Computer Science and Information Systems ?(?):1–6 DOI: N/A

RSA algoritam za šifrovanje i dešifrovanje podataka

Danijel Rujević

Matematički fakultet,Studentski trg 16
11000 Belgrade, Serbia
rujevic@gmail.com

Abstract. Upotreba i opis RSA algoritma za šifrovanje i dešifrovanje podataka.

Keywords: RSA, asimetrična kriptografija, šifarski sistem, sistem sa javnim ključem.

Table of Contents

1. Uvod

Ovaj sistem dobio je ime po trojici svojih pronalazača (Ron Rivest, Adi Shamir, Leonard Adleman). Rad su prvi put objavili javno 1977. Od 1973. Engleski matematičar Clifford Cox razvijao je ekvivalentan sistem ali je njegov rad čuvan u strogoj tajnosti čak do 1997.
RSA je jedan od prvih praktično izvodljivih šifarskih sistema sa javnim ključem. U ovakvom sistemu ključ za šifrovanje je javni i razlikuje se od ključa za dešifrovanje koji se čuva u tajnosti. Odatle naziv asimetrična kriptografija.

2. Osnovni pojmovi u kriptografiji

Otvoren tekst je poruka koju treba poslati (npr. ZDRAVO).
Šifrat je šifrovana poruka (npr. XQABER).
Šifrovanje je transformacija otvorenog teksta u šifrat.
Dešifrovanje je inverzna transformacija šifrata u otvoren tekst.
Kodiranje je transformacija otvorenog teksta u niz cifara ili bita npr. A $\rightarrow$ 0, B $\rightarrow$ 1 ... Z $\rightarrow$ 25, onda se kodira otvoren tekst ZRDAVO $\rightarrow$ 25 3 17 0 21 14.
Dekodiranje transformiše niz cifara ili bita u polazni tekst.
Procesi koriranja i dekodiranja nisu tajni.
Lančana šifra transformiše otvoren tekst simbol po simbol, odnosno najčesšće bit po bit.
Blokovska šifra primenjuje se na simbole otvorenog teksta grupisane u blokove (mogu biti bigrami - parovi slova, trigrami - trojke slova...).
Šifra premeštanja premešta (premutuje) slova (znakove, bitove).
Šifra zamene zamenjuje slova (znakove, bitove) drugim, ne menjajući im redosled.
Kombinovana šifra primenjuje naizmenično premeštanja i zamene.
Šifarski sistem (ili samo sistem) je par čiji su elementi algoritam za šifrovanje i algoritam za dešifrovanje.
Simetrični sistem podrazumeva upotrebu istog tajnog ključa za šifrovanje i dešifrovanje. *Ključ* je parametar kojim se bira konkretna šifarska transformacija u okviru izbranog sistema. Dva korisnika unapred moraju dogovoriti koji će ključ koristiti.
Asimetričan sistem (sistem sa javnim ključem) podrazumeva da svaki korisnik objavi svoj ključ za šifrovanje, a da u najvećoj tajnosti čuva ključ za dešifrovanje.
Kriptoanaliza je proces pomoću koga neprijatelj pokušava da šifrat transformiše u odgovarajući otvoren tekst, ne znajući ključ.
Dekriptiranje je uspešna kriptoanaliza (makar i delimično). Akteri u sistemima kriptoanalize su *Alice* (pošiljalac šifrovane poruke), *Bob* (primalac) i *Eve* (prisluškuje vezu i pokušava da pročita šifrovanu poruku).

3. Sistemi sa javnim ključem

U simetričnom šifarskom sistemu, ako znamo algoritam šifrovanja i ključ za šifrovanje, onda možemo lako da odredimo algoritam za dešifrovanje tj. ključ za dešifrovanje u polinomijalnom vremenu.
Šifarski sistem sa javnim ključem je sistem u kome svako zna algoritam šifrovanja, ali se ne zna polinomijalni algoritam za određivanje ključa za dešifrovanje polazeći od ključa za šifrovanje.
Jednosmerna funkcija. Neka su X, Y skupovi i neka je $f : X \longrightarrow Y$ funkcija. Za dato $x \in X$ lako je izračunati $f(x)$. Za dato $y \in Y$ tesko je odrediti x tako da je $y = f(x)$.
Primer: Kada se u računaru regisruje *lozinka* faktički se zapisuje *f(lozinka)*, gde je f jednosmerna funkcija. Prilikom prijavljivanja unosi se lozinka za koju računar izračunava f i to upoređuje sa zapisanom vrednošću.
Prividno jednosmerna funkcija (trapdoor function) je invertabilna jednosmerna funkcija f, za koju je određivanje vrednosti f^{-1} lako uz poznavanje potrebne informacije (trapdoor).
Najvažnije primene kriptografije sa javnim ključem su:

1. Usaglašavanje ključa za simetrični šifarski sistem,

2. Digitalni potpis.

Dok se retko koriste za šifrovanje celih poruka, jer su sporiji od simetričnih sistema.

4. Opis sistema i postupak algoritama

U osnovi sistem se sastoji od tri koraka (algoritma): generisanje ključa, enkriptovanje i dekriptovanje.
Najpre Bob bira dva prosta broja sa oko 150 dekadnih cifara. Zatim izračunava $n = pq \approx 10^{300}$ i
$\varphi(n) = (p - 1)(q - 1)$. Potom određuje neki broj e takav da je $nzd(e,\varphi(n)) = 1$ i izračunava $d \equiv e^{-1} \pmod{\varphi(n)}$. Javno se objavljuju (n, e), dok se d, p, q čuva u tajnosti (p i q se više ne koriste pa se mogu obrisati). Ovaj postupak se ne obavlja često, može jednom godišnje.
Neka je M poruka koju Alice želi poslati Bobu. Ako je ta poruka veća od n, onda se razbija na blokove koji se mogu predstaviti brojevima manjim od n. Alice pronalazi Bobov javni par (n, e). Ona izračunava $C \equiv M^e \pmod{n}$, to je prividno jednosmerna funkcija. Bobu šalje C.
Bob izračunava $C^d \pmod{n}$ i dobija M (tj. $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^1 \equiv M$). U slučaju da Eve presretne poruku C, ona to ne može iskoristiti ako ne zna Bobov parametar d.

4.1. Primer upotrebe

Bob bira brojeve $p = 17$, $q = 41$. Zatim izračunava $n = pq = 17 \cdot 41 = 697$ i $\varphi(n) = (17 - 1) \cdot (41 - 1) = 16 \cdot 40 = 640$. Zatim bire $e = 33$ (uzajamno prost sa 640) i izračunava $d \equiv 33^{-1} \pmod{640} = 97$. Nakon toga Bob javno ojavljuje $n = 697$, $e = 33$.
Alice želi da koristi $C = aP + b \pmod{26}$ sa ključem, $C \equiv 7P + 25 \pmod{26}$ da bi Bobu poslala dugačku poruku. Ona kodira ključ brojem $7 \cdot 26 + 25 = 207$, pa izračunava šifrat $207^e \pmod{n} = 207^{33} \pmod{697}$. Za ovu operaciju se služi algoritmom stepenovanja kvadriranjem:
$33 = 32 + 1$,
$207^2 \equiv 332$,
$207^4 \equiv 332^2 \equiv 98$,
$207^8 \equiv 98^2 \equiv 543$,
$207^{16} \equiv 543^2 \equiv 18$,
$207^{32} \equiv 18^2 \equiv 324$.
Pa je $207^{33} \equiv 207^{32} 207 \equiv 324 \cdot 207 \equiv 156 \pmod{697}$.
Alice šalje Bobu broj 156. Eve koja prisluškuje teško može na osnovu toga izračunati 207. Bob prima poruku 156 i izračunava $156^d \pmod{n} = 156^{97} \pmod{697} = 207$. Nakon toga Bob dekodira poruku $207 = 7 \cdot 26 + 25$. Poslednji korak nije deo RSA algoritma.

5. Složenost sistema

Zašto je teško odrediti d na osnovu e i n? Kao što je rečeno, $d \equiv e^{-1} \pmod{\varphi(n)}$. Određivanje inverza je efikasno (polinomijalna složenost). Odredjivanje $\varphi(n)$ je teško ako znamo samo n, jer je potrbno rastaviti n na činioce, za ovaj posao znaju se subeksponencijalni, ali ne i polinomijalni algoritmi.
Predpostavimo da znamo n, tada je poznavanje $\varphi(n)$ za polinomijalno vreme ekvivalentno sa pronalazenjem p i q.
Dokaz: Ako znamo n, p, q, onda je $\varphi(n) = (p - 1)(q - 1)$, što se može izračunati za $O(\log^2 n)$.
Predpostavimo sada da znamo n i $\varphi(n)$. Tada je $x^2 + (p + q)x + pq = (x - p)(x - q)$. Znači brojevi p i q se mogu brzo odrediti rešavanjem kvadratne jednačine $x^2 + (\varphi(n) - n - 1)x + n = 0$. Izrač unavanje kvadratnog korena (koji nije

obavezno kvadrat celog broja) i obavljanje ostalih aritmetičkih operacija zahteva vreme $O(\log^3 n)$. ☺
Prema prethodnom odredjivanje $\varphi(n)$ je podjednako teško kao i faktorizacija.

5.1. Preporuke

Stvari o kojima treba voditi računa su:

1. treba birati p i q tako da $nzd((p - 1),(q - 1))$ bude mali broj,
2. oba prosta broja p i q treba da imaju veliki prost činilac,
3. brojevi p i q ne treba da budu previše blizu jedan drugom, s druge strane odnos većeg i manjeg je obično manji od 4. Postoje specijalni algoritmi za faktorizaciju, koji mogu da se iskoriste ako nije ispštovana bilo koja od ove tri preporuke,
4. obično je e relativno malo, da bi se smanjilo vreme šifrovanja (recimo često se uzima da bude $e = 3$).

6. Praktična primena

Svaki korisnik ima svoj par: Alice ima (n_A, e_A), Bob ima par (n_B, e_B), koji su javni isvako im može pristupiti (mogu biti na ličnom sajtu, "imeniku" na nekom poznatom sajtu...). d_A i d_B su privatni ključevi i samo vlasnici imaju pravo pristupa.
Kada Alice šalje Bobu poruku M ona izračunava $M^{e_B} \pmod{n_B}$. Bob za dešifrovanje koristi svoj privatni ključ d_B i tako dobija M.
Za ličnu upotrebu se obično koriste brojevi n od *1024-bita*, odnosno $n \approx 10^{308}$. Za komercijalnu upotrebu se obično koriste brojevi n od *2048-bita*, odnosno $n \approx 10^{617}$. Za važne potrebe se obično koriste brojevi od *4096-bita* odnosno $n \approx 10^{1234}$. Oko 1990. godine bilo je uobičajeno da se koriste *512-bitni* što je približno 10^{154}. Krajem 2009 broj veličine *768-bita* je rastavljen na činioce u okviru konkursa firme RSA. Vreme potrebno za faktorisanje *663-bitnog* broja, sa istog konkursa 2005. godine na jednom računaru tip Opteron 2.2GHz iznosilo bi oko 75 godina. Napredovanjem tehnologije i brzine računara vreme za faktorisanje se smanjuje, pa se u skladu sa tim povećava i broj n.
Kada koriste simetričan šifarski sistem, Alice i Bob moraju unapred dogovoriti zajednički ključ. To stvara poteškoće: potrebno je da se nadju i lično razmene ključ (nepraktično) ili da neobezbeđenom linijom da pošalju ključ (nesigurno). Na primeru RSA vidimo da kriptografija sa javnim ključem rešava problem simetrične kriptografije. S obzirom na brzinu samog algoritma RSA se može koristiti za celokupnu razmenu poruka, mada je to nepraktično. Najčešće se se RSA iskoristi za razmenu ključa, a zatim za razmenu poruka se koristi AES ili neki sličan sistem.

Reference

1. Wikipedia - RSA (cryptosystem)
2. Wikipedia - RSA numbers. [Online]. Available: http://en.wikipedia.org/wiki/RSA_numbers
3. Zivkovic Miodrag, P.D.: Kriptografija (2010)