eS-technic

RSA

jak to * funguje

funkční popis RSA šifrování s vysvětlením výpočtu a praktickým příkladem

v 1.0

RSA je označení pro způsob šifrování, které se dnes hojně využívá v elektronické komunikaci, bankovnictví, telekomunikacích a má potenciál využití ve všech odvětvích lidské činnosti. Je to extrémně účinné šifrování a při vhodném použití je nemožné ho překonat. A pokud je ho potřeba překonat, je to náročné. A pokud je to náročné, není možné to plošně využívat. A pokud je to potřeba plošně využívat (např. pro dešifrování komunikace mezi teroristy), je to drahé ... a pokud se použije RSA-2048, tak náklady na dešifrování pár slov mohou dosáhnout tisíce $. Dešifrování nákupního seznamu uloženého v zabezpečené složce je tak pro hackery jistě možné, ale náklady na dešifrování dosáhnou HDP menšího státu a nebude to hlavně do druhého dne.

Celá problematika RSA tkví v tom, že lze docela dobře a jednoduše násobit prvočísla mezi sebou, ale podstatně složitější je nějaké číslo na prvočísla rozdělit. Např. šifra RSA-2048 používá číslo v řádu 2048 bitů. Takové číslo si lze představit jednoduše, tvoří ho 617 číslic. Při uvážení, že miliardu tvoří 10 číslic, tak číslo s 617 číslicemi ani nemůže mít nějaký název, jednoduše proto, že je lidsky nepoužitelné. I jeho faktorizace (rozdělení na prvočísla = prvočinitele) je v reálném čase zatím s použitím současné techniky nepředstavitelná.

Vynásobit prvočísla jako jsou např. 191 * 271 = 51761 dokáže každá kalkulačka. Rozdělit ale libovolné číslo na dvě prvočísla je trochu oříšek. Tak např. číslo 41989 ...

Dobře, tak zkusíme jednodušší, třeba 924. Když nevím hned, zkouším dělit postupně všemi prvočísly, od nejmenšího. Sudé číslo číslem 2 a liché začínám číslem 3. Když to nejde, postupně zvyšuji 5, 7, 11, 13, 17, 19, ...

924 : 2 = 462

462 : 2 = 231

231 : 3 = 77

77 : 7 = 11

Číslo 924 lze rozložit tedy na součin prvočinitelů 2 * 2 * 3 * 7 * 11.

Výše uvedené číslo 41989 = 199 * 211 ... to ale chvilku trvá. A s číslem v řádu 2048 bitů je to už časově neúnosné.

RSA šifrování probíhá tak, že se zpráva, která může obsahovat čísla, písmena, obrázek nebo dokument zašifruje matematickým způsobem. Jelikož jsou všechna tato data v paměti počítače uložena v podobě souboru čísel, není problém s libovolnými daty pracovat jako s čísly. Tedy je sčítat, násobit dělit, zaokrouhlovat. Takový soubor se zašifruje dále uvedeným způsobem pomocí dvou obrovských čísel, které tvoří soukromý klíč. Ten vytvořil a zná jen odesílatel. Pak může putovat zašifrovaný soubor dat nezabezpečeným prostorem k adresátovi bez obav, že by mohl být jednoduše někým neoprávněným získán a dešifrován. Adresát obdrženou zprávu dešifruje pomocí veřejného klíče, který tvoří také dvojice obrovských čísel. Veřejný klíč ale musí adresát od odesílatele dostat předem. Neznamená to, že veřejný klíč je veřejně dostupný, ale je určen jen pro "zasvěcené" adresáty, kterým je odesílaný soubor dat určen. Pomocí veřejného klíče není ale možné nějakou další zprávu zašifrovat. Adresát se tak nemůže v budoucnu vydávat za odesílatel. Může jen s tím, co má, nějaká budoucí data od stejného odesílatele dešifrovat. Situace je tedy asymetrická. Šifrování a dešifrování probíhá s jinými klíči.

V následujícím příkladu bude šifrováno číslo [2] a šifrování bude probíhat pro názornost s miniaturními klíči, ovšem reálným "ostrým" způsobem. Bez přehánění lze konstatovat, že se jedná o počítání "na prstech"! Je zbytečné z toho dělat vědu. 1+1=2 a není potřeba $1+1=2\pi e^{j\phi}/e\pi^{j\phi}$. Ale i při tak elementárních úkonech s malými čísly je evidentní, jak je šifra RSA účinná a efektivní i proti útoku s vysokým výpočetním výkonem.

Postup vytvoření soukromého klíče

Soukromý klíč tvoří dvojice čísel (N, e). Postup výpočtu je následující.

1. Je potřeba zvolit (nejlépe náhodně) dvě obrovská prvočísla. Čísla „p“ a "q".
   Velikost těchto prvočísel určuje složitost šifry a záleží na jejich velikosti "prolomitelnost" šifry.

   př.:

   p = 2
   q = 7

2. Vypočítá se číslo "N" jako násobek čísel "p" a "q".

   př.:

   N = p * q
   N = 2 * 7
   N = 14

3. Vypočítá se funkční hodnota Eulerovy funkce ϕ(N). Kde ϕ(N) = (p-1) * (q-1)

   př.:

   ϕ(N) = (p-1) * (q-1)
   ϕ(N) = (2-1) * (7-1)
   ϕ(N) = 1 * 6
   ϕ(N) = 6

   Vypočtená hodnota [6] odpovídá také počtu čísel, která jsou menší než "N"
   a jsou s ním nesoudělná:

   1 *
   2 stejně jako číslo [14] je dělitelné číslem [2]
   3 *
   4 stejně jako číslo [14] je dělitelné číslem [2]
   5 *
   6 stejně jako číslo [14] je dělitelné číslem [2]
   7 stejně jako číslo [14] je dělitelné číslem [7]
   8 stejně jako číslo [14] je dělitelné číslem [2]
   9 *
   10 stejně jako číslo [14] je dělitelné číslem [2]
   11 *
   12 stejně jako číslo [14] je dělitelné číslem [2]
   13 *

   jsou to tedy čísla:[1; 3; 5; 9; 11; 13].

4. Zvolí se číslo "e", které splňuje následující požadavky:

   a) 1 < e < ϕ(N)
   b) je nesoudělné s N
   c) je nesoudělné s ϕ(N)

   př.:

   K dispozici je tedy soubor čísel [1; 3; 5; 9; 11; 13]
   Z nich se vyřadí všechna taková čísla, které neodpovídají výše uvedeným podmínkám.

   a) na základě omezení rozsahu intervalu "1 < e < ϕ(N)" zbyde soubor čísel: [3; 5]
   b) soubor čísel [3; 5] vyhovuje, s číslem N=14 jsou obě čísla nesoudělná
   c) číslo [3] je soudělné s ϕ(N)=6
      Zbyde tedy číslo [5].
      (pokud zbyde čísel více, lze si náhodně jedno z nich zvolit)

   e = 5

Postup vytvoření veřejného klíče

Veřejný klíč tvoří dvojice čísel (N, d). Číslo "N" je stejná část soukromého klíče. Postup výpočtu "d" je následující.

Číslo "d" musí splňovat podmínku (d * e) (mod ϕ(N)) = 1

Pro výpočet se použijí prvky ze soukromého klíče e = 5 a ϕ(N) = 6

př.:

(d * 5) (mod 6) = 1

hledáme pro jednotlivá "d":

d = 1: 5 (mod 6) = 5
d = 2: 10 (mod 6) = 4
d = 3: 15 (mod 6) = 3
d = 4: 20 (mod 6) = 2
d = 5: 25 (mod 6) = 1
d =6: 30 (mod 6) = 0
d =7: 35 (mod 6) = 5
d = 8: 40 (mod 6) = 4
d = 9: 45 (mod 6) = 3
d = 10: 50 (mod 6) = 2
d = 11: 55 (mod 6) = 1
d = 12: 60 (mod 6) = 0

Podmínce vyhovuje d = 5, ale lze použít libovolné vyšší číslo, které se periodicky vyskytuje, např. d = 11.

Šifrování zprávy pomocí soukromého klíče

Pro zašifrování jednoho čísla "M" se použije vzorec: $M^e \pmod N = m$
kde "M" je číslo, které bude šifrováno a výsledkem je číslo "m".

př.:

číslo, které bude šifrováno M = 2
soukromý klíč (N = 14, e = 5)

$M^e \pmod N = m$
$M^5 \pmod{14} = m$
$2^5 \pmod{14} = m$
$32 \pmod{14} = 4$

m = 4

protože: 32 : 14 = 2,2857
2,2857 je celočíselně 2
nazpět: 2 * 14 = 28
32 - 28 = 4

Výsledkem šifrování čísla [2] je číslo [4]. Číslo [4] tak může putovat nezabezpečeným prostorem, protože neoprávněný pozorovatel nebude moci bez správného klíče číslo dešifrovat a získat tak původní zprávu [2].

Dešifrování zprávy pomocí veřejného klíče

Pro dešifrování jednoho čísla "m" se použije vzorec: $m^d \pmod N = M$
kde "m" je číslo které bude dešifrováno a výsledkem je číslo "M".

př.:

číslo, které bude dešifrováno m = 4
veřejný klíč (N = 14, d = 11)

$m^d \pmod N = M$
$m^{11} \pmod{14} = M$
$4^{11} \pmod{14} = M$
$4194304 \pmod{14} = M$

4194304 :14 = 299593,142857 celočíselně = 299593

celočíselně vynásobené nazpět 299593 * 14 = 4194302

rozdíl čísla "m^d"před dělením modulo a jeho zpětné celočíselné rekonstrukce 4194304 - 4194302 = 2

M = 2

Adresát, který přijal zašifrovanou zprávu v podobě čísla [4] a použil veřejný klíč, dešifrováním získal původní číslo [2].

Slovníček pojmů

PRVOČÍSLO

Je větší než 1 a nedá se vydělit žádným celým číslem, aby bylo výsledkem celé číslo.

př.:
2, 3, 5, 7, 11, 13, …

FAKTORIZACE

Rozložení čísla na prvočísla.

př.:
15 = 3 * 5

NESOUDĚLNÁ ČÍSLA

Čísla, která nemají společného dělitele.

př.:
8 = 2 * 2 * 2
15 = 3 * 5
[8] a [15] jsou čísla nesoudělná

12 = 3 * 4
9 = 3 * 3
[12] a[9] jsou soudělná díky číslu [3]

DĚLENÍ MODULO (mod x)

Výsledkem dělení modulo je zbytek po dělení. Dělitel modulo se zapisuje společně s "mod" do závorek.

př.:
20 (mod 6) = 2
protože celočíselně 20 : 6 = 3 a zbyde právě zbytek 2,
jelikož zpětná celočíselná rekonstrukce 3 * 6 = 18
a její rozdíl s původním číslem před dělením modulo je 20 - 18 = 2

Použité zdroje

RSA (cryptosystem) - Wikipedia. [online]. Dostupné z: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Euler's totient function - Wikipedia. [online]. Dostupné z: https://en.wikipedia.org/wiki/Euler%27s_totient_function

Online RSA Key Generator. Travis Tidwell [online]. Dostupné z: https://travistidwell.com/jsencrypt/demo/