Activitat 6 parcial AA

Hugo Aranda Sánchez

April 2023

Diem que el sistema RSA és fàcilment vulnerable quan donada la clau pública i un missatge codificat, aquest es pot decodificar en temps polinòmic. (i) Demostreu que si P = NP, aleshores els sistema RSA seria fàcilment vulnerable. (ii) I si tinguéssim manera de vulnerar fàcilment el sistema RSA, això implicaria que P = NP?

1 Respostes

1.1 (i)

Si tinguessim $P = NP$, això implicaria que tot problema que pertanyi a NP tindria una reducció en temps polinomic a un problema polinomic, esdevenint el primer en essencia un problema de la classe polinomica. Llavors tindriem que, donat el fet que la factoritzacio de nombres arbitrariament grans es un problema que pertany a NP (demostració més avall) aquesta podria ser resolta en temps polinomic.

Ara bé, com la seguretat de el sistema RSA radica en aquesta dificultat algorismica, atés que si existeix aquest hipotétic algorisme polinomic capaç de factoritzar en nombres primers podriem facilment calcular les claus privades a partir de la clau publica (N,e) de la seguent manera:

1. Obtenim la descomposició en primers de $N = p \cdot q$
2. Ara amb aquesta descomposició obtenim la Euler Totien Function $\phi(N) = (p-1)\dot{(}q-1)$
3. Amb la qual podem computar la clau privada $e \equiv c^{-1} mod \phi(N)$

A partir d'aquest moment ja tenim la clau privada i per a poder desencriptar tots els missatges interceptats que hagin sigut encriptat mitjançant la clau publica. Aconseguint aixi una decodificació en temps polinomics fent que RSA sigui un sistema facilment vulnerable.

1.1.1 Factorització pertany NP

La factorització de N en $p\dot{q}$ es un probema numeric mentres que NP realment es una clase de complexitat per a problemes decisionals. Llavors hem de repensar un problema que en un numero finit de passos decisionals ens permeti obtenir els valors que volem.

Donades input N i M, té N un factor en l'interval $(1, M]$?

Podem donar un certificat de mida polinomica el qual seria un divisor particular dints de l'interval

Podem evaluar un certificat particular en temps polinomic amb un input de llargaria $\log_2(N)$ veient si aquest es o no divisor.

cal veure si son primers? També gracies al Agrawal–Kayal–Saxena primality test podem veure si es primer en temps polinomic i això podria formar part de la evaluació del ceritificat, tot i que no es necessari que sigui primer, podem trobar factors en general fins trobar el mes petit, es a dir q, i despres obtenir p de la seguent manera $p = N/q$

Per tant de la modalitat decisional del problema de la factoritzacio, podem obtindre una solució mes complexa mitjançant cerques binaries obtenint el minim factor.

1.2 (ii)

Per demostrar $NP = P$, hem de demostrar que $P \subseteq NP$ i $NP \subseteq P$. La primera implicació es trivial, i la segona es la que hauriem de obtindre si volem respondre la pregunta del mil·lio de dolars.

Si tinquessim una manera facil de vulnerar el sistema RSA, això només implicaria que la factoritzacio de nombres primers es P, atés que aquesta es la unica vulnerabilitat coneguda. Abans hem vist que aquest problema es NP, pero això no és suficient per demostrar la part de la implicació que no sabem, $NP \subseteq P$. Atés que per això hauriem de saber que la factorització es NP-hard, i per tant NP-completa, cosa que no esta demostrada encara. Si fos NP-complete, tot problema NP tindria una reducció cap a aquest problema particular i per tant que aquet sigui P, ens ajudaria a obtindre la implicació desitjada, peró no tenim informació suficient per afirmar això.