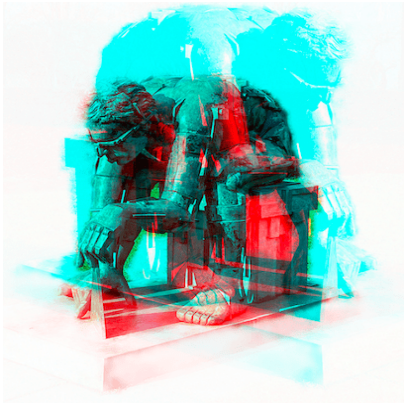


RSA public key encryption

Description

Iâ??m continuing this dive into public-private key encryption. As outlined in a helpful blog post by Nick Sullivan, the kind of encryption I described in the last two posts relies on a simple property of numbers. Itâ??s easy to multiply two numbers, even if very large, but more difficult to factor a number, i.e. find two numbers that when multiplied result in that number. Itâ??s especially difficult if the two numbers multiplied are primes. They will be the unique factors of their product. So thereâ??s only one solution to the factor challenge for a number so produced. Factoring is a trivial calculation for small prime products, but is computationally taxing for prime products over 100 digits long.

The procedure recounted in this and the previous post exploit this property of very large prime numbers. The property is used to generate two numbers: a public key number and a private key number. Sullivan says

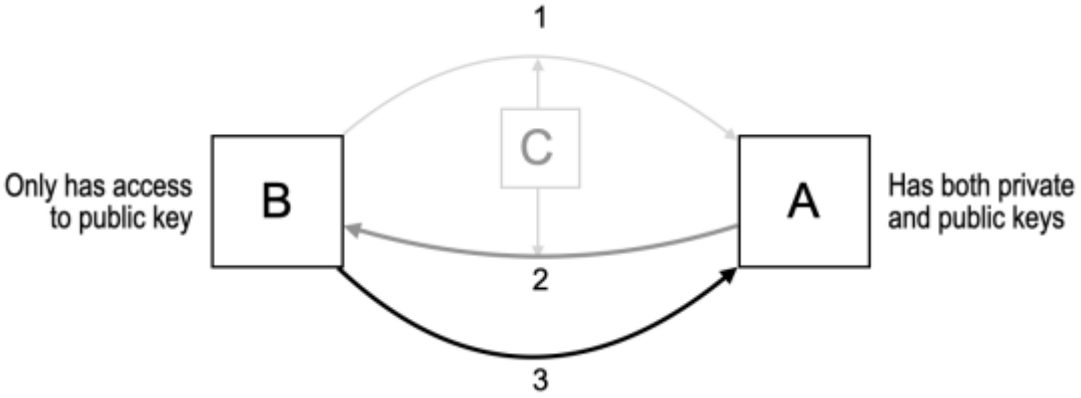
> â??The takeaway is that you can take a number, multiply it by itself a number of times to get a random-looking number, then multiply that number by itself a secret number of times to get back to the original number.â?•

RSA recap

Person B wants to send person A a secret message and so asks A for Aâ??s public encryption key. Person A transmits Aâ??s public encryption key to B to facilitate this. Person B uses that public key information to encode a message according to the algorithm described below. Person A has the private key and can decode the message. Three items are transferred in sequence.

1. Bâ??s initial low security request for Aâ??s public key.
2. The public key transferred from A to B which is low risk. It doesnâ??t matter if hacker C intercepts that transfer and finds out what the public key is. All that would enable C to do at best is to encrypt a message; not to decrypt a message.
3. The encrypted message from B to A which is secure. A can read this with the private encryption key. The message could only be read by C if C had the private key. The private key is never

transmitted and stays with A.



These operations are of course invisible to the device user, and are the kinds of operations carried out by browser and server software in requesting and transmitting information securely across the Internet. Hereâ??s the algorithm from the previous post for encrypting a message using prime numbers.

- choose ***p*** and ***q*** large primes
- ***n*** = ***p***.***q***
- ***z*** = (***p***-1).(***q***-1)
- choose ***e*** such that ***e*** < ***n*** and **z** mod **e** â? 0
- choose large number ***d*** such that ***d*** < ***n*** and ***d***.***e*** mod ***z*** = 1
- transmit the public encryption key = [***n***, ***e***]
- convert a text message to a number ***m***
- convert ***m*** to encrypted form ***c***
- ***c*** = m^e mod ***n***

Sullivan notes that ***n*** is a maximum value for ***c***. So, the mod calculation implies a looping operation that ignores the repeated components up to the max ***n*** and only takes the remainder that is less than the max.

> â??We can make sure that the numbers we are dealing with do not get too large by choosing a maximum number and only dealing with numbers less than the maximum. We can treat the numbers like the numbers on an analog clock. Any calculation that results in a number larger than the maximum gets wrapped around to a number in the valid range.â?•

The following is the â??reverseâ?• operation for recovering the message.

- the recipient recovers the message ***c*** with the private encryption key [***n***, ***d***]
- ***m*** = c^d mod ***n***

Codebreakers without the public key wonâ??t know ***d***. If they could discover ***m*** by some other means then they might be able to derive ***d*** and thereby decode other messages. But the codebreaking software would have to iterate through every possible value of ***d*** to reproduce the message ***m***. If ***d*** is very large, say 100 digits long, then even with supercomputer speeds there would be insufficient time in the projected duration of the universe to complete the task. See the quote in earlier post about the computational challenge. Some cryptography experts think that quantum computers may break that

constraint. See post: Quantum Internet.

This method of encryption is called RSA encryption after the three inventors, Ron Rivest, Adi Shamir, and Leonard Adleman (1977). The more recent (2004) ECC encryption method (Elliptic-curve cryptography) supports shorter keys and is more efficient for communications that involve mobile devices.

Reference

- Sullivan, Nick. 2013. A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography. *The Cloudflare Blog*, 24 October. Available online: https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/ (accessed 6 May 2021).

Category

1. Architecture

Tags

1. cryptography
2. prime numbers

Date Created
May 22, 2021
Author
rcoyne99