναι ανεξάρτητο της επιλογής του $b$, η πιθανότητα ότι το $b = b^*$ είναι $1/2$.

$$\Pr_{v \leftarrow \langle \langle p,m,g \rangle, g^x, g^y, g^z \rangle}[\mathcal{A}(v) = 1] = \text{Prob}[b = b^*] = \frac{1}{2}.$$

Βασιζόμενοι σε αυτο, καταλήγουμε πως

$$\left| \Pr_{v \leftarrow \langle \langle p,m,g \rangle, g^x, g^y, g^{xy} \rangle}[\mathcal{A}(v) = 1] \; - \Pr_{v \leftarrow \langle \langle p,m,g \rangle, g^x, g^y, g^z \rangle}[\mathcal{A}(v) = 1] \right| \geq \alpha.$$

Αφού το $\alpha$ είναι μη αμεληταίο, αυτό παραβιάζει την υπόθεση DDH όπως επιθυμούμε.

Notes by S. Pehlivanoglu, J. Todd, & H.S. Zhou