RSA

RSA šifra bola svojho času prevratný vynález. Vytvorili ju autori Rivest, Shamir a Adleman, takže názov je vytvorený z ich mien. Prečo je taká prelomová, vysvetlím na príklade.

Substitučné šifry sú fajn, ale bežne sa veľmi nepoužívajú. Dôvod je, samozrejme, spojený s ich bezpečnosťou. Jednorazová správa, ktorú si vymenia dve osoby, ktoré sa vopred zoči-voči dohodli na šifrovacom kľúči, je zabezpečená naozaj dobre. V iných situáciách už to tak nemusí byť.

Príklad použitia

Predstavme si hypotetickú situáciu. Starosta mesta pošle svojho špióna, aby sa infiltroval k nepriateľovi. Bude od neho chcieť dostávať veľa správ v priebehu možno až niekoľkých rokov. V tomto čase sa špión nemôže vracať do svojho mesta, aby si preberal nové šifrovacie kľúče, používať dlhodobo ten istý je nebezpečné a posielať kľúče po tretej osobe tiež nebude dobrý nápad.

Riešením je asymetrické šifrovanie. Aby sme pochopili, čo je asymetrické šifrovanie, vysvetlím najprv opačný pojem. Symetrické šifrovanie je také, pri ktorom vieme zo šifrovacieho kľúča ľahko odvodiť dešifrovací. Pozrite si, napríklad, stránku Šifry dole, kde vieme ľahko z kľúča pre Vigenèrovu šifru odvodiť opačný kľúč. Takže, ak niekto vie, ako bola správa zašifrovaná, dokáže ju aj ľahko dešifrovať. Naopak asymetrické šifrovanie, ktorého najznámejším príkladom je RSA šifra, má tú vlastnosť, že aj keď každý dokáže správu zašifrovať, rozšifrovať ju dokáže len ten, kto šifru vytvoril. Dešifrovací kľúč sa nedá odvodiť z kľúča šifrovacieho.

Konkrétne, pri RSA šifre máme dva kľúče, ktoré môže poznať hocikto – verejný kľúč a spoločný kľúč, ktorý v reálnych situáciách býva až niekoľko sto-ciferné číslo. Tieto dva kľúče úplne stačia k zašifrovaniu správy. Tretí -dešifrovací kľúč sa nazýva súkromným a tento pozná iba jediná osoba.

Špión: *Mám novinky.*

Starosta: *19, 10602637.*

Špión: *huhuk dudox ibiqp tvvcj srggx.*

Ako špión zašifroval svoju správu? Podľa spoločného kľúča zistil, že môže zašifrovať štvor- až päťpísmenkové správy. Takže svoju správu rozdelil na Garma,donuž,nemá,gene,rálov. Každý kúsok správy zašifroval napríklad pomocou aplikácie

nižšie na tejto stránke.

Starosta použije svoj súkromný kľúč 143557, ktorý nikdy nikomu neukázal a správu rozšifruje.

Tvorba kľúčov pre RSA šifru

Z dôvodu bezpečnosti je ideálne, ak vieme pred každou poslanou správou vytvoriť nové kľúče tak, ako to urobil starosta v našom príklade. Základom sú veľké prvočísla. Čím väčšie, tým lepšie. Na ich hľadanie poslúži nasledujúca aplikácia. Stačí zadať nepárne číslo menšie ako päťdesiata tretia mocnina dvoch, čo je asi 9 biliárd (15 núl za deviatkou). Toto obmedzenie je tu z technických dôvodov. Chceme totiž získať výsledok v rozumnom čase. Aplikácia nájde najbližšie prvočíslo menšie od zadaného čísla. Zaujímavé čítanie o prvočíslach nájdete tu.

Nájdi prvočíslo!

Prvočísla:

Do okienok dole zadajte tri prvočísla. Z prvých dvoch sa vytvorí spoločný kľúč. Tieto majú byť čo možno najväčšie. Tretie prvočíslo bude verejným kľúčom. Toto prvočíslo nemusí a ani nemá byť príliš veľké. Nezľaknite sa, ak vás program vyzve na zmenu tohto verejného kľúča. Dôvod nájdete nižšie v poznámkach.

Prvočíslo 1:

Prvočíslo 2:

Verejný kľúč:

Kľúče

Spoločný kľúč:

Verejný kľúč:

Súkromný kľúč:

RSA šifrovanie

Z predchádzajúcej aplikácie si treba uložiť tri kľúče - dva sa zverejnia, tretí zostane utajený. Prvočísla, z ktorých vznikol spoločný kľúč, pre istotu úplne zabudneme. Nasledujúca aplikácia už priamo šifruje správu vo forme čísla alebo vo forme reťazca z písmen, ktoré program prevedie na číslo. V oboch prípadoch môžeme šifrovať iba správy menšie ako spoločný kľúč.

Vstup:

Kľúč (verejný alebo súkromný):

Spoločný kľúč:

Šifruj

Výstup:
Pri tomto spoločnom kľúči možno posielať ľubovoľné - písmenkové správy. Ak je prvé písmenko zo začiatku abecedy,

možno aj o jedno písmenko dlhšie.

Poznámky

- Bezpečnosť RSA šifry je založená na nemožnosti nájsť v dostupnom čase prvočísla, z ktorých vznikol spoločný kľúč. Výpočtovo je to podobné ako Nájdi prvočíslo. Už 15-miestne zadania chvíľu trvajú. Ak vynásobíme dve takéto čísla, dostaneme až 30-miestne číslo. Nájsť jeho delitele netrvá dvakrát toľko, ale približne 1 000 000 000 000 000-krát toľko. Čiže, ak nájsť deliteľa 15-miestneho čísla trvá 1 sekundu, nájsť deliteľa 30-miestneho čísla by trvalo asi 31 miliárd rokov. Vážne, prepočítajte si to sami, ak neveríte. Obyčajný smartfón, na ktorom tieto výpočty pravdepodobne vykonávate, ale nie je vrchol súčasnej technológie, takže 30-miestny spoločný kľúč v súčasnosti nemožno považovať za bezpečný.
- Nájdi prvočísla funguje tak, že testuje deliteľnosť daného čísla všetkými nepárnymi číslami od 3 až do odmocniny z tohto čísla. Ak žiadneho deliteľa nenájde, výsledkom je dané číslo. Ak nájde deliteľa, zmení zadané číslo na číslo o dve menšie (aby bolo stále nepárne). Toto robí, až kým nenájde prvočíslo.
- Hľadanie kľúčov je matematicky trošku komplikovanejšie, ale zato technicky rýchlejšie. Preto tu pracujem aj s väčšími číslami. Vy zadáte tri prvočísla ideálne získané v predchádzajúcom kroku. Program prvé dve vynásobí (tu môže vzniknúť viac ako 16miestne číslo) - to bude spoločný kľúč, tretie prvočíslo bude verejný kľúč. Výpočet súkromného čísla vo veľmi zjednodušenej podobe prebieha asi takto: najprv vypočítame najmenší spoločný násobok čísel p-1 a q-1, kde p a q sú prvočísla, z ktorých vznikol spoločný kľúč. Ak prvočísla boli 7 a 13,

nsn(6,12) = 12. Verejný kľúč musí byť s týmto násobkom nesúdeliteľný, preto vás niekedy program vyzve na výber iného verejného kľúča. Navyše by nemal byť väčši ako tento nsn. V našom minipríklade môžeme ako verejný kľúč použiť iba 5, 7 alebo 11. Potom určíme *x* ako to číslo, ktoré po vynásobení verejným kľúčom dá zvyšok 1 po delení spomínaným najmenším spoločným násobkom. Ak nsn bolo 12 a verejný kľúč 5, súkromný bude tiež 5, pretože 5 • 5 = 25 a to dáva zvyšok 1 po delení dvanástimi. Z tohto krátkeho vhľadu vyplývajú dve dôležité veci. Po prvé, súkromný kľúč sa nedá vypočítať, ak nevieme, z ktorých prvočísel vznikol spoločný kľúč. Po druhé súkromný a verejný kľúč sú navzájom zameniteľné, takže je na nás, ktorý zverejníme a ktorý zostane utajený. (Ak zašifrujeme správu súkromným kľúčom, verejným ju môžeme odšifrovať.)

- Pri samotnom šifrovaní používam niekoľko matematických trikov, takže výpočty sú naozaj rýchle. Program rozoznáva, či je vstup číslo alebo nie. Číslo šifruje tak, že ho umocní na verejný kľúč a nájde zvyšok výsledku po delení spoločným kľúčom. Pri samotnom umocňovaní používam podobný princíp ako v tomto príspevku na blogu. Dešifrovanie prebieha presne tak isto ako šifrovanie, ibaže vy namiesto verejného kľúča vložíte súkromný.
- Šifrovanie slova prebieha tak, že slovo je zakódované do jedného čísla v 26tkovej číselnej sústave s ciframi A=0, B=1, ... Z=25. Je to výhodnejšie ako šifrovať každé písmeno zvlášť, pretože dĺžka jednotlivo šifrovanej správy môže byť rôzne veľká. Vyplýva z toho ale jeden dôsledok, na ktorý treba myslieť. Nesmieme posielať slovo začínajúce písmenom A, pretože to sa zakóduje ako číslo typu 0105 = 105, takže to A na začiatku sa stratí. Preto špión v úvodnom príklade nerozdelil slovo generalov na gener,alov, ale na gene,ralov.