ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

ΕΙΣΑΓΩΓΗ ΣΤΙΣ ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

- **Σε αυτή την παρουσίαση, θα ασχοληθούμε με τα Σχήματα Ψηφιακών Υπογραφών, εξετάζοντας την αναγκαιότητα και τον κρίσιμο ρόλο τους στην ασφάλεια των ηλεκτρονικών συναλλαγών.**
- **Οι ψηφιακές υπογραφές αποτελούν ένα σύστημα δημόσιου κλειδιού που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού εγγράφου, παρέχοντας μηχανισμούς εγκυρότητας και εφαρμοσιμότητας σε μία συναλλαγή.**
- **Θα αναλύσουμε τον γενικό ορισμό, τα βασικά σχήματα (όπως RSA, ElGamal, DSA) και τις ιδιότητές τους, καθώς και πιο εξειδικευμένες μορφές υπογραφών.**

ΑΝΑΓΚΑΙΟΤΗΤΑ ΤΩΝ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ

- **Η χειρόγραφη υπογραφή βασίζεται στη δημιουργία ενός χαρακτηριστικού σημείου με κάποιο είδος γραφής, παρέχοντας στοιχεία για την αυθεντικοποίηση ενός κειμένου και την αποδοχή του από τον συγγραφέα του.**
- **Στον ψηφιακό κόσμο, αντίστοιχα, οι ψηφιακές υπογραφές είναι απαραίτητες για την πιστοποίηση της γνησιότητας και της ακεραιότητας ψηφιακών εγγράφων. Η αναγκαιότητά τους πηγάζει από την ανάγκη να παρέχεται απόδειξη ότι ένα μήνυμα προήλθε από συγκεκριμένο αποστολέα και ότι το μήνυμα είναι αυθεντικό (δεν έχει αλλάξει κατά την αποστολή του), μια ιδιότητα που είναι γνωστή και ως "αδυναμία αποκήρυξης" (non-repudiation). Οι κώδικες αυθεντικοποίησης MAC δεν παρέχουν αυτήν την ιδιότητα.**

Ο ΡΟΛΟΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΝΑΛΛΑΓΩΝ

- **Οι ψηφιακές υπογραφές επιτελούν έναν κρίσιμο ρόλο, όμοιο με αυτόν της παραδοσιακής υπογραφής, δίνοντας το νόημα της "τέλεσης" (ceremony) σε μία πράξη. Υπογραμμίζουν στους συμμετέχοντες ότι η συναλλαγή ή συμφωνία είναι δεσμευτική και μπορεί να έχει νομικές συνέπειες.**

Σε γενικό επίπεδο, παρέχουν:

- **α) Αυθεντικοποίηση του κειμένου και**
- **β) Αποδοχή του από τον συγγραφέα του. Επιπλέον, σε αντίθεση με τις MAC, όπου οι διαδικασίες υπογραφής και επαλήθευσης γίνονται με ένα κοινό μυστικό κλειδί, στις ψηφιακές υπογραφές χρησιμοποιούνται διαφορετικά κλειδιά (ιδιωτικό για υπογραφή, δημόσιο για επαλήθευση).**

ΓΕΝΙΚΟΣ ΟΡΙΣΜΟΣ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ

Ένα **Σχήμα Ψηφιακής Υπογραφής** αποτελείται από τρεις αλγορίθμους:

1. **G** (Παραγωγής Κλειδιών - Key Generation): Ένας πιθανοτικός αλγόριθμος που παράγει ένα ζεύγος (pk, sk). Το pk είναι το **δημόσιο κλειδί** (κλειδί επαλήθευσης), ενώ το sk είναι το **ιδιωτικό κλειδί** (κλειδί υπογραφής).
2. **S** (Υπογραφής - Sign): Ένας πιθανοτικός αλγόριθμος που δέχεται ως είσοδο το ιδιωτικό κλειδί sk και ένα μήνυμα m, και εξάγει την υπογραφή $s = S(sk, m)$.
3. **V** (Επαλήθευσης - Verify): Ένας ντετερμινιστικός αλγόριθμος που δέχεται το δημόσιο κλειδί pk, το μήνυμα m και την υπογραφή s, και επιστρέφει 1 (έγκυρη) ή 0 (άκυρη).

ΣΥΣΤΑΤΙΚΑ ΣΧΗΜΑΤΟΣ: ΠΑΡΑΓΩΓΗ ΚΛΕΙΔΙΩΝ (G)

Ο αλγόριθμος Παραγωγής Κλειδιών (G) είναι το πρώτο βήμα σε κάθε σχήμα ψηφιακής υπογραφής.

- **Λειτουργία:** Είναι συνήθως ένας πιθανοτικός αλγόριθμος πολυωνυμικού χρόνου.
- **Είσοδος:** Δεν δέχεται καμία είσοδο (ή δέχεται παραμέτρους ασφαλείας).
- **Έξοδος:** Παράγει ένα ζεύγος (pk, sk):
  - pk (Public Key/Κλειδί Επαλήθευσης): Χρησιμοποιείται από οποιονδήποτε για την επαλήθευση της υπογραφής.
  - sk (Secret Key/Κλειδί Υπογραφής): Πρέπει να παραμένει μυστικό στον υπογράφοντα και χρησιμοποιείται μόνο για την παραγωγή της υπογραφής.

ΣΥΣΤΑΤΙΚΑ ΣΧΗΜΑΤΟΣ: ΑΛΓΟΡΙΘΜΟΣ ΥΠΟΓΡΑΦΗΣ (S)

Ο αλγόριθμος Υπογραφής (S) είναι η διαδικασία με την οποία ο κάτοχος του ιδιωτικού κλειδιού παράγει την ψηφιακή υπογραφή για ένα μήνυμα.

- **Λειτουργία:** Είναι ένας πιθανοτικός αλγόριθμος πολυωνυμικού χρόνου.
- **Είσοδος:** Δέχεται ως είσοδο το ιδιωτικό κλειδί sk και το μήνυμα m.
- **Έξοδος:** Παράγει την υπογραφή $s = S(sk, m)$.
- **Σημασία:** Μόνο ο χρήστης που κατέχει το ιδιωτικό κλειδί μπορεί να παράγει την υπογραφή, διασφαλίζοντας την **αυθεντικότητα**. Η παραγόμενη υπογραφή s αποστέλλεται μαζί με το μήνυμα m στον παραλήπτη.

ΣΥΣΤΑΤΙΚΑ ΣΧΗΜΑΤΟΣ: ΑΛΓΟΡΙΘΜΟΣ ΕΠΑΛΗΘΕΥΣΗΣ (V)

Ο αλγόριθμος Επαλήθευσης (V) είναι η διαδικασία με την οποία ο παραλήπτης ελέγχει τη γνησιότητα της υπογραφής.

- **Λειτουργία:** Είναι ένας ντετερμινιστικός αλγόριθμος πολυωνυμικού χρόνου.
- **Είσοδος:** Δέχεται το δημόσιο κλειδί pk, το μήνυμα m και την υπογραφή s.
- **Έξοδος:** Επιστρέφει **1** (ή "δέχεται") αν η υπογραφή είναι έγκυρη και έχει παραχθεί από τον κάτοχο του sk, ή **0** (ή "απορρίπτει") αν η υπογραφή είναι άκυρη.
- **Αρχή:** Βασίζεται στο δημόσιο κλειδί, καθιστώντας την επαλήθευση ανοικτή σε όλους. Η επιτυχής επαλήθευση αποδεικνύει την προέλευση του μηνύματος.

ΒΑΣΙΚΕΣ ΙΔΙΟΤΗΤΕΣ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ

Οι ψηφιακές υπογραφές πρέπει να ικανοποιούν κρίσιμες ιδιότητες για να είναι λειτουργικές και ασφαλείς:

- **Αυθεντικότητα (Authenticity): Μόνο ο χρήστης που κατέχει το ιδιωτικό κλειδί μπορεί να παράγει την υπογραφή.**
- **Επαληθευσιμότητα (Verifiability): Η υπογραφή μπορεί να επαληθευτεί από οποιονδήποτε χρησιμοποιώντας το δημόσιο κλειδί.**
- **Αδυναμία Παραχάραξης (Unforgeability): Είναι υπολογιστικά αδύνατο για έναν επιτιθέμενο να κατασκευάσει μια έγκυρη υπογραφή για ένα μήνυμα.**
- **Εξάρτηση από το Μήνυμα: Η υπογραφή s εξαρτάται από το μήνυμα m. Δεν μπορεί να χρησιμοποιηθεί για άλλο μήνυμα (ανεξάρτητα από το περιεχόμενο).**

Η ΙΔΙΟΤΗΤΑ ΤΗΣ ΑΔΥΝΑΜΙΑΣ ΑΠΟΚΗΡΥΞΗΣ (NON-REPUDIATION)

Η αδυναμία αποκήρυξης είναι μια από τις πιο σημαντικές υπηρεσίες που παρέχουν οι ψηφιακές υπογραφές.

- **Ορισμός: Είναι η υπηρεσία που παρέχει απόδειξη ότι ένα μήνυμα προήλθε από συγκεκριμένο αποστολέα και ότι είναι αυθεντικό.**
- **Διαφορά με MAC: Οι κώδικες αυθεντικοποίησης (Message Authentication Code - MAC) δεν παρέχουν αδυναμία αποκήρυξης, επειδή το μυστικό κλειδί είναι κοινό μεταξύ αποστολέα και παραλήπτη. Ο παραλήπτης θα μπορούσε να ισχυριστεί ότι ο αποστολέας έστειλε το μήνυμα, αλλά δεν μπορεί να το αποδείξει μαθηματικά σε τρίτο μέρος.**
- **Ψηφιακές Υπογραφές: Επειδή η υπογραφή παράγεται μόνο με το ιδιωτικό κλειδί του αποστολέα, η υπογραφή μπορεί να χρησιμοποιηθεί ως αδιάψευστη απόδειξη της προέλευσης του μηνύματος.**

ΚΕΝΤΡΙΚΕΣ ΔΙΑΦΟΡΕΣ MAC ΜΕ ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Χαρακτηριστικό	MAC (Κώδικας Αυθεντικοποίησης)	Ψηφιακή Υπογραφή
Τύπος Κρυπτογραφίας	Συμμετρική	Ασύμμετρη
Κλειδί (Υπογραφή/Δημιουργία)	Κοινό Μυστικό Κλειδί (k)	Ιδιωτικό Κλειδί (sk)
Κλειδί (Επαλήθευση)	Κοινό Μυστικό Κλειδί (k)	Δημόσιο Κλειδί (pk)
Παροχή Non-Repudiation	**ΟΧΙ**	**ΝΑΙ**

Δεδομένου ότι το κλειδί k είναι κοινό μεταξύ αποστολέα και παραλήπτη, ο παραλήπτης δεν μπορεί να αποδείξει σε ένα τρίτο μέρος (π.χ., σε έναν διαιτητή) ότι το μήνυμα στάλθηκε όντως από τον αποστολέα, αφού ο ίδιος ο παραλήπτης θα μπορούσε να είχε παράγει το MAC. Αυτή η αδυναμία είναι ο κύριος λόγος που, για νομικά έγγραφα ή δεσμευτικές συναλλαγές, χρησιμοποιούνται Ψηφιακές Υπογραφές αντί για MAC.

ΟΡΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ: ΚΑΤΑΣΚΕΥΑΣΤΙΚΕΣ ΕΠΙΘΕΣΕΙΣ

Η ασφάλεια ενός σχήματος ψηφιακής υπογραφής ορίζεται από την αδυναμία ενός επιτιθέμενου να κατασκευάσει μια έγκυρη υπογραφή. Υπάρχουν διάφορα επίπεδα επιθέσεων (από ισχυρότερη σε ασθενέστερη):

- **Κατασκευή Υπογραφής Ολικής Παραχάραξης (Universal Forgery): Ο επιτιθέμενος μπορεί να υπογράψει οποιοδήποτε μήνυμα επιλέξει.**
- **Κατασκευή Υπογραφής Επιλεκτικής Παραχάραξης (Selective Forgery): Ο επιτιθέμενος μπορεί να υπογράψει ένα μήνυμα m που επέλεξε πριν ξεκινήσει την επίθεση.**
- **Κατασκευή Υπογραφής Υπάρχουσας Παραχάραξης (Existential Forgery): Ο επιτιθέμενος μπορεί να υπογράψει τουλάχιστον ένα μήνυμα m που δεν είχε επιλεγεί από τον ίδιο. Αυτή είναι η πιο αδύναμη μορφή επίθεσης και πρέπει να αντιμετωπίζεται από ένα ασφαλές σχήμα.**

ΜΟΝΤΕΛΟ ΕΠΙΘΕΣΗΣ: CHOSEN MESSAGE ATTACK (CMA)

Η πιο ισχυρή μορφή επίθεσης στην οποία πρέπει να αντέχει ένα σχήμα ψηφιακής υπογραφής είναι η **Επίθεση Επιλεγμένου Μηνύματος (Chosen Message Attack - CMA).**

Σενάριο: Ο επιτιθέμενος παρακολουθεί την επικοινωνία, έχει πρόσβαση στο δημόσιο κλειδί του θύματος p_k και έχει τη δυνατότητα να επιλέξει συγκεκριμένα μηνύματα και να ζητήσει την υπογραφή τους (μέσω ενός **Oracle Υπογραφής**).

Γνώση: Ο επιτιθέμενος αποκτά ένα σύνολο ζευγαριών (m_i, s_i), όπου s_i είναι η έγκυρη υπογραφή του μηνύματος *mi* από το θύμα.

•**Στόχος:** Να κατασκευάσει μια έγκυρη υπογραφή *s′* για ένα **νέο** μήνυμα *m′* που **δεν** έχει προηγουμένως υπογραφεί από το θύμα. Ένα ασφαλές σχήμα πρέπει να είναι **ανθεκτικό σε υπάρχουσα παραχάραξη υπό CMA.**

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΑΠΟ TRAPDOOR FUNCTIONS (TDF)

Πολλά σχήματα ψηφιακών υπογραφών, όπως το RSA, βασίζονται σε συναρτήσεις μονής κατεύθυνσης με "παγίδα" (Trapdoor Functions - TDF).

- **Αρχή:** Μια TDF f επιτρέπει τον εύκολο υπολογισμό της προς τα εμπρός ($c = f(x)$) αλλά είναι υπολογιστικά ανέφικτη η αντιστροφή της ($x = f^{-1}(c)$), εκτός αν κάποιος κατέχει τη μυστική πληροφορία.
- **Υλοποίηση:** Για την ψηφιακή υπογραφή, ο ρόλος των κλειδιών αντιστρέφεται σε σχέση με την κρυπτογράφηση: το **ιδιωτικό κλειδί** sk επιτρέπει την **αντιστροφή** της συνάρτησης.
- **Υπογραφή:** Η υπογραφή s είναι η αντιστροφή της f στο μήνυμα m (ή στη σύνοψή του): $s = f^{-1}(sk, m)$.
- **Επαλήθευση:** Ο παραλήπτης ελέγχει αν ισχύει $f(pk, s) = m$.

ΧΡΗΣΗ ΣΥΝΑΡΤΗΣΕΩΝ ΣΥΝΟΨΗΣ (HASH FUNCTIONS)

Στην πράξη, αντί να υπογράφεται ολόκληρο το μήνυμα, υπογράφεται η σύνοψή (hash) του, χρησιμοποιώντας μια κρυπτογραφική Συνάρτηση Σύνοψης (Hash Function).

- **Λόγος:** Οι σύγχρονοι αλγόριθμοι ψηφιακών υπογραφών, όπως το RSA, λειτουργούν σε μπλοκ δεδομένων σταθερού (μικρού) μήκους. Η χρήση μιας συνάρτησης σύνοψης επιτρέπει την υπογραφή **οποιουδήποτε μήκους** μηνύματος.
- **Διαδικασία:**
  1. Υπολογισμός της σύνοψης του μηνύματος: $h = H(m)$.
  2. Υπογραφή της σύνοψης: $s = S(sk, h)$.
  3. Ο παραλήπτης επαληθεύει: $V(pk, h, s) = 1$ και στη συνέχεια ελέγχει αν $h = H(m)$.
- **Ασφάλεια:** Η ασφάλεια της ψηφιακής υπογραφής εξαρτάται άμεσα από τις ιδιότητες της συνάρτησης σύνοψης, κυρίως την **αδυναμία εύρεσης συγκρούσεων**.

ΠΑΡΑΔΕΙΓΜΑ 1:ΣΧΗΜΑ ΥΠΟΓΡΑΦΗΣ RSA - ΛΕΙΤΟΥΡΓΙΑ

Το σχήμα υπογραφής **RSA** είναι ένα από τα πιο γνωστά και βασίζεται στην αντιστροφή του ρόλου των κλειδιών του κρυπτοσυστήματος RSA.

- **Παραγωγή Κλειδιών:**
  - **Δημόσιο Κλειδί:** (e, N). **Ιδιωτικό Κλειδί:** d.
- **Υπογραφή (Sign):** Ο υπογράφων (Alice) υπολογίζει την υπογραφή s του μηνύματος m (ή της σύνοψής του h):

$$s = m^d \pmod{N}$$

(d είναι ο ιδιωτικός εκθέτης, η αντιστροφή της συνάρτησης $f(x) = x^e \pmod{N}$).

- **Επαλήθευση (Verify):** Ο παραλήπτης (Bob) χρησιμοποιεί το δημόσιο κλειδί e για να επαληθεύσει:

$$s^e \stackrel{?}{\equiv} m \pmod{N}$$

Αν η ισοτιμία ισχύει, η υπογραφή είναι έγκυρη.

ΠΑΡΑΔΕΙΓΜΑ 2: ΣΧΗΜΑ ΥΠΟΓΡΑΦΗΣ RSA - ΑΡΙΘΜΗΤΙΚΟ ΠΑΡΑΔΕΙΓΜΑ

- **Παράμετροι:** Έστω $N = 323$ ($p = 17, q = 19$), $\phi(N) = 288$.
  - **Δημόσιο Κλειδί** $e = 17$.
  - **Ιδιωτικό Κλειδί** $d = 305$ (επειδή $17 \cdot 305 \equiv 1 \pmod{288}$).
- **Μήνυμα προς Υπογραφή:** Έστω $m = 4$ (ή η σύνοψή του).
- **Υπογραφή (Alice):**

$$s = 4^{305} \pmod{323}$$

Η Alice υπολογίζει το s και στέλνει το ζευγάρι $(m = 4, s)$ (Σημείωση: $4^{305} \pmod{323} \equiv 4$).

- **Επαλήθευση (Bob):**

$$s^e \pmod{N} = 4^{17} \pmod{323}$$

$$4^{17} \pmod{323} \equiv 4 \pmod{323}$$

Εφόσον $s^e \equiv m \pmod{N}$ (δηλαδή $4 \equiv 4$), η ψηφιακή υπογραφή **δέχεται** ως σωστή.

ΣΧΗΜΑ ΥΠΟΓΡΑΦΗΣ ELGAMAL - ΓΕΝΙΚΗ ΠΕΡΙΓΡΑΦΗ

Το σχήμα υπογραφής **ElGamal** είναι ένα σχήμα δημόσιου κλειδιού που βασίζεται στο πρόβλημα του **διακριτού λογαρίθμου** (DLOG).

- **Παραγωγή Κλειδιών:**
  - Επιλέγεται ένας μεγάλος πρώτος αριθμός p και ένα πρωταρχικό στοιχείο g.
  - **Ιδιωτικό κλειδί:** Ένας τυχαίος αριθμός x.
  - **Δημόσιο κλειδί:** $y \equiv g^x \pmod{p}$.
- **Υπογραφή:** Για ένα μήνυμα m (ή τη σύνοψή του $H(m)$), η υπογραφή s είναι ένα ζεύγος (r, δ) που υπολογίζεται με βάση τον m, το x (ιδιωτικό κλειδί) και ένα τυχαίο k (εφήμερο κλειδί).
- **Επαλήθευση:** Η επαλήθευση γίνεται ελέγχοντας αν ικανοποιείται μια συγκεκριμένη ισοτιμία που συνδέει το m, το δημόσιο κλειδί y και την υπογραφή (r, δ).

ΣΧΗΜΑ ΥΠΟΓΡΑΦΗΣ ELGAMAL - ΠΡΟΒΛΗΜΑ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια του σχήματος υπογραφής ElGamal βασίζεται στην υπολογιστική δυσκολία της επίλυσης του προβλήματος του **διακριτού λογαρίθμου** (DLOG).

- **Επίθεση:** Ένας επιτιθέμενος θα μπορούσε να προσπαθήσει να παραχαράξει μια υπογραφή επιλέγοντας ένα r και το μήνυμα m, και να προσπαθήσει να υπολογίσει την αντίστοιχη τιμή δ λύνοντας το πρόβλημα του διακριτού λογαρίθμου. Η επίλυση του DLOG είναι υπολογιστικά ανέφικτη για μεγάλους πρώτους.
- **Κρίσιμο Σημείο:** Ένα σοβαρό πρόβλημα ασφαλείας προκύπτει αν στο ElGamal ή στο DSA κάποιος χρησιμοποιήσει **δύο φορές το ίδιο εφήμερο κλειδί** k για δύο διαφορετικά μηνύματα. Σε αυτή την περίπτωση, μπορεί να υπολογιστεί το ιδιωτικό κλειδί x του υπογράφοντα, οδηγώντας σε ολική παραχάραξη.

ΠΡΟΤΥΠΟ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ (DSA/DSS) - ΟΡΙΣΜΟΣ

Το **Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard - DSS)**, που υλοποιείται από τον αλγόριθμο **DSA (Digital Signature Algorithm)**, είναι ένα ευρέως χρησιμοποιούμενο σχήμα που βασίζεται στο πρόβλημα του **διακριτού λογαρίθμου**.

- **Εξέλιξη:** Λόγω της ανάγκης για μικρότερο μέγεθος κλειδιών και υπογραφών, χρησιμοποιείται κυρίως η εκδοχή με ελλειπτικές καμπύλες, η **ECDSA** (Elliptic Curve Digital Signature Algorithm).
- **Εφαρμογές:** Η ECDSA είναι κρίσιμη σε πολλές εφαρμογές, όπως το πρωτόκολλο του Bitcoin για την υπογραφή των συναλλαγών και στα πιστοποιητικά SSL/TLS.

ΠΑΡΑΔΕΙΓΜΑ 3: ΠΡΟΤΥΠΟ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ (DSA/DSS) - ΜΕΓΕΘΟΣ

Το DSA/DSS έχει ένα σημαντικό πλεονέκτημα σε σχέση με το ElGamal όσον αφορά το μέγεθος της υπογραφής, κάτι που το καθιστά πιο πρακτικό.

- **Αρχή Λειτουργίας:** Στο DSA/DSS, όλοι οι κρίσιμοι υπολογισμοί της υπογραφής γίνονται $(\mathrm{mod}\ q)$, όπου q είναι ένας μικρότερος πρώτος αριθμός.
- **Μείωση Μεγέθους:** Το γεγονός αυτό μειώνει δραστικά το μέγεθος της τελικής υπογραφής, η οποία αποτελείται από το ζεύγος (r, s).
- **Αριθμητική Σύγκριση:**
  - Για έναν πρώτο p μεγέθους 768 bit, το ElGamal παράγει υπογραφή **1536 bit**.
  - Το DSS (με q 160 bit) παράγει υπογραφή **320 bit** (2×160 bit), κάνοντάς το πολύ πιο αποδοτικό σε αποθηκευτικό χώρο και εύρος ζώνης.

ΥΠΟΓΡΑΦΕΣ ΜΙΑΣ ΧΡΗΣΗΣ (ONE-TIME SIGNATURES - OTS)

Οι υπογραφές μιας χρήσης είναι σχήματα που έχουν σχεδιαστεί για να χρησιμοποιούνται για την υπογραφή **μόνο ενός μηνύματος**.

- **Βάση:** Βασίζονται σε συναρτήσεις μονής κατεύθυνσης (one-way functions), όπως οι κρυπτογραφικές συναρτήσεις σύνοψης (π.χ. SHA-256).
- **Ασφάλεια:** Η ασφάλειά τους είναι υψηλή, καθώς οφείλεται στην αδυναμία αντιστροφής της συνάρτησης μονής κατεύθυνσης.
- **Περιορισμός:** Για κάθε μήνυμα απαιτείται η δημιουργία ενός **νέου ζεύγους** δημόσιου/ιδιωτικού κλειδιού. Εάν το κλειδί χρησιμοποιηθεί δεύτερη φορά, η ασφάλεια χάνεται.
- **Σημασία:** Χρησιμοποιούνται κυρίως ως δομικά στοιχεία σε πιο πολύπλοκα σχήματα (π.χ. σε δενδροειδείς δομές για την υπογραφή πολλών μηνυμάτων).

ΤΥΦΛΕΣ ΥΠΟΓΡΑΦΕΣ (BLIND SIGNATURES) - ΟΡΙΣΜΟΣ & ΧΡΗΣΗ

Οι τυφλές υπογραφές είναι μια κατηγορία υπογραφών με επιπρόσθετη λειτουργικότητα που επιτρέπουν την υπογραφή ενός μηνύματος **χωρίς ο υπογράφων να γνωρίζει το περιεχόμενό του**.

- **Διαδικασία:** Ο χρήστης **"τυφλώνει"** (blinds) το μήνυμα m με έναν τυχαίο παράγοντα, ζητά την υπογραφή του τυφλωμένου μηνύματος, και στη συνέχεια **"ξε-τυφλώνει"** (un-blinds) την υπογραφή για να πάρει την έγκυρη υπογραφή για το αρχικό μήνυμα m.
- **Κύρια Εφαρμογή:** Η πιο σημαντική εφαρμογή τους είναι στα **ψηφιακά μετρητά (digital cash)**, όπου επιτρέπουν την έκδοση νομισμάτων που διασφαλίζουν την ανωνυμία του χρήστη.

ΠΑΡΑΔΕΙΓΜΑ 4: ΤΥΦΛΕΣ ΥΠΟΓΡΑΦΕΣ - ΕΦΑΡΜΟΓΗ ΣΤΑ ΨΗΦΙΑΚΑ ΜΕΤΡΗΤΑ

Οι τυφλές υπογραφές (Chaum) είναι η βάση για την υλοποίηση ψηφιακών νομισμάτων που διασφαλίζουν την ανωνυμία.

- **Στόχος:** Η τράπεζα να υπογράψει το ψηφιακό νόμισμα χωρίς να γνωρίζει τον μοναδικό σειριακό αριθμό του, διασφαλίζοντας έτσι την **ανωνυμία** του πελάτη.
- **Διαδικασία:**
  1. Ο πελάτης δημιουργεί τον σειριακό αριθμό (μήνυμα m).
  2. Τυφλώνει το m σε m' και το στέλνει στην τράπεζα.
  3. Η τράπεζα υπογράφει **τυφλά** το m' και επιστρέφει την υπογραφή s'.
  4. Ο πελάτης **ξε-τυφλώνει** την s' για να πάρει την έγκυρη υπογραφή s για το αρχικό m.
- **Ανώνυμη Συναλλαγή:** Η τράπεζα μπορεί να επαληθεύσει την υπογραφή της, αλλά **δεν μπορεί να συνδέσει το νόμισμα με τον αρχικό πελάτη**, λόγω του "τυφλώματος".

ΑΔΙΑΜΦΙΣΒΗΤΗΤΕΣ ΥΠΟΓΡΑΦΕΣ (UNDENIABLE SIGNATURES)

Οι αδιαμφισβήτητες υπογραφές εισήχθησαν από τους Chaum και van Antwerpen.

- **Ορισμός:** Σε αντίθεση με τις κοινές ψηφιακές υπογραφές, η επαλήθευση μιας αδιαμφισβήτητης υπογραφής **απαιτεί τη συνεργασία του υπογράφοντα**.
- **Διαδικασία:** Ο υπογράφων συμμετέχει σε ένα **διαλογικό πρωτόκολλο** (interactive protocol) για να αποδείξει στον παραλήπτη ότι η υπογραφή είναι γνήσια.
- **Άρνηση:** Εάν η υπογραφή είναι πλαστή, ο υπογράφων μπορεί να αποδείξει ότι δεν υπέγραψε το μήνυμα μέσω ενός πρωτοκόλλου "**άρνησης**" (disavowal protocol).
- **Πλεονέκτημα:** Δυσκολεύει τη χρήση της υπογραφής ως απόδειξη σε τρίτους χωρίς τη συγκατάθεση του υπογράφοντα, προσφέροντας μεγαλύτερο έλεγχο στον υπογράφοντα.

ΟΜΑΔΙΚΕΣ ΥΠΟΓΡΑΦΕΣ (GROUP SIGNATURES)

Οι ομαδικές υπογραφές επιτρέπουν σε μια ομάδα οντοτήτων να υπογράφει μηνύματα με κοινές ιδιότητες, διατηρώντας παράλληλα ένα επίπεδο **ανωνυμίας**.

- **Ιδιότητες:**
  1. **Περιορισμένη Υπογραφή:** Μόνο τα μέλη της ομάδας μπορούν να υπογράφουν μηνύματα.
  2. **Ανωνυμία:** Ο παραλήπτης μπορεί να επαληθεύσει την εγκυρότητα της υπογραφής, αλλά **δεν μπορεί να διακρίνει** το μέλος της ομάδας που υπέγραψε.
  3. **Ανιχνευσιμότητα (Traceability):** Σε περίπτωση αντιδικίας ή κακόβουλης χρήσης, μπορεί να **ανακαλυφθεί** το μέλος που υπέγραψε, με τη βοήθεια ενός ειδικού μέλους, του **αρχηγού** της ομάδας.

ΕΦΑΡΜΟΓΕΣ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ

Οι ψηφιακές υπογραφές είναι θεμελιώδεις για την ασφάλεια σε πολλές σύγχρονες εφαρμογές:

- **Blockchain & Bitcoin (E5):** Στο πρωτόκολλο του Bitcoin, οι χρήστες υπογράφουν τις **συναλλαγές** τους με τον αλγόριθμο **ECDSA** (Elliptic Curve Digital Signature Algorithm). Αυτό αποδεικνύει ότι ο αποστολέας είναι ο νόμιμος κάτοχος των ψηφιακών νομισμάτων.
- **Υποδομή Δημοσίου Κλειδιού (PKI):** Οι Αρχές Πιστοποίησης (Certificate Authorities) χρησιμοποιούν ψηφιακές υπογραφές για να υπογράψουν τα **πιστοποιητικά** που συνδέουν ένα δημόσιο κλειδί με μια ταυτότητα (π.χ. σε SSL/TLS).
- **Ασφαλή E-mail:** Χρησιμοποιούνται σε πρωτόκολλα όπως το **PGP** (Pretty Good Privacy) και το **S/MIME** για την υπογραφή και την κρυπτογράφηση ηλεκτρονικών μηνυμάτων, διασφαλίζοντας την αυθεντικότητα και την ακεραιότητα του περιεχομένου.

ΣΥΝΟΨΗ - ΚΥΡΙΑ ΣΗΜΕΙΑ

Οι ψηφιακές υπογραφές είναι ο ακρογωνιαίος λίθος της ασφάλειας στον ψηφιακό κόσμο, παρέχοντας μηχανισμούς για την αντικατάσταση της φυσικής υπογραφής.

- **Λειτουργία:** Λειτουργούν ως σύστημα **δημόσιου κλειδιού**, όπου η υπογραφή παράγεται με το ιδιωτικό κλειδί (sk) και επαληθεύεται με το δημόσιο (pk), εξασφαλίζοντας **αυθεντικότητα** και **επαληθευσιμότητα**.
- **Κεντρική Ιδιότητα:** Η πιο κρίσιμη ιδιότητα είναι η **Αδυναμία Αποκήρυξης** (Non-Repudiation), η οποία διασφαλίζει ότι ο υπογράφων δεν μπορεί να αρνηθεί την υπογραφή του.
- **Ασφάλεια:** Η ασφάλεια ορίζεται από την αντοχή σε **Κατασκευή Υπογραφής Υπάρχουσας Παραχάραξης υπό CMA** (Existential Unforgeability under CMA).
- **Βασικά Σχήματα:** Τα κυριότερα σχήματα είναι το **RSA** (που βασίζεται σε TDF) και το **DSA/ElGamal** (που βασίζονται στο πρόβλημα του διακριτού λογαρίθμου).

ΣΥΜΠΕΡΑΣΜΑΤΑ - ΜΕΛΛΟΝΤΙΚΕΣ ΤΑΣΕΙΣ

Οι ψηφιακές υπογραφές έχουν καθιερωθεί ως απαραίτητο εργαλείο για την αυθεντικοποίηση και την εμπιστοσύνη στις ψηφιακές συναλλαγές.

Πρακτική Υλοποίηση: Η χρήση κρυπτογραφικών συναρτήσεων σύνοψης είναι πρακτικά απαραίτητη για την υπογραφή μεγάλων μηνυμάτων, διασφαλίζοντας την ακεραιότητα και μειώνοντας τον χρόνο υπολογισμού.

Εξειδικευμένες Μορφές: Οι εξειδικευμένες μορφές όπως οι Τυφλές Υπογραφές (για ανωνυμία, π.χ. ψηφιακά μετρητά) και οι Ομαδικές Υπογραφές (για ανωνυμία εντός ομάδας με δυνατότητα αναγνώρισης) συνεχίζουν να επεκτείνουν τη λειτουργικότητα και τις εφαρμογές τους.

Μελλοντική Τάση: Δεδομένης της απειλής των κβαντικών υπολογιστών που θα μπορούσαν να "σπάσουν" τους αλγορίθμους RSA και DSA/ElGamal, η έρευνα στρέφεται σε νέα σχήματα υπογραφών που είναι ανθεκτικά σε κβαντικές επιθέσεις (Post-Quantum Cryptography - PQC).

ΕΡΩΤΗΣΕΙΣ ΑΝΑΠΤΥΞΗΣ

Ερώτηση 1: Ανάλυση Ασφάλειας και Ιδιότητες

Ποια είναι η κεντρική διαφορά μεταξύ ενός Κώδικα Αυθεντικοποίησης Μηνυμάτων (MAC) και μιας Ψηφιακής Υπογραφής όσον αφορά την υπηρεσία ασφαλείας που παρέχουν; Εξηγήστε λεπτομερώς την έννοια της Αδυναμίας Αποκήρυξης (Non-Repudiation) και γιατί αυτή η ιδιότητα είναι εγγενής στις Ψηφιακές Υπογραφές, αλλά όχι στους MAC. Περιγράψτε, επίσης, το πιο ισχυρό μοντέλο επίθεσης (π.χ., CMA) στο οποίο πρέπει να αντέχει ένα ασφαλές σχήμα ψηφιακής υπογραφής.

Ερώτηση 2: Η Σημασία των Συναρτήσεων Σύνοψης (Hash Functions)

Εξηγήστε γιατί, στην πράξη, οι περισσότεροι αλγόριθμοι ψηφιακών υπογραφών (π.χ., RSA, DSA) δεν υπογράφουν απευθείας το μήνυμα (m), αλλά την κρυπτογραφική του σύνοψη (H(m)). Ποιοι είναι οι δύο κύριοι πρακτικοί λόγοι για αυτή τη μεθοδολογία; Ποιες δύο κρίσιμες ιδιότητες πρέπει να έχει η συνάρτηση σύνοψης H ώστε να διασφαλίζεται η ασφάλεια της ψηφιακής υπογραφής έναντι επίθεσης παραχάραξης;

ΕΡΩΤΗΣΕΙΣ ΑΝΑΠΤΥΞΗΣ

Ερώτηση 3: **Εξειδικευμένα Σχήματα Υπογραφών και Εφαρμογές**

Αναλύστε τη λειτουργία και τον κύριο σκοπό των Τυφλών Υπογραφών (Blind Signatures), εστιάζοντας στη διαδικασία του "τυφλώματος" και του "ξε-τυφλώματος". Ποια είναι η κυριότερη εφαρμογή των Τυφλών Υπογραφών και ποια υπηρεσία ασφαλείας εξασφαλίζεται με αυτόν τον τρόπο; Συγκρίνετε το με το βασικό πλεονέκτημα των Ομαδικών Υπογραφών (Group Signatures), εξηγώντας πώς συνδυάζουν την ανωνυμία με την ανιχνευσιμότητα.

ΠΡΟΒΛΗΜΑΤΑ ΕΞΑΣΚΗΣΗΣ

Πρόβλημα 1: Υπογραφή και Επαλήθευση με RSA

Δίνεται ένα απλοποιημένο σύστημα ψηφιακής υπογραφής RSA:

- **Δημόσιο Κλειδί:** $(N = 39, e = 11)$
- **Ιδιωτικό Κλειδί:** $d = 3$
- **Μήνυμα προς υπογραφή (ή σύνοψή του):** $m = 5$

1. **Υπογραφή:** Υπολογίστε την ψηφιακή υπογραφή s του μηνύματος $m = 5$, χρησιμοποιώντας το ιδιωτικό κλειδί $d = 3$.

$$s = m^d \pmod{N}$$

2. **Επαλήθευση:** Επαληθεύστε την υπογραφή s που βρήκατε, χρησιμοποιώντας το δημόσιο κλειδί $e = 11$.

$$s^e \stackrel{?}{\equiv} m \pmod{N}$$

(Δείξτε αναλυτικά τους υπολογισμούς για την επαλήθευση).

ΠΡΟΒΛΗΜΑΤΑ ΕΞΑΣΚΗΣΗΣ

Πρόβλημα 2: Επίθεση σε DSA/ElGamal λόγω Επαναχρησιμοποίησης Εφήμερου Κλειδιού

Στα σχήματα DSA ή ElGamal, η ασφάλεια βασίζεται στην τυχαία επιλογή του εφήμερου κλειδιού k. Έστω ότι ένας υπογράφων (Alice) χρησιμοποιεί το ίδιο κλειδί k για να υπογράψει δύο διαφορετικά μηνύματα, m_1 και m_2.

Αν γνωρίζετε τις εξής παραμέτρους:

- **Μήνυμα 1:** m_1
- **Υπογραφή 1:** (r_1, s_1)
- **Μήνυμα 2:** m_2
- **Υπογραφή 2:** (r_2, s_2)

Ερώτηση: Εξηγήστε πώς ένας επιτιθέμενος, γνωρίζοντας μόνο τα δημόσια κλειδιά και τις δύο υπογραφές (και υποθέτοντας ότι k επαναχρησιμοποιήθηκε), θα μπορούσε να **υπολογίσει το ιδιωτικό κλειδί** x της Alice. (Δώστε τον τύπο ή τη διαδικασία που χρησιμοποιείται για την εξαγωγή του x).

(Υπόδειξη: Στο DSA/ElGamal, η σχέση για το s είναι περίπου: $s \equiv k^{-1}(H(m) + x \cdot r) \pmod{q}$)