RSA алгоритам

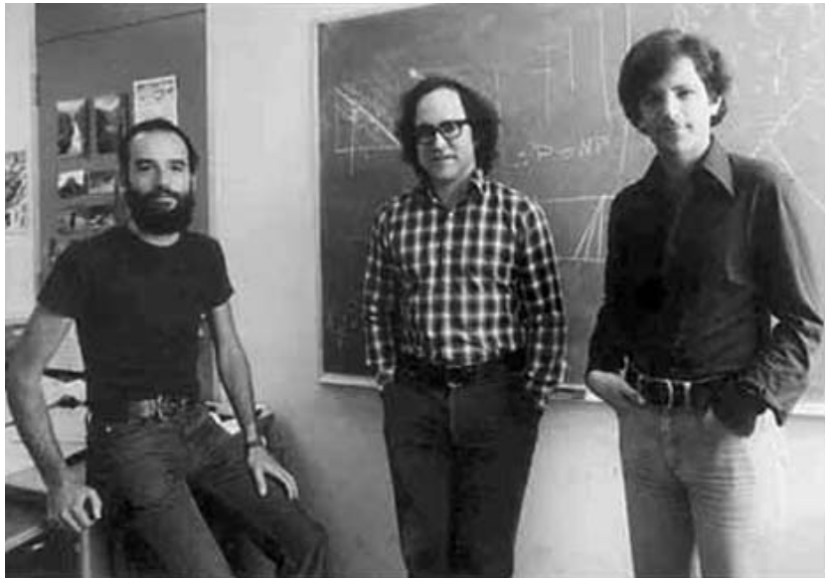
Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Први асиметрични крипто-систем

Након што су Дифи и Хелман, 1976. године у свом утицајном научном раду представили идеју асиметричне криптографије, започела је нова ера у криптографији.



- Почела је потрага за сличним, алгоритмима асиметричне криптографије.
- Ривест, Шамир и Адлеман су 1977. представили алгоритам (RSA) чија се употреба веома брзо проширила.

Математичка припрема за RSA

Математичка основа RSA алгоритма је веома једноставна и дјелимично заснована на следећој теореми.

Теорема

Нека су p и q прости бројеви и нека је

$$g = (p-1, q-1).$$

Тада је

$$a^{\frac{(p-1)(q-1)}{g}} \equiv 1 \pmod{pq},$$

за свако a које задовољава $(a, pq) = 1$.

Математичка припрема за RSA

Као што знамо, Дифи-Хелман проблем и ЕлГамал почивају на тежини проблема рјешавања једначине $a^x \equiv b \pmod{p}$, гдје су a, b, p познате, а x непозната величина.
На другој страни, RSA почива на тежини проблема типа

$$x^e \equiv c \pmod{N},$$

гдје су e, c, N познате, а x непозната величина.

Теорема

Нека је p прост број, а $e \geq 1$ цио број за који вриједи $(e, p-1) = 1$. Тада конгруенција

$$x^e \equiv c \pmod{p}$$

има јединствено рјешење $x \equiv c^d \pmod{p}$ гдје је $de \equiv 1 \pmod{p-1}$.

Основна теорема RSA алгоритма

Следећа теорема представља срце RSA алгоритма и у директној вези је са претходном теоремом.

Теорема

Нека су p и q прости бројеви, а $e \geq 1$ цио број за који вриједи $(e, (p-1)(q-1)) = 1$. Тада конгруенција

$$x^e \equiv c \pmod{pq}$$

има јединствено рјешење $x \equiv c^d \pmod{pq}$ гдје је $de \equiv 1 \pmod{(p-1)(q-1)}$.

Боб и Алиса у RSA сценарију

Боб: Бира просте бројеве p и q
Бира експонент за енкрипцију e
тако да **нзд**$(e, (p-1)(q-1)) = 1$.
Објављује $N = pq$ и e.

Алиса: Бира текст поруке m.
Користи Бобов јавни кључ (N, e)
за рачунање $c \equiv m^e \pmod{N}$.
Шаље криптовани поруку c Бобу.

Боб: Рачуна d који задовољава
$ed \equiv 1 \pmod{(p-1)(q-1)}$.
Рачуна $m_1 = c^d \pmod{N}$.
Тада је m_1 једнако поруци m коју је послала Алиса.

Сигурност RSA крипто-система

Поставка Нека су p и q велики прости бројеви, $N = pq$, а e и c цијели бројеви.

Проблем Ријешити конгруенцију $x^e \equiv c \pmod{N}$ за промјенљиву x.

Лако Боб, ако зна вриједности p и q, лако налази x као што је објашњено у претходно датој теореми.

Тешко Ева, ако не зна p и q, нема довољно добар начин за налажење x.

Подјела Рјешавање $x^e \equiv c \pmod{N}$ је лако за неког ко посједује додатну информацију а тешко за остале.

Почетничке замисли разбијања RSA

- Сигурност RSA се темељи на чињеници тешког факторисања броја $N = pq$.
- Да ли је могуће сазнати $\phi(N) = (p-1)(q-1)$ знајући N?
- Множењем $(p-1)(q-1)$ добијамо

$$(p-1)(q-1) = pq - (p+q) + 1 = N - (p+q) + 1.$$

- Уколико Ева зна вриједности $p+q$ і pq, тада једноставно долази до бројева p и q рјешавајући квадратну једначину

$$X^2 - (p+q)X + pq.$$

Увијек дође неко трећи...

(Wo)man in the middle attack

Pam Wellington

Да ли знате са ким причате?

Подсјетимо се Дифи-Хелмановог протокола. Нека је дато поље $\mathbb{Z}_p$, као и његов генератор α.

Алиса бира a, рачуна $A = \alpha^a$ и шаље Бобу.
Боб бира b и шаље $B = \alpha^b$ Алиси.

Ева пресреће поруке, бира своје c
и шаље Алиси и Бобу $\tilde{A} = \alpha^c$.

Алиса, мислећи да разговара са Бобом, има кључ са Евом

$$k_{AE} \equiv A^c \pmod{p} \equiv \alpha^{ac} \pmod{p},$$

а Боб, мислећи да комуницира са Алисом, има заједнички кључ са Евом

$$k_{BE} \equiv B^c \pmod{p} \equiv \alpha^{bc} \pmod{p}.$$

Како заобићи RSA?

Алиса се "пеца" на Евин изазов

Претпоставимо да је Ева убиједила Алису да декриптује неку "случајну" поруку у циљу потврде њеног идентитета. (За ову ситуацију се каже да Ева има приступ RSA ораклу).

Ева "пакује" Бобову поруку и шаље Алиси

Ева пресреће Бобову поруку $c = m^e$ и шаље Алиси "препакован" израз за декрипцију

$$c' \equiv k^e c, \text{ гдје је } k \text{ произвољно изабран број.}$$

Алиса декриптује c' и враћа Еви

$$(c')^d \equiv (k^e c)^d \equiv (k^e m^e)^d \equiv km \pmod{N}$$

Како заобићи RSA?

Боб шаље исту поруку на више адреса

Претпоставимо да Боб енкриптује исту поруку m са два експонента e_1 и e_2 и шаље их различитим субјектима, Алиси и Ани. Ева пресреће двије поруке

$$c_1 = m^{e_1} \pmod{N} \quad \text{и} \quad c_2 = m^{e_2} \pmod{N}$$

Ева је "happy" ако је **нзд**(e_1,e_2)=1

Ева налази коефицијенте u, v линеарне комбинације

$$ue_1 + ve_2 = \textbf{нзд}(e_1, e_2).$$

Ева потом рачуна

$$c_1^u c_2^v \equiv (m^{e_1})^u (m^{e_2})^v \equiv m^{ue_1+ve_2} \equiv m^{\textbf{нзд}(e_1,e_2)} \pmod{N}$$

Параметри RSA и сигурносна питања

- Тајни кључ d не смије имати мали број бита. Показује се да дужина тајног кључа мора бити најмање $0.3t$ гдје је t број бита модула N.
- Због величине тајног кључа d, процес декрипције траје дуго.
- Зато се на специфичан начин користи идеја кинеске теореме о остацима.

Хвала на пажњи :)