Абсолютное шифрование (одноразовые блокноты)

Привет, друзья!

Сегодня речь снова пойдет о криптографии. Только теперь мы Вам расскажем то - что Вас поистине удивит. Как Вы думаете - любой ли на свете шифр можно взломать?

Вот, например, возьмем из прошлых статей знаменитый метод шифрования RSA, обеспечивающий безопасность всего интернета. Для взлома он требует просто космических вычислительных мощностей - и все-таки теоретически взломать его можно за очень долгое время. Особенно если люди изобретут квантовые компьютеры - обладающие почти неограниченной вычислительной мощностью.

И все-таки если представить, что квантовые компьютеры созданы и вычислительные мощности станут бесконечными - останется ли хоть один способ по-прежнему надежно шифровать информацию?

Ответ - да, такой способ есть. И называется он - Абсолютное шифрование или Одноразовые Блокноты. И что удивительно - он еще проще чем RSA. Понять его может даже ученик начальной школы.

Рассмотрим следующую схему (в конце чисел в скобках напишем остатки от деления на 2: так у нечетных чисел остаток при делении на 2 = 1, у четных чисел = 0)

четное (0) + четное (0) = четное (0), пример 4+6=10
нечетное (1) + нечетное (1) = четное (0), пример 3+7=10
нечетное (1) + четное (0) = нечетное (1), пример 3+6=9
четное (0) + нечетное (1)= нечетное (1), пример 6+3=9

Получается такая арифметика сложения остатков от деления на 2:

0+0=0
1+1=0
1+0=1
0+1=1

Теперь представим, что наше сообщение, которое мы хотим зашифровать и передать - состоит из 0 и 1, например такое

0 1 1 1 0 1 0 0 1 - это исходное сообщение

Для зашифровки возьмем случайный набор 0 и 1, равный по длине шифруемому сообщению - назовем этот набор одноразовый блокнот:
1 0 1 1 0 1 0 1 1 - это блокнот

И сделаем по столбцам операцию сложения в арифметике остатков
0 1 1 0 1 0 0 1 - это исходное сообщение
1 0 1 0 1 0 1 1 - это блокнот
_____
1 1 0 0 0 0 1 0 - это зашифрованное сообщение.

А теперь внимание - как по этому сообщение можно узнать, какое сообщение было исходным? Ответ - никак!!! - если у Вас нет одноразового блокнота.

Действительно, в первой позиции зашифрованного сообщения стоит 1, из чего она могла получиться в исходном сообщении? Из 0, если в блокноте была 1 (как в первом столбце). Из 1, если в блокноте был 0 (как во 2-м столбце)

В третьей позиции зашифрованного сообщения стоит 0, из чего он мог получиться в исходном сообщении? Из 1, если в блокноте была 1 (как в 3-м столбце). Из 0, если в блокноте был 0 (как во 4-м столбце)

То есть еще раз - в зашифрованном сообщении 0 мог получиться из чего угодно (из 0 или 1 в исходном сообщении) - все зависит от блокнота, и 1 могла получиться из чего угодно (из 0 или 1 в исходном сообщении) - все зависит от блокнота
Т.е. прообразом зашифрованного сообщения мог быть абсолютно любой набор 0 и 1 - в котором могла быть зашифрована абсолютно любая информация! Это в равной мере могли быть как сверхсекретные данные, так и стихи знаменитого поэта.

Чтобы расшифровать сообщение - надо сделать все наоборот - к зашифрованному сообщению снова применить одноразовый блокнот - и получится исходное сообщение:

1 1 0 0 0 0 1 0 - это зашифрованное сообщение.
1 0 1 0 1 0 1 1 - это блокнот

_____
0 1 1 0 1 0 0 1 - это исходное сообщение

Этот способ шифрования невозможно взломать никак, если не иметь шифрующего и того же самого дешифрующего блокнота. Блокноты называются одноразовыми, потому как в целях безопасности рекомендуется для каждого нового сообщения использовать новый блокнот.

Так почему же тогда в шифровании интернета применяют RSA? Одна из основных причин - это то, что блокноты должны быть такими же длинными, как шифруемые сообщения. Это ведет к перерасходу трафика. В то время как в RSA даже 100 значные простые числа относительно малы в сравнении с гигантскими объемами трафика передаваемого в интернете. И кроме того, абсолютное шифрование - это симметричное шифрование - один и тот же блокнот (ключ) используется как для шифровки - так и для дешифровки сообщения. RSA - это редкий пример ассиметричного шифрования - где ключи шифровки и дешифровки - разные - и это эффективнее. Но это тема для отдельных статей.

И тем не менее - все эти никак не умаляет того факта, что сообщения, зашифрованные одноразовыми блокнотами - расшифровать невозможно в принципе. Сколь бы мощными компьютерами Вы ни пользовались.

აბსოლუტური კოდირება (ერთჯერადი ბლოკნოტები)

გამარჯობა მეგობრებო!

დღეს კვლავ ვისაუბრებთ კრიპტოგრაფიის შესახებ. მხოლოდ ახლა ჩვენ ვისაუბრებთ იმაზე, რაც ნამდვილად თქვენ გაგაოცებთ. როგორ ფიქრობთ - შეიძლება თუ არა ნებისმიერი შიფრის გატეხვა?

მაგალითად, განვიხილოთ წარსულ სტატიებიში ცნობილი შიფრაციის მეთოდი RSA, რომელიც უზრუნველყოფს მთელი ინტერნეტის უსაფრთხოებას. მაგის გატეხვისთვის საჭირო იქნება კოსმიური მოცულობის გამოთვლითი სიმძლავრე, თეორიულად ეს შესაძლებელია ძალიან დიდი ხნის განმავლობაში გაიტეხოს.
მით უმეტეს, თუ ადამიანები კვანტურ კომპიუტერებს გამოიგონებენ- რომლებსაც თითქმის შეუზღუდავი გამოთვლითი სიმძლავრე გააჩნდებათ.

და მაინც, წარმოიდგინეთ, რომ კვანტური კომპიუტერები შეიქმნა და კომპიუტერული ძალაუფლება უსასრულო გახდება -დარჩება თუ არა გზა ინფორმაცია საიმედოდ დავიცვათ?

პასუხი - კი, დიახ, არსებობს ასეთი გზა და მას უწოდებენ -აბსოლუტურ კოდირებას ან ერთჯერად ბლოკნოტს და რა საკვირველია - იგი უფრო მარტივია, ვიდრე RSA. მის გაგებას შეძლებს თუნდაც დაწყებითი სკოლის მოსწავლე.

განვიხილოთ შემდეგი სქემა (რიცხვების ბოლოში დაწეროთ 2-ზე გაყოფის შედეგად მიღებული ნაშთები: ლუწი რიცხვის 2-ზე გაყოფის შედეგეგად მიღებული ნაშთი არის 0, ხოლო კენტის - 1)

ლუწი (0) + ლუწი(0) = ლუწი (0), მაგალითად 4+6=10
კენტი (1) + კენტი (1) = ლუწი (0),მაგალითად 3+7=10
კენტი(1) +ლუწი (0) = ლუწი (1),მაგალითად 3+6=9
ლუწი(0) + კენტი(1) = კენტი (1), მაგალითად 6+3=9

გამოდის 2-ზე გაყოფის შედეგად მიღებული ნაშთების შეკრების არითმეტიკა:

0+0=0
1+1=0
1+0=1
0+1=1

ახლა წარმოიდგინეთ, რომ ჩვენი გზავნილი, რომელიც ჩვენ გვინდა დავშიფროთ და გადავცეთ - შედგება ნულებისგან და ერთებისგან. ეხლა წარმოიდგინეთ, რომ ჩვენი გზავნილი, რომელიც თქვენ გინდათ დაშიფროთ და გადასცეთ - შედგება ნულებისგან და ერთებისგან, მაგალითად ესეთი

0 1 1 1 0 1 0 0 1 - ეს არის თავდაპირველი შეტყობინება

დაშიფრისთვის ავიღოთ შემთხვევითი კომპლექტი 0 და 1, სიგრძე ტოლია დაშიფრული შეტყობინებას - მოდით დავარქვათ ამ კომპლექტს ერთჯერადი ბლოკნოტი:
1 0 1 1 0 1 0 1 1 - ეს არის ბლოკნიტი

და ჩვენ გავაკეთებთ დამატებით ოპერაციას სვეტების ნარჩენი არითმეტიკას
0 1 1 0 1 0 0 1 - ეს არის თავდაპირველი შეტყობინება
1 0 1 0 1 0 1 1 - ეს ბლოკნოტია
_____
1 1 0 0 0 0 1 0 - ეს დაშიფრული შეტყობინებაა.

და ახლა ყურადღება -როგორ შეიძლება ამ შეტყობინებით გავიგოთ, რომელი არი თავდაპირველი შეტყობინება? პასუხი არნაირად!!! - თუ არ გაქვთ ერთჯერადი ბლოკნოტი.

მართლაც, დაშიფრული შეტყობინებების პირველ პოზიციაში არის 1, რა შეიძლება იყოს ეს თავდაპირველი შეტყობინება? 0 გან, თუ ბლოკნოტში იყო 1 (როგორც პირველ სვეტში). 1დან, თუ ბლოკნოტში იყო 0 (როგორც მეორე სვეტში)

დაშიფრული შეტყობინების მესამე პოზიციაში არის 0, რისგან შეიძლება იყოს ეს ორიგინალური შეტყობინება? 1 სგან, თუ ბლოკნოტში იყო 1 (როგორც მე 3 სვეტში). 0 გან, თუ ბლოკნოტში იყო 0 (როგორც მე 4 სვეტში)

კიდევ ერთხელ- დაშიფრულ შეტყობინებაში 0 ის მიღება შეგვეძლი ნებისმიერი წიფრიდან (0 დან ან 1 თავდაპირველ გზავნილში) - ყველაფერი დამოკიდებულია ბლოკნოტზე, და 1 შესაძლებელია მივიღოთ რისგანაც გნებავთ. (0 დან ან1 в თავდაპირველი შეტყობინება) - ეს ყველაფერი დამოკიდებულია ბლოკნოტზე

ე.ი პროტოტიპი დაშიფრული შეტყობინების შეიძლება იყოს აბსოლუტურად ნებისმიერი კომპლექტი 0 და 1 - რომელშიც აბსოლუტურად ნებისმიერი ინფორმაცია შეიძლება დაშიფრული იყოს! ეს შეიძლება იყოს თანაბრად საიდუმლო მონაცემები ან ცნობილი პოეტის ლექსები.
იმისათვის რომ გავშიფროთ შეტყობინება- ყველაფერი უნდა გავაკეთოთ პირიქით - დაშიფრულ შეტყობინებისთვის კვლავ გამოვიყენოთ ერთჯერადი ბლოკნოტი - და მაშინ გამოვა თავდაპირველი შეტყობინება:

1 1 0 0 0 0 1 0 - ეს დაშიფრული შეტყობონებაა.
1 0 1 0 1 0 1 1 - ეს ბლოკნოტია

_____
0 1 1 0 1 0 0 1 - ეს თავდაპირველი შეტყობინებაა

ეს დაშიფვრის მეთოდი შეუძლებელია გატყდეს თუ არ გაქვთ დაშიფვრა და იგივე გაშიფვრის ბლოკნოტი.
ბლოკნოტებს ერთჯერადს უწოდებენ, რადგან უსაფრთხოების მიზეზების გამო რეკომენდირებულია გამოიყენოს ახალი ბლოკნოტი ყოველ ახალი შეტყობინებისთვის.

მაშ რისთვის იყენებენ ინტერნეტის დაშიფრისთვის RSA? ერთ-ერთი მთავარი მიზეზია-ბლოკნოტი უნდა იყოს იგივე სიგრძის რაც არის დაშიფრული შეტყობინება ეს იწვევს ტრაფიკის გადამეტებას.
RSA- ში ყოფნისას კი 100-ზე მეტი რიცხვი შედარებით მცირეა, ვიდრე ინტერნეტში ტრანსპორტირების დიდი რაოდენობით.გარდა ამისა,აბსოლუტური კოდირება - ეს არის სიმეტრიული კოდირება - ერთი და

იგივე ბლოკნოტი (გასაღები) გამოიყენება როგორც დაშიფრისთვის - ასევე შეტყობინების გაშიფრისთვის. RSA -ეს არის ასიმეტრიული დაშიფვრის იშვიათი მაგალითი. -სადაც დაშიფვრის და დეშიფრაციის გასაღებები განსხვავებულია - და ეს უფრო ეფექტურია. მაგრამ ეს არის ცალკეული სტატიების თემა.

და მაინც - ეს ყველაფერი არანაირად არ ამცირებს იმ ფაკტს, რომ შეტყობინებები რომელიცა დაშიფრულია ერთჯერადი ბლოკნოტებით, პრინციპში შეუძლებელია იყოს გაშიფრული - არ აქვს მნიშვნელობა, თუ რამდენად ძლიერი კომპიუტერს იყენებთ.

Absolute encryption (one-time notepads)

Hello friends!

Today we will talk again about cryptography. But now we will tell you something that truly surprises you. Do you think that any cipher in the world can be hacked?

Here, for example, take from past articles the famous RSA encryption method that ensures the security of the entire Internet. For hacking, it just requires space computing power - and yet, theoretically, it can be hacked in a very long time. Especially if people invent quantum computers - with almost unlimited computing power.

And yet, if you imagine that quantum computers are created and the computing power becomes infinite - will there be at least one way to still securely encrypt information?

The answer is yes, there is such a way. And it is called Absolute Encryption or one-time Notepads. And surprisingly, it is even easier than RSA. Even an elementary school student can understand it.

Consider the following scheme (at the end of the numbers in brackets we write the remainder of division by 2: so for odd numbers, the remainder when divided by 2 = 1, for even numbers = 0)

even (0) + even (0) = even (0), example 4 + 6 = 10
odd (1) + odd (1) = even (0), example 3 + 7 = 10
odd (1) + even (0) = odd (1), example 3 + 6 = 9
even (0) + odd (1) = odd (1), example 6 + 3 = 9

It turns out this arithmetic of addition of residues from division by 2:
0+0=0
1+1=0
1+0=1

0+1=1

Now imagine that our message that we want to encrypt and transmit - consists of 0 and 1, for example

0 1 1 1 0 1 0 0 1 - this is the original message

To encrypt take a random set of 0 and 1, equal in length
encrypted message - we will call this set a one-time notepad:
1 0 1 1 0 1 0 1 1 - this is a one-time notepad

And make the addition operation in columns in the arithmetic of the residuals
0 1 1 0 1 0 0 1 - this is the original message
1 0 1 0 1 0 1 1 - this is a one-time notepad
_____
1 1 0 0 0 0 1 0 - This is an encrypted message.

And now attention - how can you find out about this message, which message was the original one? The answer is no way !!! - If you do not have a one-time notepad.

Indeed, in the first position of the encrypted message is 1, from which it could come in the original message? From 0, if the notebad was 1 (as in the first column). From 1, if the notepad was 0 (as in the 2nd column)

In the third position of the encrypted message is 0, from which it could turn out in the original message? From 1, if the notepad was 1 (as in the 3rd column). From 0, if the notepad was 0 (as in the 4th column)

That is, once again - in an encrypted message, 0 could come out of anything (from 0 or 1 in the original message) - it all depends on the notepad, and 1 could come out of anything (from 0 or 1 in the original message) - everything depends on the notepad

That is absolutely any set of 0 and 1 could be a prototype of an encrypted message - in which absolutely any information could be encrypted! It could be equally as top-secret data, and poems of the famous poet.

To decrypt a message — you must do the opposite — again, apply a one-time notepad to the encrypted message — and you'll get the original message:

1 1 0 0 0 0 1 0 - This is an encrypted message.
1 0 1 0 1 0 1 1 - this is a one-time notepad
_____
0 1 1 0 1 0 0 1 - this is the original message

This encryption method is impossible to crack in any way, if you do not have an encrypting and the same decrypting notepad.
Notepads are called one-time, because for security purposes it is recommended to use a new notepad for each new message.

So why, then, use RSA in Internet encryption? One of the main reasons is that notepads should be as long as encrypted messages. This leads to traffic overspending. While in RSA, even 100-digit prime numbers are relatively small compared to the huge amounts of traffic transmitted on the Internet. And besides, absolute encryption is symmetric encryption - the same notepad (key) is used for both encryption and decryption of a message. RSA is a rare example of asymmetric encryption — where encryption and decryption keys are different — and this is more efficient. But this is a topic for individual articles.

And nevertheless - all these in no way detract from the fact that messages encrypted with one-time notepads cannot be decrypted in principle. No matter how powerful computers you use.