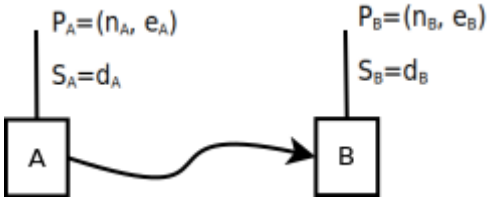
4/5/2017

Υπενθύμιση

Ψηφιακή Υπογραφή με RSA και hash



-με παράρτημα

Αποστολέας:

1. $M \rightarrow h(M)$
2. $\sigma=h(M)^{dA} \bmod n_A$
3. $C_1=h(M)^{eB} \bmod n_B$

   $C_2=\sigma^{eB} \bmod n_B$

Παραλήπτης

4. $M_1=C_1^{dB} \bmod n_B=(\underline{M}^{eB} \bmod n_B)^{dB} \bmod n_B=\underline{M}^{eB\ dB(\bmod nB)} \bmod n_B=\underline{M}$

   $M_2=C_2^{dB} \bmod n_B=(\sigma^{eB} \bmod n_B)^{dB} \bmod n_B=\sigma^{eBdB(\bmod nB)} \bmod n_B=\sigma$
5. $\underline{M} \rightarrow h(\underline{M})$
6. $M_3=\sigma^{eA} \bmod n_A=h(\underline{M})^{dAeA} \bmod n_A=h(\underline{M})$
7. verify αν το 5 και το βήμα 5 και το βήμα 6 είναι ίσα

-με ανάκτηση μηνύματος

Αποστολέας

1. $M \rightarrow R(M)$
2. $\sigma=R(M)^{dA} \bmod n_A$
3. $c=\sigma^{eB} \bmod n_B$

Παραλήπτης

4. $M_1=C^{dB} \bmod n_B=\sigma^{eB\ dB(\bmod nB)} \bmod n_B=\sigma$
5. $M_2=\sigma^{eA} \bmod n_A=R(M)^{eAdA} \bmod n_A=R(M)$
6. Ελέγχω αν το R(M) είναι σωστό σε μορφή
7. $R(M) \rightarrow M$

Authentication
Ή πώς μπορούμε να πείσουμε κάποιον για την ταυτότητά μας ή ότι διαθέτουμε κάποια ιδιότητα.

Πρωτόκολλα μηδενικής γνώσης: Zero knowledge/proof of knowledge
Προσπαθώ να πείσω κάποιον για την ταυτότητά μου χωρίς να μάθει τίποτα για μένα.

- **Πληρότητα:** Αν η πρόταση είναι αληθής, τότε ένας έντιμος επαληθευτής την αποδέχεται.
- **Ορθότητα:** Αν η πρόταση είναι λανθασμένη, ένας έντιμος επαληθευτής την αποδέχεται με πολύ μικρή πιθανότητα.
- **Μηδενική γνώση:** Ο επαληθευτής δεν μαθαίνει τίποτα πέρα από την ορθότητα της πρότασης.

Fiat-Shamir Zero Knowledge Protocol
Υποθέτουμε ότι υπάρχει μια έμπιστη αρχή Τ.

Αρχικοποίηση: η Τ διαλέγει μεγάλους πρώτους p, q και κοινοποιεί n=pq.

Κάθε χρήστης: διαλέγει s ώστε gcd(s,n)=1

υπολογίζει $u=s^2 \bmod n$

κοινοποιεί u

Έτσι ο Α θέλει να πείσει τον Β ότι γνωρίζει το s.

A	t γύροι	B
1. διαλέγει τυχαίο r υπολογίζει $x^2 \equiv r^2 \bmod n$ στέλνει x	→	
	← πρόκληση	2. Διαλέγει e στο {0,1} στέλνει e
3. Υπολογίζει $y=xs^e$ στέλνει y	απάντηση→	4. δέχεται το γύρο -αν y≠0 ελέγχει αν $y^2=xu^e \bmod n$. Αν δεν ισχύει, τότε ο Α λέει ψέματα -αν y=0 ο γύρος τελειώνει

Για e=0

3. $y=r \bmod n$ και το 4. είναι $r^2=x \bmod n$ που ισχύει λόγω του 1.

Για e=1

3. $y=rs \bmod n$ και το 4. είναι $r^2s^2=xu \bmod n$

Αν το e=1 τότε το μυστικό μένει στο παιχνίδι, αλλά αν είναι 0, τότε μένει μόνο το r και στην ουσία ο επαληθευτής δεν ελέγχει το μυστικό. Άρα γιατί χρειαζόμαστε τον έλεγχο για e=0;

Έστω ότι το e είναι πάντα 1. Μπορούμε να ξεγελάσουμε τον επαληθευτή ως εξής:
1. επιλέγουμε x ώστε $x'=r^2u^{-1}\mod n$
3. στέλνουμε y'=r, άρα $y'^2=x'u \mod n$. Ο επαληθευτής θα ελέγξει το $y'^2=x'u \mod n$, που είναι $r^2=r^2u^{-1}u \mod n$ δηλαδή θα επαληθεύεται ακόμα και αν δεν γνωρίζουμε το s.
Πώς βοηθάει λοιπόν τον επαληθευτή ο συνδυασμός των δύο τρόπων επαλήθευσης;
Έστω ότι ο επαληθευτής στέλνει e=0 ενώ ο αποδείκτης περιμένει να του σταλεί 1.
1. $x'=r^2u^{-1}\mod n$
2. e=0
3. y=; Θα πρέπει ο αποδείκτης να βρει ένα y τέτοιο ώστε $y^2=r^2u \mod n$, δηλαδή να βρει τον αντίστροφο ενός αριθμού modulo ένα σύνθετο αριθμό, που είναι δύσκολο πρόβλημα.