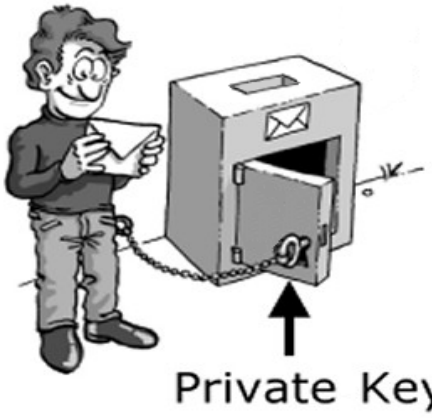
អត្ថបទដកស្រង់ចេញពី

Klein Project Blog

កូដការ (កូនសោសាធារណៈនៃកូដការ) *Cryptography (Public-key Cryptography)*



រៀបរៀងដោយអ្នកនិពន្ធ: Graeme L. Cohen, Steven Galbraith និង*Edoardo Persichetti*។

តើយើងអាចផ្ញើទិន្នន័យកាតឥណទាន *(Credit Card)* របស់យើងដោយសុខសុវត្ថិភាព លើប្រព័ន្ធបណ្តាញសាកល (ឬអ៊ីនធឺណែត) ឬការប្រើទូរស័ព្ទទំនើបពេលអ្នកដ៏ទៃអាចនឹងស្តាប់យក សាររបស់យើង ដោយរបៀបណា? តើយើងអាចទុកចិត្តកម្មវិធីអាប់ដេត ពេលយើងដឹងថាកុំព្យូទ័រជារឿងធម្មតាអាចមានវីរុស ដោយរបៀបណា ? កូដការ (*Cryptography*) (គឺសិក្សា អំពីវិធីសម្រាប់គមនាគមន៍ប្រកបដោយ សុវត្ថិភាព ដ៏រឹងមាំតទល់និងសត្រូវ) ផ្តល់ចម្លើយតបនឹងសំនួរទាំងនេះ ហើយគណិតវិទ្យាបានផ្តល់គ្រិះសម្រាប់កិច្ចការនេះ។

ប្រវត្តិខ្លី

សុវត្ថិភាពគមនាគមន៍មានតួនាទីសំខាន់ច្រើនពាន់ឆ្នាំមកហើយ៖ ជាភស្តុតាង គឺការដែល ជូលូស ស៊ីស៊ើរ (*Julius Caesar*) បានប្រើកូដការដ៏សាមញ្ញ សម្រាប់ទំនាក់ទំនងជាមួយឧត្តមសេនីរបស់គាត់។ គោងការណ៍នេះមានឈ្មោះថា «កូដការស៊ីស៊ើរ» ដែលផ្អែកលើការប្តូរទីតាំងអក្សរមួយចំនួនក្នុងសារ ដើម្បីបង្កើតជាអត្ថបទថ្មី ហៅថា អត្ថបទកូដការ *(ciphertext)*។ សារដើមអាចទទួលបានមកវិញ ដោយអ្នកទទួលត្រូវប្រតិបត្តិបញ្ច្រាស គឺធ្វើ ការត្រឡប់ទីតាំងអក្សរមកវិញតាមទម្រង់ដើម។

គំនិតសំខាន់គឺថាទាំងអ្នកផ្ញើនិងទាំងអ្នកទទួលត្រូវដឹងតម្លៃសម្ងាត់មួយ (ក្នុងករណីនេះគឺចំនួននៃទីតាំង) ដែលអ្នកដ៏ទៃមិនអាចដឹងពេលសាកល្បងមើលសារនោះ។ តម្លៃសម្ងាត់នោះ ហៅថាកូនសោ *(Key)*។នៅក្នុងករណី កូដការស៊ីស៊ើរខាងលើ កូនសោ ជាចំនួនរវាងពី 0 ទៅ 26។ វិធីសាស្ត្រកូដ ការ *Enc* ដាក់បញ្ចូលក្នុងសារ *M* នូវកូនសោ K ជាឧទាហរណ៍Enc_3 *(Hello) = Khoor*។ នៅវិធីសាស្ត្រ *Dec* វិញ គឺ ដាក់បញ្ចូល អត្ថបទកូដការ *C* នូវកូនសោ ដូចគ្នា *K* ជាឧទាហរណ៍Dec_3*(Khoor) = Hello*។

ប្រព័ន្ធកូដការដែលប្រើកូនសោដូចគ្នា ត្រូវបានគេប្រើសម្រាប់សរសេរកូដសម្ងាត់ *(encrypting)* និងបកស្រាយកូដសម្ងាត់ *(decrypting)* មានឈ្មោះថាគោលការណ៍កូនសោស៊ីមេទ្រី *(Symmetric-Key schemes)*។

កូដការស៊ីស៊ើរ គឺសាមញ្ញពេកណាស់ សម្រាប់ ពិភពលោកទំនើបនេះ ប៉ុន្តែ ក៏នៅតែមាន កូនសោស៊ីមេទ្រីប្រើក្នុងសម័យបច្ចុប្បន្ន ដូចជានៅ ស្តាប់ដ៏ល្បីល្បាញ *AES* ដែលជាស្តង់ដាររដ្ឋាភិបាល សហរដ្ឋអាមេរិច សម្រាប់ផ្ទេរទិន្នន័យជាដើម។ ប្រព័ន្ធនេះមានប្រសិទ្ធភាព និងសុវត្ថិជាព តែ មានបញ្ហាមួយ៖ ទាំងអ្នកផ្ញើនិងអ្នកទទួលត្រូវត្រូវដឹងនូវអាថិកំបាំង។ តើយើងអាចទាក់ទងជាសម្ងាត់តាមអ៊ីនធឺណែត ជាមួយមុនស្សដែលយើងមិនដែលបានឃើញមុខដោយរបៀបណា?

គោលការណ៍ដ៏អស្ចារ្យមួយហៅថា កូនសោសាធារណៈនៃកូដការ (*Public-Key cryptography*) បង្កើតឡើងនៅឆ្នាំ 1976 ក្នុងអត្ថបទ «ទិសដៅថ្មីនៃកូដការ» *"New directions in cryptography"* ដោយលោក វីតហ្វៀល ឌីហ្វី (*Whitfield Diffie*) និង ម៉ាកទីន ហែលម៉ាន់ (*Martin Hellman*) បានដោះស្រាយបញ្ហានេះ។ នៅទីនេះ ជំនួសឱ្យការប្រើកូនសោ ដូចគ្នាសម្រាប់សរសេរកូដសម្ងាត់ *(encrypting)* និងការបកស្រាយកូដសម្ងាត់ *(decrypting)* មានសោសាធារណៈ (***public key)*** ដែលអ្នកប្រើប្រាស់ទាំងឡាយអាចទទួលបាន និងកូនសោឯកជន ***(private key)*** ដែលគង់នៅជាសម្ងាត់ អ្នកប្រើប្រាស់ពិសេស។ ពោលបានម៉្យាងទៀតថា អ្នកដ៏ទៃអាចផ្ញើសារបាប ប៉ុន្តែមានមនុស្សតែម្នាក់គត់អាចទទួលវា។ អ្នកណាក៏ដោយបោះសំបុត្រទៅក្នុងប្រអប់សំបុត្រ តែមានមនុស្សតែម្នាក់គត់ ដែលមានកូនសោសម្រាប់បើកប្រអប់សំបុត្រនោះ។ អ្នកចង់ទាក់ទងជាមួយ

ណារី ត្រូវប្រើកូនសោសាធារណៈរបស់ខ្លួនបង្កើតអត្ថបទកូដការ *(cipher text)* មួយ។ មានតែ ណារី ម្នាក់គត់ ដែលអាច បកស្រាយកូដសម្ងាត់ក្នុងអត្ថបទកូដការនោះ ព្រោះមានតែនាងទេដែលមាន កូនសោឯកជន។

ប្រព័ន្ធកូដការ កូនសោសាធារណៈ ត្រូវពឹងផ្អែកលើចំណោទគណនាមួយ ដែលពិបាកដោះស្រាយ។ គណិតវិទ្យា ជាអ្នកដោះស្រាយបញ្ហានេះ ជាឧទាហរណ៍ ប្រព័ន្ធកូដការ *RSA* ដែលផ្អែកលើភាពស្មុគស្មាញ នៃ ការស្វែងរក កត្តាបឋមនៃចំនួនគត់ដ៏ធំ។

ទ្រឹស្តីបទចំនួនខ្លះៗ

មុនរៀបរាប់ពី គោលការណ៍ នៃកូដការ កូនសោសាធារណៈ *RSA* ដ៏ល្បីល្បាញ យើងត្រូវការលទ្ធផលខ្លះ ពីទ្រឹស្តីបទចំនួនសិន។ គឺត្រូវការចំណេះដឹងសមល្មមនូវទ្រឹស្តីបទទ្វេធា *(binomial theorem)* និងនព្វន្តសាស្ត្រ នៃម៉ូឌុលឡា។

នៅក្នុងនព្វន្តសាស្ត្រនៃម៉ូឌុលឡា យើងប្រមែប្រមូលថ្នាក់ដែលមានសំណល់ ផលចែកដូចគ្នា ពីការចែកចំនួន P មួយ ដែលគេត្រូវបានហៅថាម៉ូឌុលឡា។ ឧទាហរណ៍ បើ $P = 7$ យើងបាន 9 ស្ថិតនៅថ្នាក់ 2 ហើយ 12 និង 19 មានថ្នាក់ដូចគ្នា ពោលគឺថ្នាក់ 5។ យើងអាចសរសេរថា $9 \equiv 2 \pmod 7$និង $12 \equiv 19 \equiv 5 \pmod 7$។ ងាយយល់ណាស់ថាថ្នាក់ដែលមានតែ 7 ដែលតាងដោយ{0,1,2,3,4,5,6} ពេលយើងសង្កេត *(mod 7)*។ យើងអាចធ្វើ ប្រមាណវិធី បូកនិងគុណលើ (mod 7) ដោយបង្រួមនូវលទ្ធផលយ៉ាងសាមញ្ញ បន្ទាប់ពីការធ្វើប្រមាណវិធីធម្មតា ព្រោះ ថា $3+8=11 \equiv 4 \pmod 7$ និង$3.5=15\equiv 1 \pmod 7$។ គួរចាំថាបើ $a\equiv b \pmod p$នោះ $(a-b)$ចែកដាច់នឹង p។

តាង p និង q ជាចំនួនបឋមដែល $p \neq q$ និង $t > 0$ ជាចំនួនគត់ដែលមិនចែកដាច់នឹងp ឬ q នោះយើងនឹង បង្ហាញថារូបមន្ត$t^{(p-1)(q-1)} \equiv 1 \pmod{pq}$ ពិត។ នេះជារូបមន្តពិសេសនៃទ្រឹស្តី បទ ហ្វៃម៉ា-អឺល័រ (*Fermat-Euler*)។ ការបកស្រាយចាប់ផ្តើមជាមួយរូបមន្តមេគុណទ្វេធា

$$\binom{p}{i} = \frac{p!}{i!(p-i)!},$$

ដែល i ជាចំនួនគត់ ប្រកបដោយ $0 < i < p$។ តាមរយៈ:

$$i! \binom{p}{i} = p(p-1)(p-2)\cdots(p-i+1),$$

នាំឱ្យបាន p ជាតួចែក $\binom{p}{i}$ ដោយ p ចែកដាច់ផ្នែកខាងស្តាំ ប៉ុន្តែមិនចែកដាច់នឹង$i!$ ទេ។

យើងបានសម្រាប់ចំនួនគត់A និងB តាមទ្រឹស្តីបទទ្វេធា៖

$$(A+B)^p = A^p + \binom{p}{1}A^{p-1}B + \binom{p}{2}A^{p-2}B^2 + \cdots + B^p \equiv A^p + B^p \pmod p.$$

យកចំនួនគត់ C មកបន្ថែម៖

$$(A+B+C)^p = ((A+B)+C)^p \equiv (A+B)^p + C^p \equiv A^p + B^p + C^p \pmod p.$$

តាមវិធីដដែលនេះ សម្រាប់គ្រប់ $A_1, A_2, \cdots, A_t$

$$(A_1 + A_2 + \cdots + A_t)^p \equiv A_1^p + A_2^p + \cdots + A_t^p \pmod p.$$

យកតម្លៃ $A_1 = A_2 = \cdots = A_t = 1$ នោះយើងបាន

$$t^p \equiv t \pmod p.$$

សមីការនេះមានន័យថា $(t^p - t) = t(t^{p-1} - 1)$ ចែកដាច់នឹងp ។ ដោយ p មិនចែកដាច់នឹង t ហើយ p ជាចំនួនបឋម ដូចនេះ នាំឱ្យ៖

$$t^{p-1} \equiv 1 \pmod p.$$

ឥលូវយើងលើកស្ងួយគុណអង្គទាំងពីរនៃសមភាព ដោយស្ងួយគុណ $q - 1$:

$$t^{(p-1)(q-1)} \equiv 1 \pmod{p}.$$

ដោយប្រើអំណះអំណាងដដែលឡើងវិញ ដោយប្រើ q ជំនួស pយើងបាន៖

$$t^{(p-1)(q-1)} \equiv 1 \pmod{q}.$$

ដូចនេះ យើងអាចនិយាយបានថា មានចំនួនគត់ h និងk រៀងគ្នា ដែល

$$t^{(p-1)(q-1)} = 1 + ph, \quad t^{(p-1)(q-1)} = 1 + qk,$$

ដូចនេះ $ph = qk$ ។ ឯ p ចែកដាច់នឹង k (ដោយ pនិង qជាចំនួនបឋមផ្សេងគ្នា) នោះ $k = pl$ ដែល l ជាចំនួនគត់។ យើងមាន $t^{(p-1)(q-1)} = 1 + pql$ ឬក៏

$$t^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

នេះជាចុងបញ្ចប់នៃសម្រាយបំភ្លឺ។

ប្រព័ន្ធកូដការ *RSA*

ពាក្យកាត់នៃ*RSA* មកពីពាក្យពេញថា*Rivest, Shamir* និង *Adleman* ដែលអ្នកទាំងនេះបានលើកជាសំណើដំបូងពីគោលការណ៍នេះ នៅឆ្នាំ1977។ ដែលវាដំណើរការដូចខាងក្រោម៖

ជាដំបូងជ្រើសរើសចំនួនបឋមពីរផ្សេងគ្នា p និង q បន្ទាប់មកចាប់ផ្តើមគណនា$N = pq$ និង $\phi = (p-1)(q-1)$ ។ រើសយកចំនួនគត់ e មួយដោយចៃដន្យរវាង 3 ដល់ N – 2 តែ e និង ϕ មិនត្រូវមានកត្តាបឋមរួមទេ។ កូនសោសាធារណៈគឺជាគូ (N,e) ចំណែកឯកូនសោឯកជន d ដែលអ្នកធ្វើនឹងរក្សាទុក គឺជាការគណនា $d \equiv e^{-1} \pmod{\phi}$ ដូចជាចំនួន $de \equiv 1 \pmod{\phi}$ (វាងាយទទួលបានពីវិធីសាស្ត្រអឺគ្លីដ)។ ជាឧទាហរណ៍យក $N = 437 = 19 \cdot 23$, $\phi = 396$, $e = 5$ និង $d = 317$។

សារនៅក្នុងប្រព័ន្ធ *RSA* ជាចំនួនគត់ x ដែល $0 < x < N$។ ប្រហែលជាមិនច្បាស់លាស់ទេថា តើកូដការសារអក្សរ មានគោលការណ៍បែបណា តាមរយៈការប្រើចំនួនគត់នោះ។

យ៉ាងនេះក្តីក៏គោលការណ៍នៃកូដការនេះបានបំពាក់លើកុំព្យូទ័រ ដែលឯកសារជាទិន្នន័យប្រព័ន្ធគោលពីរ ដែលអាចធ្វើកូដការដោយប្រើចំនួនគត់បាន។

កូដការប្រព្រឹត្តដូចតទៅ។ ឧបមាថា បូណា ចង់ផ្ញើសារ x ទៅ ណារី ។ គាត់ស្វែងរកកូនសោសាធារណៈ(N,e) របស់ ណារី ហើយ គណនា$y \equiv x^e \pmod{N}$ផ្ញើ y នេះទៅ ណារី ។ដើម្បី បកប្រែកូដសម្ងាត់ y ណារី យកកូនសោឯកជន d ដើម្បីគណនា

$$x \equiv y^d \pmod{N}$$

ចំណុចសំខាន់ គួរកត់សម្គាល់ថា ដោយ e, dនឹង Nជាចំនួនធំណាស់ វាទាមទារការគណនាធំធេង ឧទាហរណ៍ $y^d \pmod{N}$ គណនាដោយប្រើបច្ចេកទេសឈ្មោះថា *modular exponentiation*។

ការបកប្រែកូដសម្ងាត់ ចាប់ផ្តើមដោយ$de = 1 + k\phi$ ពីចំនួនគត់ k ណាមួយ ហើយដូចជាយើងបានបង្ហាញពីខាងលើ៖

$$x^{\phi} = x^{(p-1)(q-1)} \equiv 1 \pmod{N}$$

(ក្នុងការអនុវត្តន៍ អាចរំលងករណី x ចែកដាច់នឹង p ឬនិង q) យើងបាន។

$$y^d \equiv (x^e)^d = x^{1+\phi k} = x(x^{\phi})^k \equiv x \cdot 1^k = x \pmod{N}.$$

អ្នកប្រើប្រាស់ខិលខូច មិនស្គាល់ កូនសោឯកជន d ត្រូវរារកកត្តាបឋមនៃ Nដើម្បីបាន តម្លៃ p និង q ដែលហួសសមត្ថភាព នៃការគណនា ព្រោះ ប្រសិនបើចំនួនបឋមទាំងនោះធំដូចជាមានលេខ 200 ខ្ទង់សម្រាប់ចំនួននិមួយ។ (ឯកទគ្គកម្មពិភពលោកបច្ចុប្បន្នសម្រាប់ផលគុណពីរកត្តា $N = p$ បានត្រឹម p និង q និមួយ។ត្រឹម100ខ្ទង់ប៉ុណ្ណោះ)។

ទាំងនេះជាការពិតក្នុងការកំណត់កម្រិតសុវត្ថិភាពនៃគោលការណ៍។ សញ្ញាណសំខាន់នៃកូដការកូនសោសាធារណៈតាម ពិត វាមានសុវត្ថិភាព ដោយសារថាវាទាមទារការខំប្រឹងប្រែងគណនាជាខ្លាំង ដើម្បីអាចទម្លុះការការពារបាន។ ទាំងនេះជាកំណត់ជាមុន (ធម្មតាគឺប្រព័ន្ធប្រតិបត្តិការ 2^{128} ឬ 2^{256} ប៊ីត) និងអាស្រ័យលើបរិបទ ហើយនឹងបំណងនៃការទាក់ទង។ ពិតណាស់ថា សារសម្ងាត់ *CIA* និងអ៊ីមែលរវាងអ្នកប្រើប្រាស់លើបណ្តាញសាកលប្រាកដជាឆ្លងកាត់ស្តង់ដាសុវត្ថិភាពខុសពីគ្នា!!!

ហត្ថលេខា

យើងអាចត្រឡប់មកបញ្ហាអាប់ដេតកម្មវិធី។ អាចនិយាយម៉្យាងទៀតថា បញ្ហាយថាភាព *(authentication)* ។ ដូចមុនដែរយើងមានកូនសោសាធារណៈនិងកូនសោឯកជន។ណារី ប្រើកូនសោឯកជនបង្កើតជាហត្ថលេខាឌីជីថលក្នុងការផ្ទៀជាប់ជាមួយឯកសារ ដើម្បីបង្ហាញយថាភាពរបស់ឯកសារនោះ (ហត្ថលេខាអាស្រ័យ ជាប់នឹងឯកសារ ហើយ និងមិនអាចកាត់ហើយបិទលើឯកសារផ្សេងទេ)។ អ្នកទទួលត្រូវត្រួតពិនិត្យហត្ថលេខា ដោយប្រើកូនសោ សាធារណៈ។

ជាឧទាហរណ៍ ឧបមាថាកុំព្យូទ័ររបស់ប្រាប់អ្នកថា វាកឃើញអាប់ដេតសម្រាប់*Adobe*។ តើការធ្វើកុំព្យូទ័រស្គាល់កម្មវិធីអាប់ដេតថាមកពី*Adobe* ហើយមិនមែនលាក់បាំងមេរោគ ដោយរបៀបណា? ដំណោះស្រាយគឺថា ឯកសារអាប់ដេតមានហត្ថលេខាឌីជីថល ដែល គោរពតាម កូនសោសាធារណៈរបស់ *Adobe*។ កូនសោទាំងនេះបានតម្លើង លើកុំព្យូទ័ររបស់អ្នកជាមួយកម្មវិធី *Adobe* ដូច្នេះកុំព្យូទ័រអ្នក អាចត្រួតពិនិត្យហត្ថលេខា មុនការអាប់ដេត ពោលគឺ ការផ្ទៀងផ្ទាត់ជោគជ័យជាសាក្សីថា អាប់ដេតពិតជាមកពី*Adobe* មែន មិនមែនមកពីទីដ៏ទៃទេ។

យើងបង្ហាញឥឡូវនេះពីរបៀបបបង្កើតហត្ថលេខាឌីជីថល ដោយប្រើ *RSA*។

កូនសោឯកជននិងកូនសោសាធារណៈដូចគ្នាសម្រាប់បង្កើតកូដសម្ងាត់។ ពេល ណារី ចង់ធ្វើយថាភាពឯកសារណាមួយ (ឧទាហរណ៍៖កម្មវិធីអាប់ដេត) នាងធ្វើកូដការវាជាចំនួនគត់ $0 < x < N$ គណនា $\sigma \equiv x^d \pmod N$ និងភ្ជាប់ហត្ថលេខា σ ទៅឯកសារ។ ដើម្បី ត្រួតពិនិត្យហត្ថលេខាឌីជីថល បូណា រាវរក កូនសោសាធារណៈរបស់ ណារី ហើយត្រួតពិនិត្យ ដោយការគណនា $x' = \sigma^e \pmod N$ និងពិនិត្យថា $x' = x$ ។ វាច្បាស់ណាស់ថា ដូចក្នុងប្រព័ន្ធកូដការ *RSA* ជនខិលខូចតែងប៉ងបង្កើតនូវហត្ថលេខាឌីជីថល (ឧទាហរណ៍ ពួកហែកឃ័រធ្វើវីរុស) ហើយត្រូវគណនាស្វ័យគុណ d ដែលត្រូវការកត្តាបថមរបស់ N។

ការស្រាវជ្រាវនេះ

យើងបានបង្ហាញគម្រូនៃប្រព័ន្ធកូដការ *RSA* និងការបង្កើតហត្ថលេខាឌីជីថល តែក៏ មានប្រព័ន្ធផ្សេងៗ ជាច្រើនទៀតដែលយកគណិតវិទ្យាជាគ្រិះ ដូចជា៖ កាយរាប់អស់*(finite fieds)*, ខ្សែកោងអេលីប(elliptic curves), ប្រព័ន្ធសមីការច្រើនអថេរមិនលីអែរ, កំណែកូដ និងអ្វីៗច្រើនទៀត។

កូដការកូនសោសាធារណៈនៅជាបញ្ហាសកម្មសម្រាបើធ្វើការស្រាវជ្រាវ ហើយនៅមានបញ្ហាមិនទាន់ដោះស្រាយជាច្រើនទៀត។

ខាងក្រោយឆាកក្វាន់ទុម

តើបញ្ហាទាំងអស់របស់យើងដោះស្រាយបានដោយ *RSA* ឬទេ? ជាអកុសលចម្លើយនោះគឺមិនបានទេ។ សុវត្ថិភាពនៃ *RSA* ដូច គោងការណ៍ដទៃទៀត ដែលមានមូលដ្ឋានគ្រឹះពីទ្រឹស្តីចំនួន រងការគំរាមកំហែង ដោយពិតប្រាកដពីសក្តានុពលអភិវឌ្ឍន៍នៃកុំព្យូទ័រក្វាន់ទុម។ វិធីសាស្ត្រ *Shor*បោះពុម្ពផ្សាយនៅឆ្នាំ 1994 ដែលមានចំណងជើងថា «វិធីសាស្ត្រពហុធាពេលសម្រាប់លោការីតដាច់ និងផលគុណកត្តាបបមក្នុងកុំព្យូទ័រក្វាន់ទុម» សមត្ថភាពនៃបំបែក ប្រព័ន្ធកូដការ *RSA* ពេល កុំព្យូទ័រក្វាន់ទុមមានសមត្ថភាពគ្រប់គ្រាន់នោះ។ កុំព្យូទ័រក្វាន់ទុមតូចៗមានរូចទៅហើយ ហើយកុំព្យូទ័រក្វាន់ទុមខ្នាតធំ អាចនឹងមានក្នុងអនាគតដ៏ខ្លី។ ដូច្នោះវាមានសារៈសំខាន់ណាស់ក្នុងការផ្តល់នូវប្រព័ន្ធថ្មី ដែលធានាសុវត្ថិភាព ពេលឆាកថ្មីនេះបានកើតឡើង។ សហគមន៍អ្នកធ្វើកូដការ *(The cryptographic community)* កំពុងតែស្រាវជ្រាវយ៉ាងសកម្ម ក្នុងការអភិវឌ្ឍប្រព័ន្ធកូដការពីផ្នែកផ្សេងៗនៃគណិតវិទ្យា ឈរលើ ការគណនា ដែលសង្ឃឹមថា ជាវិធីសាស្ត្រព្យាបាលនូវវិធីសាស្ត្រក្វាន់ទុមដ៏ស្រួចស្រាវនេះ។

ឯកសារយោង

[1] Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (2000), Anchor.