Κρυπτογραφία - Πρωτόκολλο Diffie-Hellman

Χρυσάνθη Μελίτα Κίτσιου

ΑΕΜ: 7115142100010, ΑΛΜΑ

Αλγόριθμοι & Πολυπλοκότητα, Χειμερινό 2023

Ασφαλής Μετάδοση Πληροφορίας

Απόρρητες πληροφορίες διέρχονται από μη ασφαλείς διαύλους επικοινωνίας ή αποθηκεύονται με διάφορους τρόπους.

Ιδιότητες

- Εμπιστευτικότητα: εξουσιοδοτημένη πρόσβαση.
- Ακεραιότητα Δεδομένων: ανίχνευση μη εξουσιοδοτημένου χειρισμού τους, πχ τροποποίηση ή αποθήκευση τους.
- Αυθεντικότητα Δεδομένων: αποδείξεις προέλευσης τους, πχ ταυτότητα αποστολέα ή ημερομηνία αποστολής μηνύματος.
- Αδυναμία Αποκήρυξης Δεδομένων: εμποδίζει εμπλεκόμενους να αρνηθούν δεσμεύσεις, πχ αποστολή ή υπογραφή κάποιου μηνύματος.

Κρυπτογράφηση

Ένα κρυπτοσύστημα είναι μια πεντάδα συνόλων (P, C, K, E, D).

- Το E αποτελείται από συναρτήσεις κρυπτογράφησης $E_k : P \to C$, $k \in K$.
- Το D αποτελείται από συναρτήσεις αποκρυπτογράφησης $D_k : C \to P$, $k \in K$.
- Για κάθε $e \in K$ υπάρχει $d \in K$ ώστε για κάθε $m \in P$ να ισχύει $D_d(E_e(m)) = m$.

Συμμετρική - Ασύμμετρη Κρυπτογραφία

Ορισμοί

- Η κρυπτογράφηση καλείται συμμετρική, αν για κάθε $e \in K$ το d που αντιστοιχεί στο e υπολογίζεται εύκολα από το e.
  Γίνεται ανταλλαγή κλειδιού e πριν ξεκινήσει η επικοινωνία, το κλειδί πρέπει να κρατείται μυστικό!
- Η κρυπτογράφηση καλείται ασύμμετρη (κρυπτογράφηση δημοσίου κλειδιού), αν ο υπολογισμός του d από το e είναι πρακτικά αδύνατος.
  Το κλειδί e δημοσιοποιείται, ενώ το d κρατείται κρυφό!

Ασφάλεια & Επιθέσεις Κρυπτοσυστήματος

Αρχή Kerckhoff

Η ασφάλεια του κρυπτογραφήματος δεν πρέπει να εξαρτάται από τη μυστική διαφύλαξη της μεθόδου κρυπτογράφησης, αλλά μόνο από τη μυστική διαφύλαξη των κλειδιών.

Γνωρίζοντας τον τύπο του κρυπτογραφήματος έχουμε τις παρακάτω επιθέσεις:

- Προσβολή κρυπτογραφημένου κειμένου.
- Προσβολή γνωστού απλού κειμένου.
- Προσβολή επιλεγμένου απλού κειμένου.
- Προσβολή επιλεγμένου κρυπτογραφημένου κειμένου.

Privacy & Authentication

Privacy System

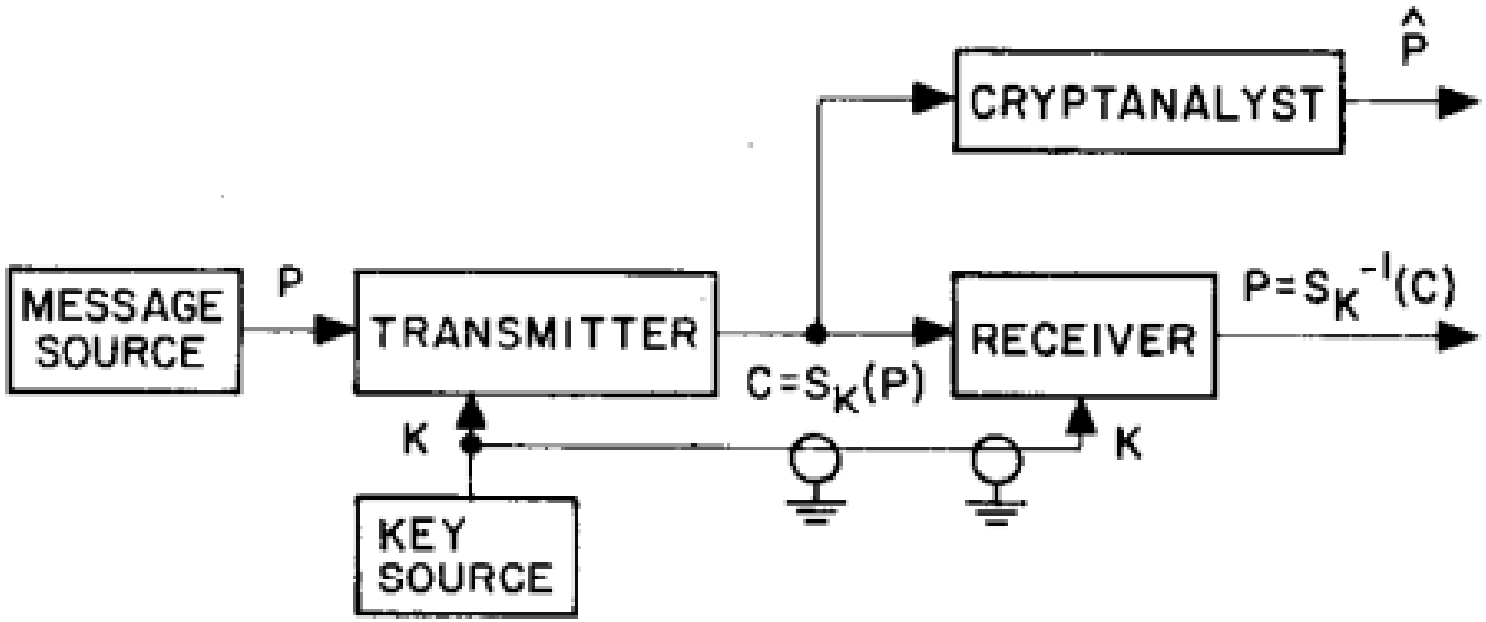
Αποτρέπει την εξαγωγή πληροφοριών από μηνύματα τα οποία μεταδίδονται σε έναν μη ασφαλή δίαυλο επικοινωνίας, (από μη εξουσιδοτημένους χρήστες), ενώ εγγυάται στον αποστολέα ότι το μήνυμα θα διαβαστεί από τον επιθυμητό παραλήπτη.

Authentication System

Αποτρέπει τη μη εξουσιοδοτημένη εισαγωγή μηνυμάτων σε έναν μη ασφαλή δίαυλο επικοινωνίας, ενώ διαβεβαιώνει τον παραλήπτη για τα διαπηστευτήρια του αποστολέα

- message authentication systems.
- user authentication systems.

Μετάδοση Πληροφορίας - Private Key Exchange



Επεξήγηση Εικόνας

Διαδικασία

Ο αποστολέας παράγει μήνυμα P, το οποίο μεταδίδεται από μη ασφαλή δίαυλο επικοινωνίας σε εξουσιοδοτημένο παραλήπτη. Για να μην μάθει ο αντίπαλος το P, εφαρμόζεται αντιστρέψιμος μετασχηματισμός ώστε $C = S_K(P)$. Το κλειδί μεταδίδεται μόνο στον εξουσιοδοτημένο παραλήπτη από ασφαλή δίαυλο. Μέσω του κλειδιού γίνεται η αποκρυπτογράφηση:

$$S_K^{-1}(C) = S_K^{-1}(S_K(P)) = P.$$

Κρυπτοσύστημα της μορφής $\{S_k\}_{k\in K}$, όπου $S_k : \{P\} \to \{C\}$ αντιστρέψιμος μετασχηματισμός.

Private Key Exchange

Λόγω φυσικών περιορισμών, είναι ανέφικτο να εφαρμοστούν συμμετρικά κρυπτοσυστήματα για μεγάλα και ασφαλή τηλεπικοινωνιακά συστήματα.

- Άμεση και γρήγορη επικοινωνία
- Επικοινωνία πολλών ατόμων (άγνωστων σε αριθμό)
- n χρήστες που θέλουν να επικοινωνούν μόνο με συγκεκριμένα άτομα, ιδιωτικά.

Κρυπτογραφία Δημοσίου Κλειδιού

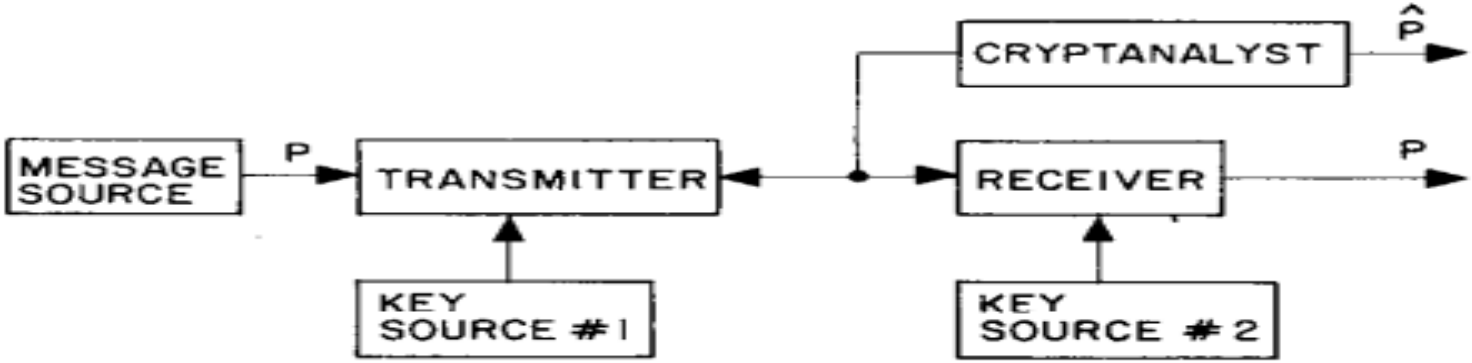
Ένα κρυπτοσύστημα δημοσίου κλειδιού αποτελείται από ζεύγη οικογενειών $\{E_k\}_{k\in K}$, $\{D_k\}_{k\in K}$ αλγορίθμων που αναπαριστούν αντίστρέψιμους μετασχηματισμούς:

$$E_K : \{M\} \to \{M\}$$
$$D_K : \{M\} \to \{M\}$$

όπου $\{M\} = \{P\} = \{C\}$ ένας πεπερασμένος χώρος μηνυμάτων.

- Για κάθε $k \in K$, το E_k αποτελεί τον αντίστροφο του D_k.
- Για κάθε $k \in K$ και $M \in \{M\}$, οι αλγόριθμοι E_k και D_k υπολογίζονται εύκολα.
- Σχεδόν για κάθε $k \in K$, κάθε εύκολα υπολογίσιμος αλγόριθμος ισοδύναμος του D_k δεν μπορεί να ανακτηθεί από το E_k.
- Για κάθε $k \in K$ είναι εφικτός ο υπολογισμός αντίστροφων ζευγών E_k και D_k από το K.

Μετάδοση Πληροφορίας - Public Key Exchange



Πρωτόκολλο Diffie - Hellman

Έστω ότι οι A, B επιθυμούν να επιλέξουν ένα κλειδί για να χρησιμοποιήσουν ένα συμμετρικό κρυπτοσύστημα. Αρχικά, συμφωνείται η χρήση ενός μεγάλου πρώτου αριθμού p και μιας αρχικής ρίζας g κατά μέτρο p, με $2 \leq g \leq p-2$. Οι p, q μπορούν να δημοσιοποιηθούν!

Πρωτόκολλο Diffie - Hellman

Diffie - Hellman

Οι A, B εργάζονται ως εξής:

1. Ο A επιλέγει $z \in \{1, ..., p-2\}$ και υπολογίζει $a = g^z \mod p$.
2. Ο A κραταέι μυστικό τον z και στέλνει τον a στον B.
3. Ο B επιλέγει $w \in \{1, ..., p-2\}$ και υπολογίζει $b = g^w \mod p$.
4. Ο B κραταέι μυστικό τον w και στέλνει τον b στον A.
5. Ο A υπολογίζει $b^z \mod p$.
6. Ο B υπολογίζει $a^w \mod p$.

Έτσι, οι A, B κατασκεύασαν ταυτόχρονα το κοινό κλειδί

$$K = b^z \mod p = a^w \mod p = g^{zw} \mod p.$$

Πρωτόκολλο Diffie - Hellman

Παράδειγμα

Οι A, B επιλέγουν $p = 257$ και την αρχική ρίζα κατά μέτρο 257, $g = 3$.

1. Ο A παίρνει $z = 123$ και υπολογίζει $g^z \equiv 202 (\mod 257)$.
2. Ο A στέλνει στον B το 202.
3. Ο B παίρνει $w = 67$ και υπολογίζει $g^w \equiv 822 (\mod 257)$.
4. Ο B στέλνει στον A το 82.
5. Ο A υπολογίζει $82^{123} \equiv 6 (\mod 257)$.
6. Ομοίως, ο B υπολογίζει $202^{67} \equiv 6 (\mod 257)$.

Το κοινό κλειδί είναι το 6.

Πρόβλημα Διακριτού Λογαρίθμου

Οι ακέραιοι p, g, a, b εύκολα γίνονται γνωστοί. Ο προσδιορισμός του κλειδιού k από τους παραπάνω αριθμούς είναι η επίλυση του Προβλήματος του Διακριτού Λογαρίθμου.

Πρόβλημα Διακριτού Λογάριθμου

Ας είναι p πρώτος και g αρχική ρίζα κατά μέτρο p.
Τότε, $\mathbb{Z}_p^* = \{1, g, g^2 \mod p, ..., g^{p-2} \mod p\}$.
Για κάθε $a \in \mathbb{Z}_p^*$ υπάρχει μοναδικός ακέραιος $x \in \{0, 1, ..., p-2\}$ ώστε $a = g^x \mod p$.
Ο x καλείται διακριτός λογάριθμος του a ως προς βάση g και συμβολίζεται με $\log_g a$.
Το Πρόβλημα του Διακριτού Λογαρίθμου αφορά την εύρεση του x όταν είναι γνωστά τα στοιχεία g και a.

Πρόβλημα Διακριτού Λογαρίθμου

Παρατήρηση

Η πιο απλή μέθοδος για τον υπολογισμό του διακριτού λογαρίθμου είναι η μέθοδος της απαρίθμησης, δηλαδή ο υπολογισμός των δυνάμεων $g, g^2, ...,$ μέχρι να βρεθεί x ώστε $a = g^x \mod p$.

Παράδειγμα

Έχουμε $291068 = 567^{2578} \mod 1048583$. Άρα, $\log_{567} 291068 = 2578$.
Ο υπολογισμός αυτού του διακριτού λογαρίθμου με τη μέθοδο της απαρίθμησης χρειάζεται περίπου 2578 πολλαπλασιασμούς μέσα στην ομάδα $\mathbb{Z}^*_{1048583}$.

Δυσκολία Διακριτού Λογαρίθμου - DLP

DLP$\in NP \cap co - NP$

Απόδειξη

Ας είναι p πρώτος και g μια αρχική ρίζα κατά μέτρο p. Αυτό σημαίνει ότι $\text{ord}_p(g) = p - 1$.

Η παραπάνω συνθήκη μπορεί να επιβεβαιωθεί σε μη ντετερμινιστικό πολυωνυμικό χρόνο ως εξής:

- Μαντεύουμε όλους τους πρώτους παράγοντες $p_1, ..., p_k$ του $p - 1$.
- Κάνουμε primality test για όλους τους παραπάνω αριθμούς.
- Υπολογίζονται τα $(p-1)/p_i$ και ελέγχεται ότι

$$g^{(p-1)/p_i} \not\equiv 1 \mod p$$

για κάθε p_i.

Επομένως, δοθέντων p, g, m, n μπορούμε να δούμε αν p πρώτος, αν g αρχική ρίζα κατά μέτρο p και αν $g^m \equiv n \mod p$. Άρα DLP $\in NP$.

Δυσκολία Διακριτού Λογαρίθμου - DLP

DLP$\in NP \cap co - NP$

Συνέχεια Απόδειξης

Αν δούμε ότι $g^m \not\equiv n \mod p$, τότε

- υπάρχουν i, j με $0 < i, j < p$ ώστε $a^i \equiv a^j \mod p$ ή
- υπάρχει $l \leq m$ ώστε $a^l \equiv n \mod p$ ή
- $n \geq p$.

Τα παραπάνω ελέγχονται σε πολυωνυμικό χρόνο, άρα DLP$\in co - NP$.
Επομένως, DLP$\in NP \cap co - NP$ □

Ψηφιακές Υπογραφές

Στόχος είναι η δημιουργία ψηφιακών υπογραφών ισοδύναμων με τις γραπτές.

One-Way Authentication

Οι τεχνικές που χρησιμοποιούνται για τη δημιουργία ψηφιακών υπογραφών με τις ακόλουθες ιδ., καλούνται one way authentication.
Ιδιότητες:

- Κάθε ένας αναγνωρίζει την υπογραφή ως αυθεντική.
- Μόνο ο εξουσιοδοτημένος αποστολέας μπορεί να αναπαράγει την υπογραφή.
- Μια ψηφιακή υπογραφή πρέπει να είναι αναγνωρίσιμη χωρίς να είναι γνωστή.

Το Πρόβλημα Login

Ανάγκη εύρεσης διαδικασίας που επαληθεύει έναν κωδικό, χωρίς να τον ξέρει!

Login Problem

- Κάθε φορά που ένας χρήστης κάνει login βάζει το σωστό password PW.
- Ο υπολογιστής υπολογίζει το $f(PW)$ μετά την πρώτη εισαγωγή του PW και το αποθηκεύει.
- Σε κάθε επιτυχημένο login, ο υπολογιστής υπολογίζει το $f(X)$, όπου X ο κωδικός και το συγκρίνει με το $f(PW)$.
- Μόνο όταν $f(X) = f(PW)$ ο χρήστης πιστοποιείταθ ως εξουσιοδοτημένος.

Το Πρόβλημα Login

Παρατηρήσεις

- Εύκολος υπολογισμός της f, όπου f κοινή γνώση.
- Ανέφικτος ο υπολογισμός της f^{-1}.
- Δε θεωρείται ασφαλής διαδικασία.

Σχήμα Ψηφιακής Υπογραφής

Ένα σχήμα Ψηφιακής Υπογραφής είναι μια πεντάδα (P, Y, K, S, V)

- Τα σύνολα S, V είναι οικογένειες συναρτήσεων της μορφής

$$sig_k : P \to Y$$
$$ver_k : P \times Y \to \{0, 1\}$$

- Για κάθε $k \in K$ έχουμε τη συνάρτηση υποπγραφής sig_k και τη συνάρτηση επαλήθευσης ver_k.
- Ένα ζεύγος $(x, y) \in P \times Y$ καλείται υπογεγραμμένο μληνυμα. Ισχύει ότι

$$ver_k(x, y) = \begin{cases} 1, sig_k(x) = y \\ 0, \text{αλλιώς} \end{cases}$$

- Για κάθε $k \in K$ οι τιμές των sig_k, ver_k υπολογίζονται στο P.
- Ανέφικτη η εύρεση $y \in Y$ χωρίς τη χρήση της sig_k ώστε να ισχύει $ver_k(x, y) = 1$.

Ψηφιακές Υπογραφές

Ψηφιακή Υπογραφή

1. Ο αποστολέας Α επιλέγει $k \in K$, δημοσιοποιεί την ver_k και κρατά κρυφή την sig_k.
2. Ο παραλήπτης Β ενός υπογεγρ. μηνύματος (x, y) υπολογίζει την τιμή της $ver_k(x, y)$.
3. Αποδέχεται το μήνυμα ως γνήσιο μόνο όταν $ver_k(x, y) = 1$.

Ο αντίπαλος δεν γνωρίζει την sig_k και άρα δεν μπορεί να βρει το κατάλληλο y.

Παρατήρηση

Οποιοσδήποτε γνωρίζει τη συνάρτηση επαλήθευσης του Α μπορεί να πιστοποιήσει την εγκυρότητα του μηνύματος (x, y).

Κρυπτογραφία Δημοσίου Κλειδιού - Υπογραφές

Έστω ότι ο A θέλει να στείλει στον B το καθαρό κείμενο x υπογεγραμμένο και κρυπτγραφημένο.

Διαδικασία

1. Ο Α υπολογίζει την υπογραφή $y = sig_k$.
2. Έπειτα, κρυπτογραφεί το υπογεγραμμένο μήνυμα (x, y) χρησιμοποιώντας το δημόσιο κλειδί του Β.
3. Ο Β λαμβάνει το κρυπτογραφημένο μήνυμα και το αποκρυπτογραφεί με το ιδιωτικό του κλειδί.
4. Ο Β παίρνει το ζεύγος (x, y) και εφαρμόζει τη συνάρτηση ver_k.
5. Αν $ver_k(x, y) = 1$ ο αποστολέας του μηνύματος είναι ο Α.

Δεν είναι το ίδιο ασφαλές αν ο Α κρυπτογραφούσε πρώτα το x κι έπειτα το υπέγραφε!

Ευχαριστώ για την προσοχή σας!