ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΚΡΥΠΤΟΓΡΑΦΙΑ

6η Διάλεξη

Κωνσταντίνου Ελισάβετ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

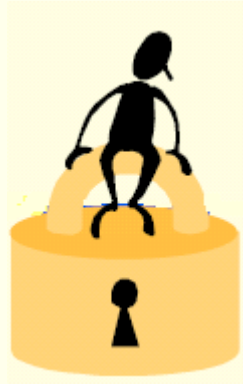
- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Κρυπτογραφία



Κωνσταντίνου Ελισάβετ
ekonstantinou@aegean.gr

http://www.icsd.aegean.gr/ekonstantinou

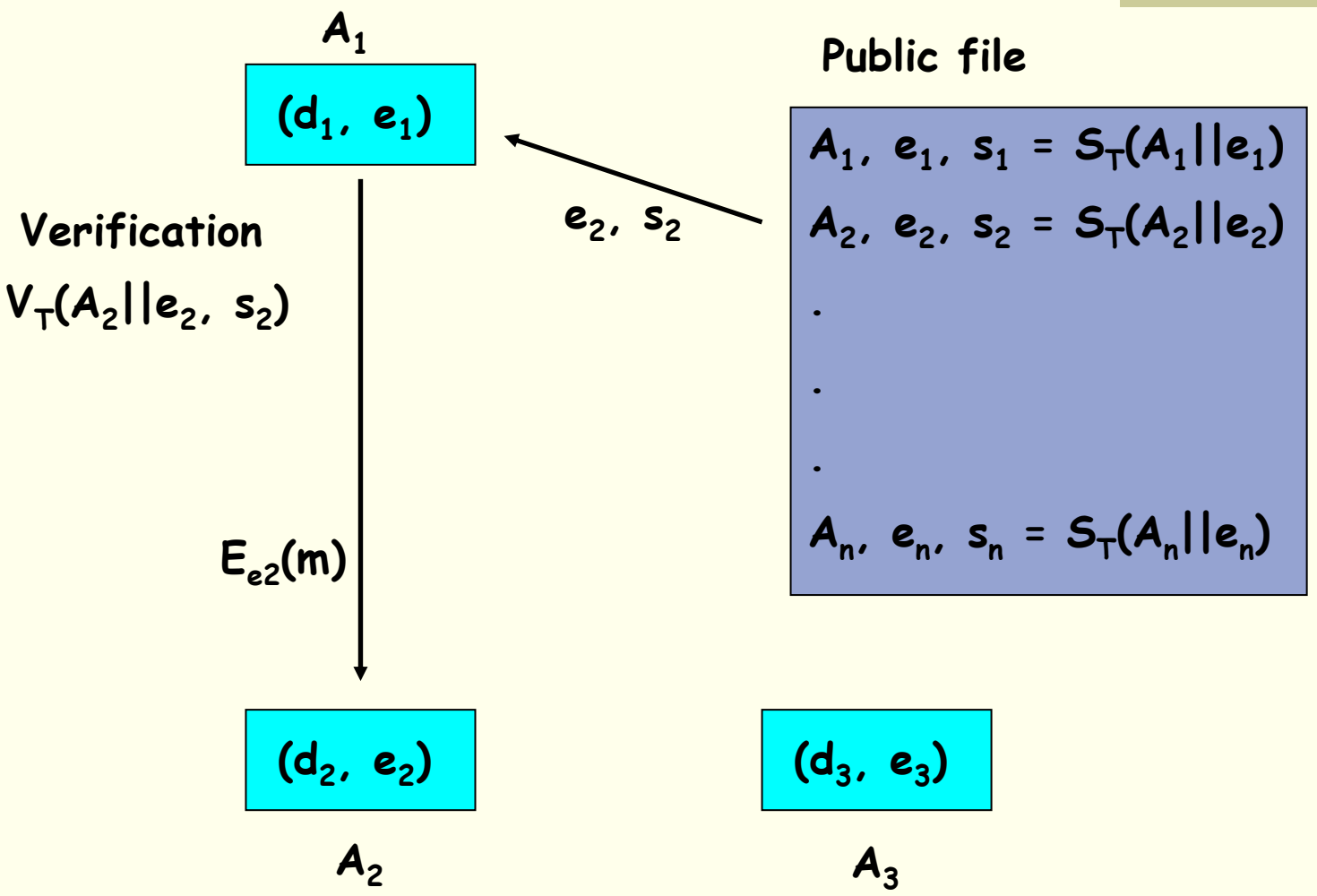
Ψηφιακές Υπογραφές

Ορίζονται πάνω σε μηνύματα και είναι αριθμοί που εξαρτώνται από κάποιο μυστικό κλειδί του υπογράφοντος και επιπλέον από το μήνυμα που υπογράφεται.

Προφανώς, οι ψηφιακές υπογραφές θα πρέπει να είναι επαληθεύσιμες.

Δηλαδή, αν προκύψει μια διαφωνία πάνω στο αν κάποιος έχει υπογράψει κάτι ή όχι, θα πρέπει η διαφωνία να μπορεί να επιλυθεί χωρίς να αποκαλυφθεί η μυστική πληροφορία του υπογράφοντος.

Παράδειγμα Εφαρμογής



Ψηφιακές Υπογραφές

Πιστοποίηση → «δένει» την ταυτότητα ενός χρήστη με ένα συγκεκριμένο δημόσιο κλειδί.

Κύριες Κατηγορίες Ψηφιακών Υπογραφών

Ψηφιακές Υπογραφές με Παράρτημα (Digital Signatures with Appendix)

Ψηφιακές Υπογραφές με Ανάκτηση του Μηνύματος (Digital Signatures with Message Recovery)

Ψηφιακές Υπογραφές

S_A: αλγόριθμος δημιουργίας υπογραφών του *A*

V_A: αλγόριθμος επαλήθευσης υπογραφών του *A*

1) Ψηφιακές Υπογραφές με Παράρτημα:

Εκτός από την υπογραφή στέλνεται και το μήνυμα το οποίο έχει υπογραφεί. Στον αλγόριθμο επαλήθευσης χρησιμοποιείται η υπογραφή και το μήνυμα.

2) Ψηφιακές Υπογραφές με Ανάκτηση Μηνύματος:

Δεν στέλνεται το μήνυμα που έχει υπογραφεί. Στον αλγόριθμο επαλήθευσης ανακτάται το μήνυμα.

Ψηφιακές Υπογραφές με Παράρτημα

Ο χρήστης *A* δημιουργεί μια υπογραφή $s \in S$ για ένα μήνυμα $m \in M$, η οποία μπορεί να επαληθευτεί αργότερα από κάθε χρήστη *B*.

Δημιουργία Υπογραφής:

1) Ο *A* υπολογίζει τις τιμές $m' = h(m)$ και $s = S_A(m')$.
2) Η ψηφιακή υπογραφή του *A* για το μήνυμα *m* είναι το ζευγάρι (s, m) το οποίο είναι διαθέσιμο σε κάθε χρήστη που θέλει να επικυρώσει την υπογραφή.

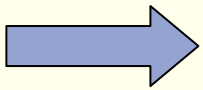
Επαλήθευση:

1) Υπολογίζονται οι τιμές $m' = h(m)$ και $u = V_A(m', s)$.
2) Ο χρήστης *B* δέχεται την υπογραφή αν και μόνο αν $u = \text{true}$.

Ψηφιακές Υπογραφές με Παράρτημα

Πρέπει να ισχύουν οι εξής ιδιότητες:

1) Οι συναρτήσεις S_A και V_A θα πρέπει να υπολογίζονται αποδοτικά (δηλ. σε πολυωνυμικό χρόνο).
2) Θα πρέπει να είναι υπολογιστικά αδύνατο για μια οντότητα εκτός του *A*, να βρει ένα μήνυμα m ϵ M και ένα s ϵ S τέτοια ώστε $V_A(m', s)$ = true (όπου m′ = h(m)).



Στις ψηφιακές υπογραφές με παράρτημα μπορούν να υπογραφούν οσοδήποτε μεγάλα μηνύματα, σε αντίθεση με τις ψηφιακές υπογραφές με ανάκτηση μηνύματος που τα μηνύματα πρέπει να έχουν συγκεκριμένο μήκος.

Ψηφιακές Υπογραφές με Ανάκτηση Μηνύματος

Το μήνυμα ανακτάται μέσω της ψηφιακής υπογραφής και επομένως δεν απαιτείται στη διαδικασία της επαλήθευσης. Αυτές οι ψηφιακές υπογραφές χρησιμοποιούνται για μικρά σε μήκος μηνύματα.

Δημιουργία Υπογραφής:

1) Υπολογίζει τις τιμές $m' = R(m)$, όπου R είναι μια συνάρτηση που καλείται redundancy function (συνάρτηση πλεονασμού).
2) Η ψηφιακή υπογραφή του A για το μήνυμα m είναι η τιμή $s = S_A(m')$.

Επαλήθευση:

1) Υπολογίζεται η τιμή $m' = V_A(s)$.
2) Επαληθεύει ότι $m' \in M_R$ (M_R είναι το σύνολο των μηνυμάτων μετά την επεξεργασία από τη συνάρτηση R).
3) Αν γίνει η επαλήθευση, τότε ανακτάται το αρχικό μήνυμα m από το m' μέσω της σχέσης $m = R^{-1}(m')$.

Redundancy Function

Αυξάνει το μήκος των μηνυμάτων και για αυτό το λόγο καλείται redundancy (πλεονασμός) function.

Ένα παράδειγμα μιας τέτοιας συνάρτησης είναι το εξής:

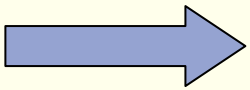
έστω $M = \{m: m \in \{0,1\}^n\}$ και $R: M \rightarrow M_R$ είναι η συνάρτηση $R(m) = m||m$. Τότε κάθε μήνυμα m πριν υπογραφεί παίρνει τη μορφή $m||m$ και στη συνέχεια περνάει από τη συνάρτηση υπογραφής S_A.

Κατά την επαλήθευση, αν η συνάρτηση V_A δεν επιστρέψει κάποιο μήνυμα που έχει την ιδιότητα ότι το πρώτο μισό του είναι ίδιο με το δεύτερο μισό, τότε η υπογραφή δεν επαληθεύεται.

Ψηφιακές Υπογραφές με Ανάκτηση Μηνύματος

Πρέπει να ισχύουν οι εξής ιδιότητες:

1) Οι συναρτήσεις S_A και V_A θα πρέπει να υπολογίζονται αποδοτικά (δηλ. σε πολυωνυμικό χρόνο).
2) Θα πρέπει να είναι υπολογιστικά αδύνατο για μια οντότητα εκτός του A, να βρει ένα s ϵ S τέτοιο ώστε $V_A(s)$ ϵ M_R.



Η μορφή της redundancy function θα πρέπει να είναι τέτοια ώστε να είναι υπολογιστικά αδύνατες τέτοιες επιθέσεις.

Τύποι Επιθέσεων

Ο σκοπός ενός επιτιθέμενου είναι να πλαστογραφήσει υπογραφές. Δηλαδή να δημιουργήσει υπογραφές που θα γίνονται δεκτές από τον αλγόριθμο επαλήθευσης και θα φαίνεται ότι στάλθηκαν από τον σωστό υπογράφοντα.

1) Total break (πλήρες 'σπάσιμο'): είτε ο επιτιθέμενος έχει βρει το μυστικό κλειδί του υπογράφοντος ή έχει βρει μια συνάρτηση που βγάζει τα ίδια αποτελέσματα με την έγκυρη συνάρτηση υπογραφής S_A.
2) Selective forgery (επιλεκτική πλαστογραφία): ο επιτιθέμενος μπορεί να δημιουργήσει έγκυρες ψηφιακές υπογραφές για ορισμένα μηνύματα που έχει επιλέξει.
3) Existential forgery (υπαρκτή πλαστογραφία): ο επιτιθέμενος μπορεί να πλαστογραφήσει μια υπογραφή για ένα τουλάχιστον μήνυμα.

Βασικές Επιθέσεις

1) Key-only attacks: ο επιτιθέμενος γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντος.

2) Message attacks: ο επιτιθέμενος γνωρίζει ζευγάρια υπογραφών-αντίστοιχων μηνυμάτων, για μηνύματα που είτε τα έχει επιλέξει ο ίδιος ή τα γνωρίζει με κάποιον τρόπο.

(a) known message attack
(b) chosen-message attack
(c) adaptive chosen-message attack

Ψηφιακές Υπογραφές RSA

Αποτελεί ένα σχήμα ψηφιακών υπογραφών με ανάκτηση μηνύματος.

Αρχικά, δημιουργούνται τα κλειδιά για κάθε χρήστη:

1) Δημιουργεί δύο μεγάλους πρώτους αριθμούς p και q, περίπου του ίδιου μεγέθους.
2) Υπολογίζει την τιμή $n = pq$ και την $\varphi = (p-1)(q-1) = \varphi(n)$.
3) Επιλέγει ένα τυχαίο e με $1 < e < \varphi$, τέτοιο ώστε $gcd(e, \varphi) = 1$.
4) Υπολογίζει τον μοναδικό ακέραιο d για τον οποίο ισχύει η ισοτιμία $ed \equiv 1 \bmod \varphi$ ($d = e^{-1} \bmod \varphi$).
5) Το δημόσιο κλειδί του A είναι το ζευγάρι (n, e) και ιδιωτικό το d.

Ψηφιακές Υπογραφές RSA

Δημιουργία υπογραφής: Ο Α υπογράφει ένα μήνυμα m

(α) Υπολογίζει την τιμή $m' = R(m)$ (redundancy function). Το m' πρέπει να ανήκει στο διάστημα $[0, n-1]$.

(β) Υπολογίζει την τιμή $s = (m')^d \bmod n$.

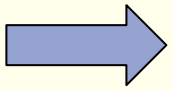
(γ) Η υπογραφή του Α είναι η τιμή s.

Επαλήθευση: Ο Β λαμβάνει την υπογραφή s και το δημόσιο κλειδί (n, e) του Α

(α) Υπολογίζει την τιμή $m' = s^e \bmod n$.

(β) Επαληθεύει ότι $m' \in M_R$. Αν δεν ανήκει τότε απορρίπτει την υπογραφή.

(γ) Υπολογίζει το αρχικό μήνυμα $m = R^{-1}(m')$.



Πως θα το υλοποιούσατε για $R(m) = m||m$?

Πιθανές Επιθέσεις

(a) Επίθεση που βασίζεται στην παραγοντοποίηση ακεραίων:

Αν βρεθούν οι πρώτοι παράγοντες p και q του n, τότε ανακτάται η τιμή φ(n) και συνεπώς το μυστικό κλειδί $d = e^{-1} \bmod \varphi$.

total break

(b) Πολλαπλασιαστική ιδιότητα του RSA (homomorphic property):

Αν $s_1 = m_1^d \bmod n$ και $s_2 = m_2^d \bmod n$ είναι δύο ψηφιακές υπογραφές πάνω στα μηνύματα m_1 και m_2 τότε η τιμή $s = s_1 s_2 = (m_1 m_2)^d \bmod n$. Δηλαδή αν $m_1 m_2 \in M_R$ τότε η s είναι έγκυρη υπογραφή για το μήνυμα $m_1 m_2$. Άρα η redundancy function δεν θα πρέπει να είναι πολλαπλασιαστική ($R(ab) \neq R(a)\,R(b)$).

RSA Υπογραφές στην Πράξη

Public = (n_A, e_A),
private = d_A

$$s = m^{d_A} \bmod n_A$$

$$c = s^{e_B} \bmod n_B$$

Public = (n_B, e_B),
private = d_B

Πρέπει $n_A < n_B$. Γιατί?

Reblocking Problem

Αντιμετώπιση προβλήματος σε περίπτωση που $n_A > n_B$:

1) Αλλαγή σειράς κρυπτογράφησης-υπογραφής.

2) Κάθε οντότητα μπορεί να έχει δύο διαφορετικά ζεύγη κλειδιών, ένα για την υπογραφή και ένα για την κρυπτογράφηση. Τα κλειδιά της υπογραφής για όλους θα πρέπει να είναι τουλάχιστον 1 bit μικρότερα από τα κλειδιά της κρυπτογράφησης.

3) Τα moduli n_A, n_B να έχουν μια συγκεκριμένη μορφή. Π.χ. το 1^o bit να είναι 1 και τα k επόμενα να είναι 0. Τότε οι υπογραφές s θα έχουν με μεγάλη πιθανότητα 1 σε κάποια από αυτές τις k θέσεις και επομένως θα είναι σίγουρα μικρότερες από τα moduli.

Ψηφιακές Υπογραφές Rabin

Παρόμοιο με το RSA, μόνο που τώρα κάθε μήνυμα που υπογράφεται θα πρέπει να είναι τετραγωνικό υπόλοιπο.

Δημιουργία κλειδιών: public = n, private = (p, q).

Δημιουργία υπογραφής για τον χρήστη *A*:

(α) Υπολογίζει την τιμή m′ = R(m) (redundancy function). Το m′ πρέπει να ανήκει στο διάστημα [0, n-1] και να είναι τετραγωνικό υπόλοιπο.

(β) Υπολογίζει μια τετραγωνική ρίζα s του m′.

(γ) Η υπογραφή του *A* είναι η τιμή s.

Ψηφιακές Υπογραφές Rabin

Επαλήθευση: Ο Β λαμβάνει την υπογραφή s και το δημόσιο κλειδί n του Α

(α) Υπολογίζει την τιμή $m' = s^2 \bmod n$.

(β) Επαληθεύει ότι $m' \in M_R$. Αν δεν ανήκει τότε απορρίπτει την υπογραφή.

(γ) Υπολογίζει το αρχικό μήνυμα $m = R^{-1}(m')$.

Το πρόβλημα στο σχήμα αυτό είναι ότι το m' μπορεί να μην είναι τετραγωνικό υπόλοιπο.

→ προστίθενται κάποια τυχαία bits στο m έτσι ώστε το m' να είναι τετραγωνικό υπόλοιπο

→ χρησιμοποιείται το modified Rabin signature scheme (ειδικές συνθήκες για τα p, q και R(.))

Ψηφιακές Υπογραφές Feige-Fiat-Shamir

Τα δύο προηγούμενα πρωτόκολλα ψηφιακών υπογραφών ήταν σχήματα με ανάκτηση μηνύματος και ντετερμινιστικά (deterministic). Το σχήμα ψηφιακών υπογραφών των Feige-Fiat-Shamir είναι με παράρτημα.

Δημιουργία κλειδιών: Κάθε χρήστης *A* κάνει τα παρακάτω.

1) Δημιουργεί δύο πρώτους p και q, καθώς και το n = pq.
2) Επιλέγει έναν θετικό ακέραιο k και διακριτούς τυχαίους αριθμούς $s_1, s_2, \ldots, s_k$ στο Z_n^*.
3) Υπολογίζει τις τιμές $u_j = s_j^{-2} \bmod n$, για όλα τα j.
4) Το δημόσιο κλειδί του *A* είναι το $(u_1, u_2, \ldots, u_k)$ και το n. Ιδιωτικό κλειδί είναι το $(s_1, s_2, \ldots, s_k)$.

Ψηφιακές Υπογραφές Feige-Fiat-Shamir

Η ασφάλεια του μυστικού κλειδιού βασίζεται στο square root modulo n problem.

Δημιουργία υπογραφής: Ο Α υπογράφει ένα μήνυμα m

(α) Επιλέγει μια τυχαία τιμή r, με $0 < r < n$.

(β) Υπολογίζει την τιμή $u = r^2 \bmod n$.

(γ) Υπολογίζει $e = h(m||u)$. Η Hash function επιστρέφει k bits.

(δ) Υπολογίζει την τιμή $s = r(s_1^{e1} s_2^{e2} \ldots s_k^{ek}) \bmod n$.

(ε) Η υπογραφή του Α είναι η (e, s).

Επαλήθευση: Ο Β λαμβάνει την υπογραφή s και το δημόσιο κλειδί $(u_1, u_2, \ldots, u_k)$, n του Α

(α) Υπολογίζει την τιμή $w = s^2 (u_1^{e1} u_2^{e2} \ldots u_k^{ek}) \bmod n$.

(β) Υπολογίζει $e' = h(m||w)$.

(γ) Αν $e = e'$ δέχεται την υπογραφή, διαφορετικά όχι.

Άλλες Ψηφιακές Υπογραφές

1) The Digital Signature Algorithm (DSA) -> το πρώτο σχήμα ψηφιακών υπογραφών που αναγνωρίστηκε από μια κυβέρνηση (Ηνωμ. Πολ.).
2) The ElGamal Signature Scheme. Το DSA αποτελεί παραλλαγή αυτού του αλγορίθμου.
3) The Schnorr Signature Scheme. Όπως και το DSA, αποτελεί παραλλαγή του σχήματος ElGamal.

Όλα βασίζουν την ασφάλειά τους στο πρόβλημα του διακριτού λογαρίθμου και είναι σχήματα ψηφιακών υπογραφών με παράρτημα.

Διάβασμα…

Κεφάλαια 11.1, 11.2, 11.3 και 11.4 του Handbook of Applied Cryptography