Дигитални потпис

Владимир Божовић

Природно-математички факултет
Подгорица

КРИПТОГРАФИЈА

Шта је дигитални поптпис?

- Криптографски алгоритми попут AES, RSA или ЕлГамал (симетрични или асиметрични) рјешавају проблем сигурне (тајне) комуникације преко несигурног канала.
- Дигитални потпис рјешава другу врсту проблема, сличну оној коју рјешава "традиционални" потпис.
- Дигитални потписом желимо да утврдимо несумњивост да је особа X заиста креирала одређени документ D, и нико други.
- Дигитални потписом постижемо и сигурносни циљ НЕПОРЕЦИВОСТИ (nonrepudation) - односно да је особа X заиста потписала документ D са датим садржајем.

Концепт дигиталног потписа

Слично, као код асиметричног крипто-система, и у алгоритмима за дигитални потпис имамо

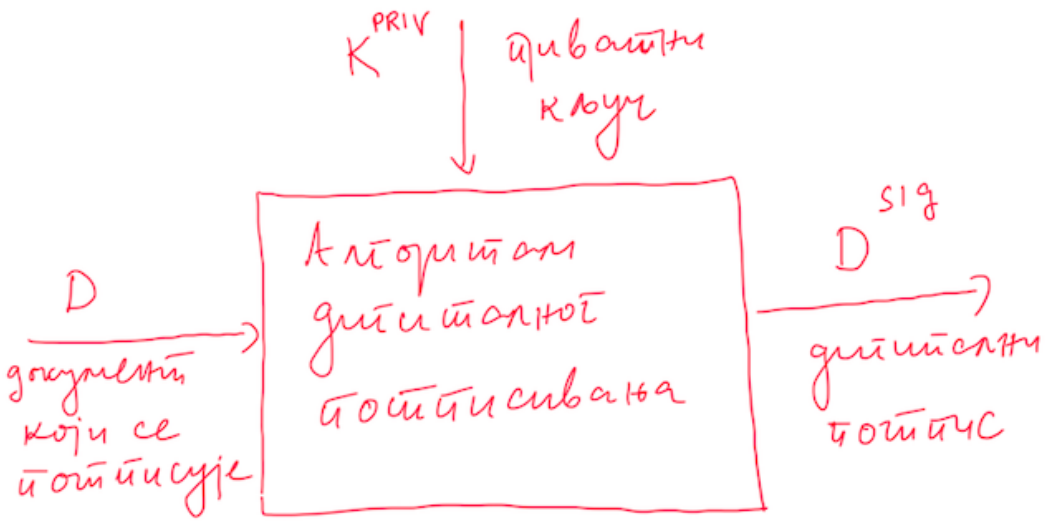
K^{priv} Тајни кључ којим се потписује документ.

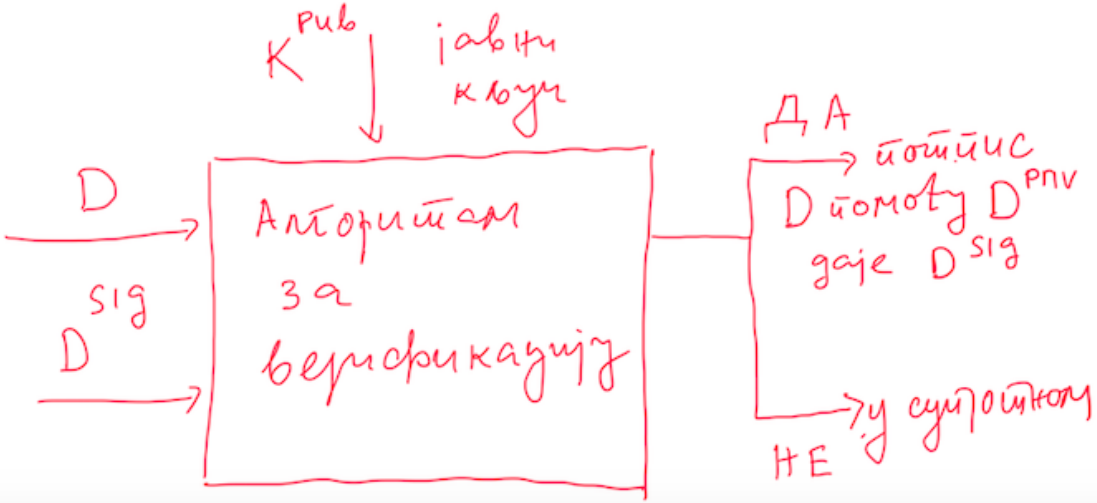
K^{pub} Јавни кључ којим се верификује документ.

Sign Алгоритам дигиталног потписа, чији је улаз документ D и K^{priv}, а излаз потпис документа D^{sig}.

Ver Верификациони алгоритам чији је улаз документ D, D^{sig} као и јавни кључ K^{pub}. Излаз овог алгоритма је "Тачно" ако је документ D повезан са K^{priv}, а "Нетачно" у супротном.

Концепт дигиталног потписа





Сигурност сигиталног потписа

Кад сматрамо да је дигитални потпис сигуран?

1. Ако је дат K^{pub}, нападач не би требало да на изводљив начин дође до K^{priv}.
2. Ако је дат K^{pub}, листа докумената $D_1, \ldots, D_n$ са потписима $D_1^{\text{sig}}, \ldots, D_n^{\text{sig}}$, нападач не би требало да на изводљив начин дође да потписа било ког новог документа D који није у низу $D_1, \ldots, D_n$.

Услов 2 прави суштинску разлику у односу на алгоритме енкрипције у којима нападач може да направи колико жели нових парова (порука, криптограм) с обзиром да познаје јавни (енкриптивни) кључ.

УСПОСТАВЉАЊЕ СИСТЕМА

Боб: објављује јавне податке (N, e). Тајни подаци које чува за себе су прости бројеви p, q, као и тајни декриптивни експонент d, такав да $ed \equiv 1 \pmod{(p-1)(q-1)}$.

ПОТПИСИВАЊЕ

Боб: шаље Алиси пар $(D, SIG(D))$ гдје је $SIG(D) \equiv D^d \pmod{N}$.

ВЕРИФИКАЦИЈА

Алиса: рачуна $S' = SIG(D)^e \pmod{N}$.
Уколико је $S' = D$, онда је верификација успјела.

Колико је тешко фалсификовати RSA дигитални потпис

Да би Ева фалсификовала Бобов потпис морала би бити у стању да ријеши бар један од проблема

- Да факторише број N и тиме нађе $\phi(N)$, па потом ријеши конгруенцију
$$ex \equiv 1 \pmod{\phi(N)}$$
како би нашла Бобов тајни кључ d.
- да за документ D нађе његов $e-$ти коријен по модулу N, односно неки број S из $\mathbb{Z}_N$ такав да
$$S^e \equiv D \pmod{N}.$$
Примјетимо да је што је заправо једнако тешко као само разбијање RSA система.

ЕлГамал дигитални систем

- Док је "транзиција" RSA криптосистема у RSA дигитални потпис, то није случај са ЕлГамалом.
- Алгоритам ЕлГамал дигиталног потписа је објављен 1985, његова унапријеђена верзија DSA 1991.
- Дигитални потписом желимо да утврдимо несумњивост да је особа X заиста креирала одређени документ D, и нико други.

УСПОСТАВЉАЊЕ СИСТЕМА

Боб: бира велики прост број p и примитивни коријен g по модулу p. Такође, бира и тајни експонент a између 1 и p, а објављује $A = g^a \pmod{p}$.

ПОТПИСИВАЊЕ

Боб: потписује документ D, заправо број који задовољава $1 < D < p$. Потом бира (једнократни) експонент k који се налази између између 1 и p. Рачуна

$$S_1 \equiv g^k \pmod{p} \text{ и } S_2 \equiv (D - aS_1)k^{-1} \pmod{p-1}.$$

Дакле, Боб шаље (D, S_1, S_2) Алиси.

ВЕРИФИКАЦИЈА

Алиса: Алиса испитује да ли је

$$A^{S_1} S_1^{S_2} \pmod p = g^D \pmod p.$$

Провјера валидности ЕлГамал потписа

$$A^{S_1} S_1^{S_2} \equiv g^{aS_1} g^{eS_2} \equiv g^{aS_1 + k(D - aS_1)k^{-1}} \equiv g^D \pmod p.$$

Примјетимо да је S_2 одабрано по модулу $p-1$, па како је $g^{p-1} \equiv 1 \pmod p$, то значи да S_2 можемо замијенити било којом вриједношћу која је конгруентна њој по модулу $p-1$.

Како Ева може фалсификовати Бобов потпис?

- Најефикаснији начин фалсификовања Бобовог потписа би било откривање његовог тајног експонента a, уколико је у стању да ријеши ДЛОГ проблем $A \equiv g^a \pmod{p}$.
- Међутим, то није једини начин. Уколико је Ева у стању да нађе бројеве x и y који за неки одабрани D задовољавају

$$A^x x^y \equiv g^D \pmod{p},$$

онда би Ева била у стању да фалсификује потпис.

Како потписати велике документе?

- Као што смо видјели, путем неког од алгоритама дигиталног потписа у стању смо да "потпишемо" само малу количину података, рецимо b битова, гдје је b између 80 и 1000.
- Према томе, прилично је неефикасно потписивање великог дигиталног документа D, како у смислу времена, тако и у смислу величине резултирајућег дигиталног потписа.

Хеш функције и дигитални потпис

- Уобичајено рјешење за претходно наведени проблем је коришћење хеш фунције, лако израчунљиве функције која даје отисак документа било које величине на k битова.

$$\text{Хеш(документ D произвољне дужине)} \to \{0,1\}^k,$$

а за коју је врло тешко наћи оригинал x ако је дато Хеш(x).

- Хеш функција мора да задовољава општије својство - да је тешко наћи пар који потврђује неинјективност ове функције, односно, тешко је наћи D и D' такве да

$$\text{Хеш}(D) = \text{Хеш}(D').$$

- Ово је пут како да ријешимо претходно наведени проблем. Дакле, умјесто потписивање документа D, Боб ће потписивати Хеш(D). За верификацију, Алиса рачуна са Хеш(D) умјесто са D.

Хвала на пажњи :)