星島教室 數學原理

作者介紹


仁濟醫院羅陳楚思中學 副校長 譚在能


仁濟醫院羅陳楚思中學 數學科老師 曾韋怡


仁濟醫院羅陳楚思中學 數學科老師 鄧頌賢

加密，究竟有幾秘密？

眾所周知，密碼與我們的日常生活息息相關，而數學在密碼學中扮演着一個非常重要的角色。「加密」(Encryption)是將原來的訊息(明文)改變為難以理解及讀取的密文。經過「解密」(Decryption)過程，密文才能還原為明文。加密法分為「對稱加密法」及「非對稱加密法」，本文將扼要介紹對稱加密法及非對稱加密法，並提供簡化例子予讀者研習，以加深各位對相關課題的認識及理解。

對稱加密法

Alice想給Bobby傳遞一個訊息 m（ m 稱為明文），為讓讀者更易理解，我們可假設m為一個整數，Alice將 m 加上一個整數 e（ e 為一個密鑰)後訊息變為 m＋e ，以上過程是為加密法。加密後訊息由 m 轉變為 m＋e ，我們稱 m＋e 為 c（ c 可稱為密文），在解密過程中，將 c 減去 e 後Bobby便可得到訊息 m 。由於在加密及解密的過程中我們使用相同的密鑰，故此以上的加密法稱為對稱加密法。

例子：
訊息 m＝3，密鑰 e 為－100，由此密文 c＝m＋e＝3－100＝－97。
解密之後，訊息為 c－e＝－97－(－100)＝3，即Bobby可接收原來的訊息。

RSA 加密演算法流程

為使讀者更易明白RSA加密演算法原理及流程，以下例子中使用了數值很小的質數示範RSA加密演算法的原理，在實際操作上，p 和 q 均為非常大的質數。選取大質數是基於保安理由，黑客在得到公開密鑰 (e, n) 後想設法得到私有密鑰 (d, n) ，他必須知道 Ø 的值(e×d≡1(mod Ø))，而由於 Ø＝(p－1)(q－1)，他要計算 p 和 q 的值，換句話說，他須使用電腦因式分解一個非常大的整數 n (n＝pq)，n 愈大，破解私有密鑰的困難便會愈大，故此對於足夠大的 n 而言，RSA加密演算法頗為安全。

RSA加密演算法(非對稱加密法)

在對稱加密法中，由於加密及解密的密鑰相同，如在過程中被黑客發現密鑰，訊息便會被破解，為提高安全性，在1977年，3名在麻省理工學院工作的科學家，羅納德．李維斯特(Ronald Linn Rivest)、阿迪．薩莫爾(Adi Shamir)和倫納德．阿德曼(Leonard Adleman)共同提出了一種非對稱加密演算法，即RSA加密演算法，RSA加密演算法在電子商業中被廣泛使用。RSA加密演算法就是以他們3人姓氏開頭字母拼在一起組成的。RSA加密演算法是一種非對稱式密碼學，它需要兩個密鑰，一個是公開密鑰，其作用是為訊息加密；另一個是私有密鑰，用作解密。公開密鑰把明文(原本訊息)加密後所得的密文，只能用相對應的私有密鑰才能解密並得到原本的明文，最初用來加密的公開密鑰並不能用作解密。由於加密和解密需要使用兩個不同的密鑰，故此RSA加密演算法被稱為非對稱加密法。

RSA加密演算法原理及流程

1. 先隨機選擇兩個非常大的質數 p 及 q 。
2. 設 n＝pq。
3. 設 Ø＝(p－1)(q－1)。
4. 選定一個足夠大的整數 e 使得 1＜e＜Ø 及 e 與 Ø 互質(即 e 和 Ø 的最大公因數為 1)。
5. 求 d 唯一的值使得 1＜d＜Ø 及 e×d≡1(mod Ø) 。[e×d≡1(mod Ø) 表示 e×d－1 可被 Ø 整除]
6. (e, n) 及 (d, n) 分別為公開密鑰及私有密鑰。
7. 假設Alice想給Bobby傳遞一個訊息 m (m≤n) ，使用公開密鑰加密後的密文 c 為 m^e 被 n 除後的餘數。
8. 使用私有密鑰 (d, n) 解密，Bobby可得到原本的明文 m ，其中 m 為 c^d 被 n 除後的餘數。

例子

我們選取兩個質數p及q，其中p＝7及q＝13 。
n＝pq＝91 及 Ø＝(7－1)(13－1)＝72 。
取 e＝29 使得 1＜e＜Ø 及 e 與 Ø 互質。
由此 d＝5（因為 e×d－1＝29×5－1＝144＝72×2 ，即是 e×d≡1(mod Ø)）
公開密鑰及私有密鑰分別為 (29, 91) 及 (5,91) 。
設 m＝2 (m≤n) ，c 為 m^e 被 n 除後的餘數，即 c 為 2^{29} 被 91 除後的餘數，得 c＝32 。
使用私有密鑰 (5, 91) 解密密文，m 為 c^d 被 n 除後的餘數，即 m 為 32^5 被 91 除後的餘數，得 m＝2 。

練習

我們選取兩個質數p及q，其中 p＝3 及q＝11 。
設 m＝6 。
求 n, Ø, d, e 及 c 的值，並證明使用私有密鑰可將密文還原為明文。

建議答案：
n＝33, Ø＝20, d＝7, e＝3 及 c＝18

本欄逢周四刊登，由教育評議會邀請資深中小學老師、校長及大學講師撰稿，旨在為學生提供多元化的STEAM學習材料，引發學生探求知識的興趣，將學習融入生活，培養學生的世界觀、敏銳的觸覺、積極學習的態度。

讀社論學英文

Plug well-off tenant policy loophole & review heredity

Following the tightening of eligibility requirements for well-off public housing tenants buying Home Ownership Scheme (HOS) units, the Housing Authority (HA) is now preparing to further restrict policies on them, shortening their temporary accommodation period so as not to give them ample time to transfer assets and become eligible again. The scarce public housing supply must be used reasonably. Knowing that it has been abused, the authorities should immediately plug loopholes and review the hereditary system to ensure resources go to grassroots most in need.

The Housing Authority recently held a brainstorming session to address the issue of half the well-off tenants exploiting the 12-month temporary accommodation period to transfer their assets to avoid eviction. The HA is inclined towards plugging the loophole by shortening the grace period. It also discussed whether to amend the public housing hereditary system, but no consensus was reached as many members were concerned adjustments may lead to other social problems.

Use of big data to spot property-owning tenants

There is a need for further tightening of well-off tenant policies as public housing was originally intended to help grassroots. Through rental subsidies, tenants can improve their lives, save money, or invest until they accumulate enough wealth and ability to own a property before moving out to give way to other deserving individuals. However, after receiving a public housing unit, some grassroots tenants are not willing to give up their homes or even transfer their tenancy to their children. This has resulted in less than one per cent of units being in circulation - an unfair situation in which sub-divided flat dwellers have to wait for an average of 5.5 years.

To combat abuse, the HA has introduced well-off tenant policies that were reviewed in 2017. Tenants were required to declare their assets 10 years after moving in and every two years thereafter. If their income or assets exceed the limit, the Housing Department (HD) will issue a move-out notice with a "fixed-term licence" valid up to a year during which they have to pay market rent. However, not many public housing units have been recovered. Even the suspected killer of model Abby Choi Tin-fung was able to purchase an HOS flat using a Green Form status while owning a luxurious flat. It caused outrage and made the HA review and tighten policies.

As the HA enforcement arm, the HD is responsible for this absurd and unfair situation. Firstly, relevant policies were formulated, but it failed to implement them effectively by allowing tenants to declare their own assets and conducting random checks. People caught making false statements were lightly penalized, which gave tenants the impression that HD staff were not doing their job. They turned a blind eye to problematic declarations made by some well-off tenants.

It is not difficult to check the assets of tenants. If the HD works together with other departments, such as using big data of the property registration database of the Land Registry to check whether any adult tenants own properties. Afterwards, transaction records can be checked daily. A tenant found to own a property should be immediately informed to move out within a short period of time, without allowing them to arrange for asset transfers. A tenant's family member owning a property must also be deregistered.

Moreover, tenancy heredity should be addressed. A public housing unit is a resource, not private property, recycled for the grassroots to improve their living environment and conditions. But once their income and assets increase, they should move out to keep the units circulating among other deserving individuals instead of inheriting them indefinitely.

However, the current public housing policy allows for the spouse and children under the age of 18 of a tenant's married child to be added to the household registration or a married and deregistered daughter to be registered again to provide care. Even though they must periodically declare their assets, it is unfair to those on the waiting list and worsens the heredity problem.

Adding name unfair to those waiting

If an elderly tenant requires someone to look after, the HD can grant a temporary residence permit to one of the children on humanitarian grounds. This is similar to hiring a domestic helper, but once the contract ends or the tenant passes away, the helper should leave instead of being added to the household registration. The HA should also seriously consider whether a unit can be transferred to a child after a tenant's death. After all, public housing is not private property. The tenants' children who are adults can apply on their own if they are eligible.

The inheritance has compounded the long-term misuse. The authorities should deal with it seriously to accelerate circulation and return to the original intent of public housing policies while adhering to social justice.

翻譯自5月9日《星島日報》社論
(http://std.stheadline.com/)

Vocabulary

ample (adj) —— 充足的
hereditary (adj) —— 世襲的
brainstorm (v) —— 集體研討
exploit (v) —— 利用
eviction (n) —— 趕走
periodically (adv) —— 定期地
compound (v) —— 加劇
adhere (v) —— 遵守

Useful Terms

grace period —— 寬限期
rental subsidy —— 租金補貼
random check —— 隨機抽查
humanitarian grounds —— 人道理由

Did you know?

Public housing tenants are deemed well-off if their household income exceeds five times of the monthly income cap or if they own asset 100 times of the cap. The income cap for a two-member household, for example, is $19,550 a month. A household of that size falls into this category if it earns $97,750 a month or has a net asset of $1.96 million.

Q&A

1. The word _____ in the first paragraph is the opposite of "relaxation".
2. The Housing Authority wants to shorten the temporary _____ period.
3. In the passage, the word _____ means "regularly".
4. A child looking after a public housing tenant should be given a _____ residence permit.
5. According to the last paragraph, the authorities should seriously deal with the public housing _____.

Answers 1. tightening 2. accommodation 3. periodically 4. temporary 5. inheritance

翻譯：George