Здравствуйте, друзья!

Сегодняшняя тема - КРИПТОГРАФИЯ, наука о кодах, взломах и шифрах. И мы рассмотрим, пожалуй, самый главный и самый распространенный в мире способ шифрования - который называется RSA. Именно этот способ шифрования лежит в основе современного интернета. Именно он защищает онлайн банки, банковские карты и все сайты с адресом, начинающимся на HTTPS://

Такие сайты надежно защищены, и любые данные - которыми Вы обмениваетесь с такими сайтами - не могут быть перехвачены посередине (например, Вашим интернет провайдером). Но самое интересное - что в основе этого всемирного шифрования лежит простая школьная задачка для 5-ого класса. Как только в начальной школе дети научатся делить числа - они быстро поймут - что есть такие числа, которые ни на что не делятся, кроме самих себя и единицы. Эти числа называются “простые” в противовес обычным числам - “составным”.

Вот эти числа 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, ….

Ирония судьбы состоит в том, что “простые” числа на самом деле самые сложные на свете и никому не известна точная закономерность их распределения среди всех чисел.

А теперь задачка для 5-ого класса:
возьмем 2 простых числа и перемножим их, например 137 и 199
решение:
137*199=27263 - делается элементарно в столбик за 1 операцию, под силу любому 5-и класснику

А теперь задачка обратная:
по числу 27263 найти те исходные числа, из которых оно образовано.
решение:
эта задача несоизмеримо сложнее первой, ведь для ее решения надо перебрать все возможные делители числа 27263 и на каждый из них сделать попытку деления. Т.е. сначала надо попробовать поделить 27263 на 2, потом на 3, потом на 4 и т.д. до 27262.

Как видим - прямая задачка потребовала 1 операцию умножения, а обратная требует 27261 операций деления.

Искушенный читатель заметит, что достаточно дойти всего лишь до половины - до числа 13631 в попытках деления, математик скажет что достаточно проверить до корня квадратного из 27263 - т.е. до 165. Но даже при таком раскладе это в 165 раз сложнее прямой задачки 5-ого класса.

Но изначально мы могли брать не 3-х значные простые числа, а скажем 100 значные простые (числа со 100 цифрами) - и тогда обратная задача даже для математика с его квадратным корнем была бы сложнее уже в 100 значное число раз (в 1 и 100 нулей раз)!!! И перебрать 1 и 100 нулей попыток деления немыслимо даже для самого мощного суперкомпьютера.

Сообщения в интернете шифруются за доли секунды, перемножая гигантские простые числа - но все-таки всего за 1 операцию. А для расшифровки требуется по огромному составному числу узнать его простые компоненты. И количество операций, нужных для этого, превышает возраст Вселенной в секундах.

Никто не умеет быстро раскладывать числа на простые множители. Никто не придумал быстрого способа решить задачку уровня 5-и классника. И задача эта остается нерешенной уже более 2-х тысяч лет со времен древних греков.

На том стоит криптография в интернете.

Создатели алгоритма шифрования RSA с момента его создания в 1970 и по настоящий момент - это группа из нескольких математиков из одного из американских университетов. С момента создания алгоритма в качестве патента за использования они получают 1 млрд долларов в год. Это пример того, как математика и программирование сами по себе могут приносить огромные деньги.

В нашей школе мы научим Вас не только программировать, но и использовать математику для придания реального смысла таким фантастическим закономерностям нашего мира, как простые числа. Сама природа породила такие удивительные законы - запрограммировав которые Вы не только заработаете много денег, но и сможете изменить мир.

მოგესალმებით, ძვირფასო მეგობრებო!
დღევანდელი თემა - კრიფტოგრაფია, მეცნიერება კოდების შესახებ, გატეხვებზე და შიპტებზე. ჩვენ განვიხილავთ, მსოფლიოში ყველაზე მთავარ და ყველაზე გავრცელებულ დაშიფრვის მეთოდს - რომელსაც RSA ეწოდება. დაშიფრვის ზუსტად ეს მეთოდი დევს ტანამედროვე ინტერნეტის საფუძველში. ზუსტად ეს იცავს ონლაინ ბანკებს, საბანკო ბარათებს და ყველა მისამართიან საიტებს, რომლებიც იწყება HTTPS://

ასეთი საიტები საიმედოდაა აცული და ყველა მონაცემები - რომლებსაც თქვენ აგზავნით ამგვარ საიტებზე - შეუძლებელია ვიღაცამ შუა გზაში დაიჭიროს(მაგალითად, თქვენმა ინტერნეტ პროვაიდერმა). მაგრამ ყველაზე საინტერესო არის ის - რომ ამ მსოფლიო დაშიფრვის ფუძეში დევს მეხუთე კლასის ამოცანა. როგორც კი დაწყებით სკოლაში ბავშვი ისწავლის რიცხვების გაყოფას - მისინი მალე გაიგებენ - რომ არის ისეთი რიცხვები რომლებიც არაფერზე არ იყოფა, გარდა თავისი თავისა და ერთზე. ამ რიცხვებს ეწოდებათ “მარტივი”, მათ საწინააღმდეგო რიცხვებს ეწოდებათ “შედგენილი”.

ეს რიცხვებია: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, ….

ბედის ირონია არის იმაში, რომ “მარტივი” რიცხვები ყველაზე რთული რიცხვებია მსოფლიოში და არავინ არ იცის მათი გადანაწილების კანონზომიერება სხვა რიცხვებს შორის.

ახლა კი მე-5 კლასის ამოცანა:
ავიღოთ ნებისმიერი 2 მარტივი რიცხვი და გავამავლოთ იგი მაგალითად, 137 და 199
პასუხი:
137*199=27263 - კეთდება ელემენტარულად სტოლბში 1 ოპერაციით, ნებისმიერი მე-5 კლასის მოსწავლისთვის.

ახლა კი შექცეული ამოცანა:
27263 რიცხვით ვიპოვოთ ის რიცხვები, რომლებისგანაც იგი წარმოიქმნა.

ამოხსნა:
ეს ამოცანა გაცილებით უფრო რთულია, ვიდრე პირველი, რადგან მისი ამოხსნისთვის უნდა გადავარჩიოთ ყველა 27263 რიცხვის გამყოფი და ყოველივე მათგანი უნდა ვცადოთ გავყოთ. ანუ 27263 უნდა ვცადოთ გავყოთ 2-ზე, 3-ზე, 4-ზე და ა.შ. 27263-მდე

როგორც ხედავთ - პირდაპირმა ამოცანამ გამრავლების მხოლოდ 1 ოპერაცია მოითხოვა, ხოლო შექცეულმა ამოცანამ - 27261 გაყოფის ოპერაცია.

მოხიბლული მკითხველი შეამჩნევს, რომ საკმარისია მივიდეთ მხოლოდ შუამდე - 13631 გაყოფის მცდელობაში, მათემათიკოსი იტყვის, რომ საკმარისია 27263-ის კვადრატულ ფუძემდე შემოწმება - ანუ 165-მდე. მაგრამ ამ შემთხვევაშიც ეს 165-ჯერ უფრო ძნელია, ვიდრე მე-5 კლასის პირდაპირი ამოცანა.

მაგრამ თავიდანჩვენ ჩვენ შეგვეძლო 3-ნიშნა მარტივი რიცხვის ნაცვლად აგვეღო 100-ნიშნა მარტივი რიცხვი (რიცხვები 100 ციფრით) - მაშინ შექცეული ამოცანა მათემათიკოსისთვისაც თავისი კვადრატული ფუძით იქნება 100-ნიშნა რიცხვით უფრო ძნელი!!! და გადავარჩიოთ 1 და 100 ნულიანი გაყოფის მცდელობა შეუსრულებელია ყველაზე ძლიერი სუპერკომპიუტერისთვისაც.

შეტყობინებები ინტერნეტში იშიფრება წამის მეოთხედში, გიგანტური მარტივი რიცხვების გადამრავლებით - მაგრამ მაინც გამრავლების 1 ოპერაციით. ხოლო დეშიფრაციისთვის სჭირდება მარტივი კომპონენტების გაგება. ამისთვის საჭირო, ოპერაციების რაოდენობა, აღემატება მსოფლიოს ასაკს წამებში.

არავის არ შეუძლია სწრაფად გარდაქმნას ნამრავლი ისევ მარტივ რიცხვებად. ვერავინ ვერ შეძლო მე-5 კლასის ამოცანის სწრაფი ამოხსნის მეთოდის ნახვა. ეს ამოცანა გაჩნდა 2 ათასი წლის წინ, ძველი ბერძნების დროს და იგი დღემდე ამოუხსნელი რჩება
ამაზე დგას კრიფტოგრაფია ინტერნეტში.

RSA დაშიფრვის ალგორითმის შემქმნელი, მისი შექმნის მომენტიდან 1970 და დღემდე - ეს არის ამერიკის უნივერსიტეტებიდან შემდგარი რამოდენიმე მათემათიკოსის ჯგუფი. ალგორითმის შექმნის მომენტიდან პატენტის გამოყენებაზე მათ წელიწადში გადაეცემათ 1 მილიარდი დოლარი. ეს არის იმის მაგალითი, თუ როგორ შეუძლია მათემათიკას და პროგრამირებას მოიტანონ უდიდესი შემოსავალი.

ჩვენ სკოლაში მარტო პროგრამირებას არ გასწავლით, ჩვენ გასწავლით მათემათიკის ისეთი ფანტასტიური კანონზომიერების გამოყენებას, როგორიცაა მარტივი რიცხვები.
თვითონ ბუნებამ შექმნა ისეთი გასაოცარი კანონბი - რომლის დაპროგრამებით თქვენ მარტო ბევრ ფულს კი არ იშოვით, არამედ შეძლებთ შეცვალოთ მსოფლიო.

Hello, everyone!

Today's topic is CRYPTOGRAPHY, the science about codes, hacks and ciphers. We consider, perhaps, the most important and most common encryption method in the world - which is called RSA.
This method of encryption is the basis of the modern Internet. It is what protects online banks, bank cards and all the sites with an address starting with https: //

Such sites are securely protected, and any data - that you exchange with such sites - can not be intercepted in the middle (for example, by your Internet provider). But the most interesting thing is that the basis of this world-wide encryption is a simple school task for the 5th grade pupils. As soon as in elementary school, children will learn how to divide numbers — they will quickly understand that there are numbers that are not divided by anything except themselves and one. These numbers are called "prime" numbers as opposed to "compound" numbers.

These numbers are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 , 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199,….

The irony of fate is that in fact the "prime" numbers are the most complex in the world and nobody knows the exact pattern of their distribution among all numbers.

The problem for 5th grade pupils is given here:
We just take 2 prime numbers and multiply them, let them be 137 and 199
The solution of this problem is: 137 * 199 = 27263 - the result of this expression is computed easily using only 1 operation,
all 5th grade pupils are capable to solve that

At this time we reverse the problem mentioned above:
Find two numbers whose result of multiplication is number 27263

The solution is:
This task in comparison with previous one is more difficult to solve, because it is necessary to take all possible divisors of the number 27263 and perform operation of division. At the first step we must try to divide the number 27263 by 2, then by 3, then by 4, till 27262.

As you can see, the direct problem requires 1 operation of multiplication, and the reverse one requires 27261.

The sophisticated reader will notice that it is enough to reach only half - to the number 13631 in the attempts of division, the mathematician will say that it is enough to check to the square root of 27263 - i.e. to 165. But even in this situation, it is 165 times more difficult than the direct problem of the 5th grade.

But initially we could take not 3-digit prime numbers, but let's say 100-digit prime numbers (numbers with 100 digits) - and then the inverse problem even for a mathematician with its square root would be more difficult even 100-digit number times (1 and 100 zeros once) !!! And going through 1 and 100 zero division attempts is unthinkable even for the most powerful supercomputer.

Messages on the Internet are encrypted in a fraction of a second, multiplying giant prime numbers - but still in just 1 operation. And for decryption it is required to learn its simple components by a huge composite number.
And the number of operations needed for this is greater than the age of the Universe in seconds.

No one can quickly decompose numbers into prime factors. No one came up with a quick way to solve a 5th grade level puzzle. And this task remains unresolved for more than two thousand years since the time of the ancient Greeks.
On that there is standing a cryptography in the Internet.

The creators of the RSA encryption algorithm from 1970 to the present time are a group of several mathematicians from an American university. Since this time the creators earn USD 1 billion a year by permitting to use their cryptographic algorithm worldwide. This is an example of how mathematics and programming together can help us to make a lot of money.

In our school we will teach you not only to code programs of any complexity, but also to use mathematics to give real meaning to such fantastic laws of our world like "prime" numbers. Nature itself has generated such amazing laws - that by programming them you will not only earn a lot of money, but will also be capable to change the entire world.