1 Εισαγωγή

Θα ξεκινήσουμε τη συζήτηση για τις βασικές αρχές τις κρυπτογραφίας με ένα απλό παράδειγμα.

1.1 Στρίψιμο νομίσματος μέσω τηλεφώνου

Φανταστείτε πως η Αλίκη και ο Βασίλης μιλάνε στο τηλέφωνο, όπου διαπραγματεύονται για το που θα βγούνε το απόγευμα. Επειδή δεν μπορούν να συμφωνήσουν, αποφασίζουν πως η τύχη θα αποφασίσει για αυτούς ως εξής. Η Αλίκη θα ρίξει ένα νόμισμα και ο Βασίλης θα διαλέξει τη νικητήρια πλευρά για την Αλίκη. Αν η Αλίκη νικήσει τότε θα διαλέξει αυτή για το που θα βγουν, ενώ διαφορετικά θα το κάνει ο Βασίλης.

Αν η Αλίκη και ο Βασίλης βρίσκονταν στο ίδιο μέρος δεν θα υπήρχε κανένα πρόβλημα. Στην περίπτωση μας όμως θα θέλαμε μια διαδικασία μέσω της συνομιλίας τους από το τηλέφωνο. Δύο προβληματικές λύσεις από μεριά εγκυρότητας είναι οι εξής.

Λύση 1: Η Αλίκη ρίχνει το νόμισμα και ενημερώνει τον Βασίλη για το αποτέλεσμα. Στην συνέχεια ο Βασίλης διαλέγει την νικητήρια πλευρά. Το πρόβλημα αυτής της προσέγγισης είναι πως ο Βασίλης μπορεί να διαλέξει την πλευρά έτσι ώστε πάντα να χάνει η Αλίκη.

Λύση 2: Η Αλίκη ρίχνει το νόμισμα και δεν ενημερώνει τον Βασίλη για το αποτέλεσμα. Στην συνέχεια ο Βασίλης διαλέγει την νικητήρια πλευρά. Το πρόβλημα αυτής της προσέγγισης είναι πως η Αλίκη μπορεί να προσποιηθεί πως το αποτέλεσμα της ρίψης ήταν αυτό που της δίνει την νίκη.

Τα προβλήματα των παραπάνω λύσεων μπορούν να ξεπεραστούν με τη χρήση `` πηγαδιών".

Λύση 3: Η Αλίκη ρίχνει το νόμισμα σε ένα ``πηγάδι". Στην συνέχεια τηλεφωνεί τον Βασίλη και τον ενημερώνει για το αποτέλεσμα της ρίψης. Τώρα ο Ο Βασίλης πηγαίνει στο ``πηγάδι" για να ελέγξει το αποτέλεσμα.

Το ``πηγάδι" στην Λύση 3 αποτελεί ***δέσμευση (commitment)*** για την Αλίκη, διότι την αποτρέπει από το να αλλάξει το αποτέλεσμα. Επιπλέον η Αλίκη ενημερώνοντας απλά για την τοποθεσία του ``πηγαδιού" δεν δίνει κάποια πληροφορία στον Βασίλη για το αποτέλεσμα της ρίψης. Παρατηρείστε πως η πρόσθεση του ``πηγαδιού" τους απαλλάσσει από την ταυτόχρονη φυσική παρουσία.

Λόγω έλλειψης διαθεσιμότητας ``πηγαδιών" όμως θα πρέπει να βρούμε μια διαφορετική τεχνική. Αναθέτουμε την τιμές 1 και 0 για το αποτελέσματα της ρίψης ``Κορώνα" και ``Γράμματα" αντίστοιχα.

Επιπλέον θεωρείστε την σχέση f που στέλνει το μηδέν και το ένα σε ένα σύνολο από αντικείμενα. Εδώ, η σχέση f αντικαθιστά το ``πηγάδι". Η διαδικασία ρίψης νομίσματος πραγματοποιείτε με από τα παρακάτω βήματα.

1. Η Αλίκη ρίχνει ένα νόμισμα και ανάλογα διαλέγει $a \in \{0, 1\}$. Υπολογίζει το $f(a)$.
2. Η Αλίκη στέλνει $y = f(a)$ στον Βασίλη.
3. Ο Βασίλης ρίχνει ένα νόμισμα και ανάλογα διαλέγει $b \in \{0, 1\}$. Στέλνει το b στην Αλίκη.
4. Αν $a = b$, η Αλίκη νικάει.
5. Η Αλίκη αποκαλύπτει το a και ο Βασίλης ελέγχει αν το y είναι η σωστή δέσμευση για το a, δηλαδή αν $y = f(a)$.
6. Ο Βασίλης ελέγχει αν $a = b$ ώστε να συμπεράνει το αποτέλεσμα νίκης ή όχι της Αλίκης

Για να αποτελεί το προηγούμενο πρωτόκολλο επιτυχής λύση πρέπει η f να ικανοποιεί τα παρακάτω.

1. ***Ιδιότητα κρυψίματος (Hiding property)***: Διασφαλίζει πως η f δεν δίνει κάποια πληροφορία για το a. Δηλαδή δεδομένου του $f(a)$ δεν αντλούμε καμία πληροφορία για το a.
2. Η ***Ιδιότητα δέσμευσης (Binding property)***: διασφαλίζει πως είναι αδύνατον για την Αλίκη να αλλάξει την τιμή του a αφού υποβάλει την δέσμευση $y = f(a)$. Δηλαδή η Αλίκη να μην μπορεί να πείσει τον Βασίλη πως $y = f(a')$, όπου $a' \neq a$.

Η ικανοποίηση μιας εκ των δύο συνθηκών είναι τετριμμένη όχι όμως και των δύο ταυτόχρονα όπως θα δούμε. Π.χ. έστω f η σταθερή συνάρτηση, δηλαδή $f(x) = c$, για κάποια σταθερά c. Η f ικανοποιεί την ιδιότητα κρυψίματος γιατί δεδομένου του $f(x)$ δεν λαμβάνουμε καμία πληροφορία για το c. Όμως η f δεν ικανοποιεί την ιδιότητα δέσμευσης, αφού για οποιοδήποτε $a' \neq a$, ισχύει πως $f(a') = c$. Π.χ. έστω f η ταυτοτική συνάρτηση, δηλαδή $f(x) = x$ Η f ικανοποιεί την ιδιότητα δέσμευσης γιατί για κάθε $a' \neq a$ ισχύει πως $a' \neq f(a)$. Προς το παρόν όμως δεν θα μας απασχολήσει η υλοποίηση της συναρτήσεως f, γιατί θα θεωρήσουμε πως είναι ένα από τα στοιχεία που μας παρέχονται για την κατασκευή του πρωτοκόλλου.

Δεδομένης λοιπόν μιας f που ικανοποιεί τις παραπάνω συνθήκες αναλύουμε το πρωτόκολλο. Αναθέτουμε πάλι τις τιμές 1 και 0 για το τελικό αποτέλεσμα του πρωτοκόλλου, δηλαδή 1` αν νικά η Αλίκη (δηλαδή αν $a = 1$ και $b = 1$ ή αν $a = 0$ και $b = 0$) και 0 διαφορετικά (δηλαδή αν $a = 1$ και $b = 0$ ή $a = 0$ και $b = 1$). Παρατηρείστε πως το πρωτόκολλο ουσιαστικά υλοποιεί την λογική πράξη $a \oplus b$ (αποκλειστικό ή - XOR). Συνεπώς μπορούμε εναλλακτικά να θεωρήσουμε πως το πρωτόκολλο στριψίματος νομίσματος στοχεύει στον υπολογισμό του XOR δύο τυχαίων δυαδικών μεταβλητών.

Αν και οι δύο μεριές το ακολουθήσουν πιστά, η πιθανοτική κατανομή του $a \oplus b$ είναι ομοιόμορφη και στις δύο πλευρές; επιπλέον και οι δύο μεριές καταλήγουν στο ίδιο αποτέλεσμα.

Εξετάζουμε τώρα την περίπτωση που ένας εκ των δύο δρα διαφορετικά από ότι καθορίζει το πρωτόκολλο. Τα δυνατά σενάρια που ενδεχομένως επηρεάζεται η ασφάλεια είναι τα εξής.

1. Μόλις λάβει το b στο βήμα 3, Η Αλίκη αντικαθιστά με a' το a έτσι ώστε $y = f(a')$.
2. Ο Βασίλης προσπαθεί να μαντέψει το a αφού λάβει το y και διαλέγει το b ανάλογα.
3. Μία από τις δυο πλευρές ρίχνει το νόμισμά της με μεροληπτικό τρόπο τέτοιο ώστε η πιθανότητα της ``Κορώνας" η των ``Γραμμάτων" να μην είναι $1/2$.

Αφού υποθέσαμε πως η f ικανοποιεί την ιδιότητα δέσμευσης, η Αλίκη μέσω του y είναι δεσμευμένη στο αρχικό a, αποτρέποντας την από το να ``κλέψει" στο σενάριο 1. Παρόμοια, στην δεύτερη περίπτωση ο Βασίλης δεν μπορεί αποτελεσματικά να μαντέψει το a εξαιτίας τις ιδιότητας του κρυψίματος. Για το τελευταίο σενάριο θα χρειαστούμε ορισμένους υπολογισμούς. Μια γενική αρχή στην κρυπτογραφία είναι πως δεν μας ενδιαφέρει η ποιότητα του αποτελέσματος για τους παίκτες που το παραβιάζουν. Συνεπώς, σκοπός μας είναι να δείξουμε πως η πλευρά που μένει πιστή στο πρωτόκολλο καταλήγει σε ένα αποτέλεσμα που είναι ομοιόμορφα κατανεμημένο στο $\{0, 1\}$. Έχουμε τέσσερις δυνατότητες.

1. Η Αλίκη διαλέγει το $a = 0$ με πιθανότητα α, Ο Βασίλης διαλέγει το $b = 0$ με πιθανότητα β, και το αποτέλεσμα είναι 1;
2. Η Αλίκη διαλέγει το $a = 0$ με πιθανότητα α, Ο Βασίλης διαλέγει το $b = 1$ με πιθανότητα $1 - \beta$, και το αποτέλεσμα είναι 0
3. Η Αλίκη διαλέγει το $a = 1$ με πιθανότητα $1 - \alpha$, Ο Βασίλης διαλέγει το $b = 0$ με πιθανότητα β, και το αποτέλεσμα είναι 0
4. Η Αλίκη διαλέγει το $a = 1$ με πιθανότητα $1 - \alpha$, Ο Βασίλης διαλέγει το $b = 1$ με πιθανότητα $1 - \beta$, και το αποτέλεσμα είναι 1

Συνεπώς έχουμε πως κέρδη[Γράμματα] $= \alpha\beta + (1 - \alpha)(1 - \beta) = 1 - \alpha - \beta + 2\alpha\beta$. Στην περίπτωση που και οι δύο πλευρές δεν είναι τίμιες, το πρωτόκολλο αναγκαστικά δεν θα λειτουργήσει σωστά. Όμως όπως αναφέραμε δεν υπάρχει τότε και απαίτηση από το αποτέλεσμα του.

Αν μία από τις δύο πλευρές είναι τίμια, δηλαδή, είτε α ή $\beta = 1/2$, τότε έχουμε πως κέρδη[Heads] $= 1/2$. Π.χ. αν $a = 1/2$, αντικαθιστώντας στην πάνω σχέση, βλέπουμε πως κέρδη[Heads] $= 1 - 1/2 - \beta + \beta = 1/2$, συνεπώς έχουμε ασφάλεια έναντι κακόβουλης συμπεριφοράς; η τίμια πλευρά καταλήγει σε ένα αποτέλεσμα με ομοιόμορφη κατανομή.

1.2 Επισκόπηση της Κρυπτογραφίας

Το προηγούμενο παράδειγμα σκιαγραφεί τα βασικά στάδια στην μελέτη της κρυπτογραφίας τα οποία και χαρακτηρίζουν τον τρόπο διδασκαλίας του μαθήματος και παρουσιάζονται ως εξής:

1. **Αναγνώριση σημαντικών κρυπτογραφικών προβλημάτων που χρειάζονται επίλυση.** Το προηγούμενο παράδειγμα, το πρόβλημα ρίψης ενός νομίσματος από δύο παίκτες που δεν είναι στον ίδιο χώρο, είναι ένα πολύ σημαντικό κρυπτογραφικό πρωτόκολλο με πάρα πολλές εφαρμογές στην κατασκευή ασφαλών συστημάτων.

2. **Τυπικός ορισμός της ασφάλειας και της ορθότητας.** Αφού αναγνώρισουμε ένα πρόβλημα πρέπει να ορίσουμε τι χρειάζεται να ικανοποιεί μια προτεινόμενη λύση ώστε να θεωρηθεί ότι λύνει το πρόβλημα. Αυτό περιλαμβάνει την ορθότητα (π.χ. στο προηγούμενο παράδειγμα το γεγονός ότι οι δύο παίκτες πρέπει να καταλήγουν με την ίδια έξοδο) καθώς και την ασφάλεια (π.χ. στο προηγούμενο παράδειγμα το γεγονός ότι έαν ένας από τους δύο παίκτες δεν ακολουθεί το πρωτόκολλο πιστά εξακολουθεί να μην μπορέι να επιρρεάσει την κατανομή της εξόδου του άλλου παίκτη).

3. **Σχεδιασμός λύσεων.** Οι λύσεις για τα κρυπτογραφικά προβλήματα παρουσιάζονται στη μορφή αλγορίθμων ή πρωτοκόλλων. Ο σχεδιασμός περιλαμβάνει και την εξέταση των ανεξαρτήτων δομικών συστατικών (η αρχών) πάνω στα οποία χτίζονται οι λύσεις. Συχνά είναι πιο εύκολο να σχεδιάσουμε ένα αλγοριθμό χρησιμοποιώντας δομικά στοιχεία τα οποία θα εξετάσουμε πως μπορούν να επιλυθούν ανεξάρτητα (π.χ. στο προηγούμενο παράδειγμα, θεωρήσαμε ότι η σχέση f λειτουργεί σαν ***σχήμα δέσμευσης bit (bit commitment scheme)***.

4. **Παροχή αποδείξεων ασφάλειας και ορθότητας**. Σε αυτήν την φάση παρουσιάζουμε μια σειρά από επιχείρηματα που έχουν στόχο να πείθεται ένας χρήστης ότι η προτεινόμενη λύση ικανοποιεί τον τυπικό ορισμό ασφάλειας και ορθότητας.

Πιο συγκεκριμένα το πρότυπο ``αποδείξιμης-ασφάλειας" (provable security) εστιάζει σε δύο σημεία:

1. Κατασκευή ενός τυπικού μοντέλου ασφαλείας και ορισμού της έννοιας πως μια κρυπτογραφική σχεδίαση είναι ασφαλής, και,

2. Δείχνοντας πως η ύπαρξη ενός αντιπάλου ικανού να ``σπάει" την κρυπτογραφική σχεδίαση αποτελεσματικά ισοδυναμεί με την ύπαρξη ενός αλγορίθμου που λύνει αποτελεσματικά ένα γνωστό ``υπολογιστικά δύσκολο" πρόβλημα.

Το δεύτερο σημείο εισάγει στην κρυπτογραφία έννοιες που έχουν χρησιμοποιηθεί στην ***υπολογιστική πολυπλοκότητα (computational complexity)***. Αυτός ο κλάδος της επιστήμης υπολογιστών στοχεύει στην απάντηση προβλημάτων όπως ``Πόσα βηματα είναι απαραίτητα για την επίλυση ενός προβλήματος;" ή ``Πόσος χώρος χρειάζεται για την εύρεση λύσης για ένα πρόβλημα;" Ένας από τους στόχους την υπολογιστικής πολυπλοκότητας είναι ο υπολογισμός του απαραίτητου χρόνου υπολογισμού εύρεσης λύσης για ένα πρόβλημα. Για παράδειγμα, ένα από τα θεμελιώδη ανοικτά ζητήματα της πληροφορικής και των μαθηματικών σχετίζει τις κλάσεις P και NP. Το P είναι το σύνολο των προβλημάτων που που μπορούν να λυθούν σε πολυωνυμικό χρόνο και το NP είναι η σύνολο των προβλημάτων για τα οποία μια υποψήφια λύση επαληθεύεται σε πολυωνυμικό χρόνο. Παρότι έχει γίνει ιδιαίτερα μεγάλη προσπάθεια για την κατανόηση των σχέσεων των παραπάνω κλάσεων, είναι ακόμη άγνωστο αν $P \neq NP$. Ωστόσο είναι γνωστό, πως μια απόδειξη ασφάλειας για ένα κρυπτοσύστημα συνεπάγεται $P \neq NP$. Για την κατανόηση του παραπάνω πρέπει να δούμε την NP-φύση της κρυπτογραφίας, δηλαδή πως τα μυστικά κλειδιά παίζουν το ρόλο μιας υποψήφιας λύσης σε ένα NP πρόβλημα που μπορεί να ορισθεί βάσει των δημόσιων παραμέτρων του κρυπτογραφικών συστήματος.

Το αντίστροφο των παραπάνω σχέσεων μεταξύ κρυπτογραφίας και του κλασσικού αντικειμένου της υπολογιστικής πολυπλοκότητας δεν ισχύει. Κλάσεις όπως P, NP έχουν οριστεί συνδυασμένες με την πολυπλοκότητα της χειρότερης περίπτωσης, δηλαδή πόσος χρόνος απαιτείται για την επίλυση του χειρότερου στιγμιότυπου. Για αυτό το λόγο το γεγονός $P \neq NP$ απο μόνο του δεν είναι αρκετό για κρυπτογραφικές αποδείξεις

ασφαλείας. Τέτοιες εφαρμογές απαιτούν δυσκολία μέσης περίπτωσης, δηλαδή ένα τυχαίο στιγμιότυπο του προβλήματος πρέπει να είναι υπολογιστικά δύσκολο. Με δυο λόγια υπάρχει ένας πιθανός κόσμος που $P \neq NP$ αλλά δεν υπάρχει χρήσιμη κρυπτογραφία. Ένας τέτοιος κόσμος πάντως δεν είναι αναμενόμενος.

Ένα σημαντικό εργαλείο για την κατηγοριοποίηση των υπολογιστικών προβλημάτων είναι η έννοια της ***αναγωγής (reduction)***. Έστω δυο προβλήματα A και B. Φανταστείτε πως έχουμε ένα μαντείο (oracle) ή αλλιώς ένα ``μαύρο κουτί'' που μας δίνει τη λύση για το πρόβλημα B. Θα συμβολίζουμε έναν αλγόριθμο $\mathcal{A}$ για το πρόβλημα A, ο οποίος έχει πρόσβαση στο μαντείο του B, ως $\mathcal{A}^B$. Ορίζουμε μια σχέση[1] $\leq$ πάνω σε όλα τα προβλήματα έτσι ώστε $A \leq B$ αν και μόνο αν υπάρχει $\mathcal{A}$, όπου $\mathcal{A}^B$ λύνει το A. Ο αλγόριθμος $\mathcal{A}$ είναι η αναγωγή του προβλήματος στο B. Συνήθως απαιτούμε ο αλγόριθμος $\mathcal{A}$ να έχει κάποια δομικά χαρακτηριστικά, π.χ., να είναι πολυωνυμικού χρόνου, η να ρωτάει το μαντείο B ένα ορισμένο αριθμό από φορές.

Διαισθητικά, το γεγονός πως $A \leq B$ συνεπάγεται πως το A δεν μπορεί να είναι σημαντικά δυσκολότερο από το B. Έστω πως το A είναι ένα γνωστό δύσκολο πρόβλημα, όπως το πρόβλημα της παραγοντοποίησης ή του διακριτού λογαρίθμου που είναι χρήσιμα στην κρυπτογραφία και θα δούμε αργότερα, και το αντιστοιχεί στο ``σπάσιμο'' της ασφάλειας μιας από τις κρυπτογραφικές μας κατασκευές. Αν το είναι αποδεκτά δύσκολο και μπορούμε να κατασκευάσουμε μια αναγωγή, όπως την ορίσαμε παραπάνω, μπορούμε να υποθέσουμε πως η κατασκευή μας είναι αποδείξιμα ασφαλής. Αυτό γιατί το σπάσιμο της ασφάλειας του συστήματος μας δίνει ένα αποδοτικό αλγόριθμο για το και αυτό σε συνδυασμό με την αναγωγή μας $\mathcal{A}^B$ δίνει ένα αποδοτικό αλγόριθμο για το A που πιστεύουμε ότι δεν υπάρχει.

Παρ' ότι το γεγονός πως οι αναγωγές δεν παρέχουν πραγματική απόδειξη ασφαλείας, είναι αποδεκτές δεδομένης της γενικής ανικανότητάς μας να κατασκευάσουμε κάτω φράγματα στην δυσκολία των υπολογιστκών προβλημάτων.

[1] Η σχέση αυτή λέγεται προ-ταξινόμηση, ή pre-order: είναι ανακλαστική (reflexive), μεταβατική (transitive) σχέση.