Tr

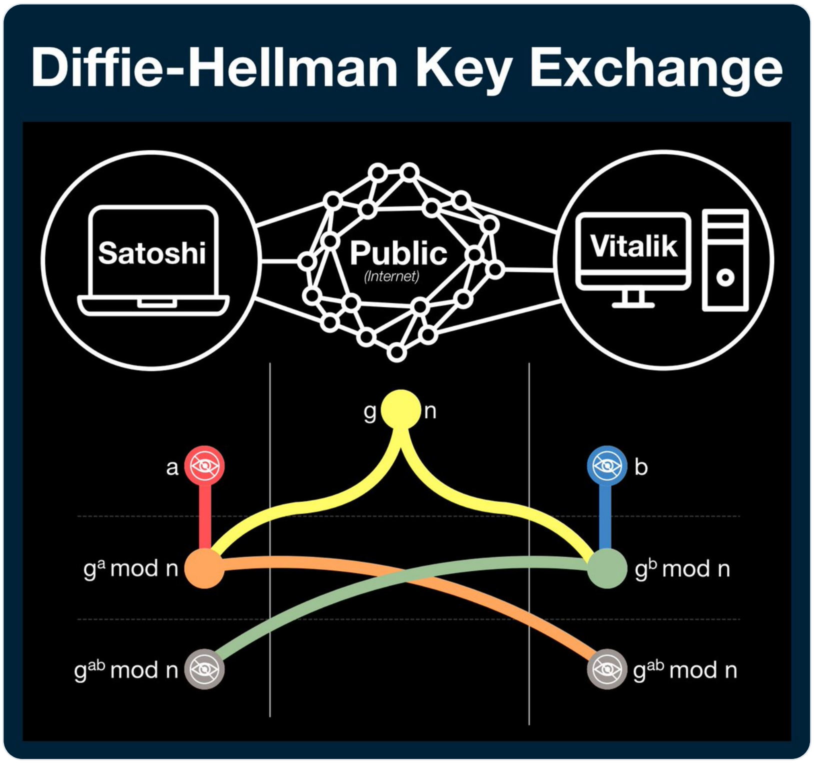
Haym @SalomonCrypto

Oct 13 • 22 tweets • SalomonCrypto/status/1580388773937881093

(1/21) Cryptography Fundamentals: Diffie-Hellman Key Exchange

How do you share private information over public networks? How can we create mathematically secure secrets? What actually is an encryption key?

A public guide for private communication.



(2/21) Let's say you need to communicate sensitive data across a public channel. If you know other people can read your data, you might decide to cryptographically encode it.

Encoding is the process of transforming the original data into an undecipherable (but reversible) form.

(3/21) Encoding is only useful in one condition: if (ONLY) the intended recipient can decode the message, transforming it back into its original form.

If we can pull this off, we can securely share sensitive data even while broadcasting it to the entire world.

(4/21) In order to do this, we use a cryptographic algorithm. A cryptographic algorithm receives a message and an encryption key.

If the message is not encrypted, the algorithm will encode it.

If the message is encrypted, the algorithm will decode it.

(5/21) We will just take the cryptographic algorithm for granted; you can just treat it like a black box. We are interested in the encryption key.

More specifically, we are interested in understanding how to create a key.

(6/21) Due to the nature of a cryptographic algorithm, anyone with the encryption key is able to decode the message.

If you don't have a private channel to create/agree upon the key, how can do it in the open?

How do you establish a shared secret in public?

(7/21) Our answer comes from over 40 years ago by Whitfield Diffie and Martin Hellman: Diffie-Hellman Key Exchange.

This scheme was the first method of creating a shared secret that didn't require the literal physical exchange of encryption keys (via paper, disk, etc).

(8/21) Before we get started, we need to cover some basic math (don't worry, it's not bad)

When you divide two integers, sometimes the result is not an integer (eg has a reminder). Modular arithmetic is a branch of math that is focused on the reminder

What is modular arithmetic? (article) | Khan Academy

https://www.khanacademy.org/computing/computer-science/cr…

(9/21) The modulo operator (written as "mod") is the operation that finds the remainder.

10 / 3 = 3 with a remainder of 1 = 10 mod 3 = 1
14 / 6 = 2 with a remainder of 2 = 14 mod 6 = 2
3 / 10 = 0 with a remainder of 3 = 3 mod 10 = 3

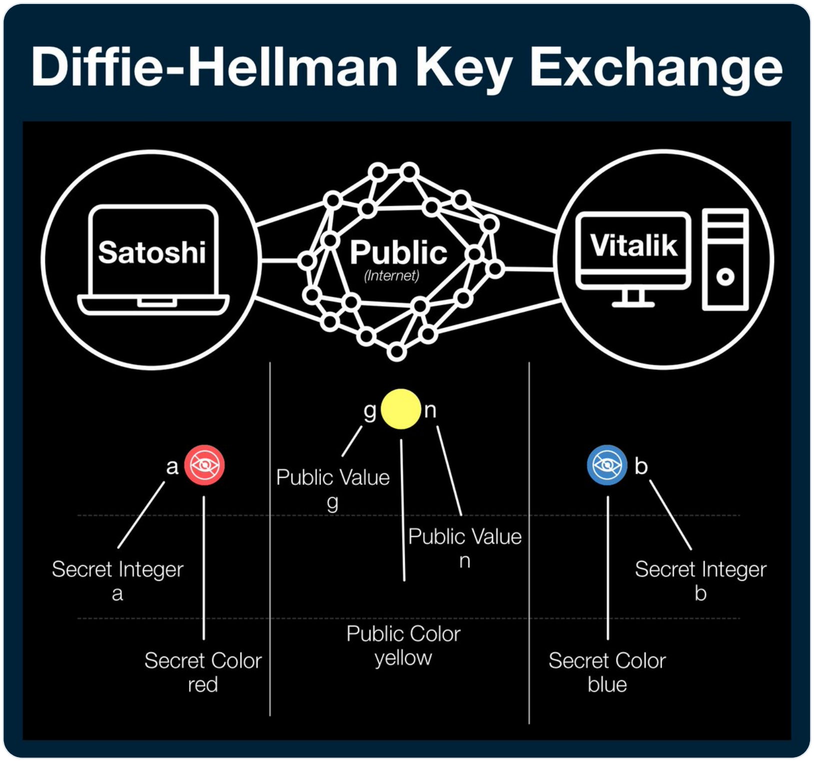
Imagine a clock being mod 12.

(10/21) Ok, that's it! All the math you need.

Is that too much? No worries! Diffie-Hellman has a classic metaphor that is very helpful: mixing paint. In the metaphor, the goal is to create a secret color that only the participants know.

(11/21) Diffie-Hellman begins with two parties (Satoshi, Vitalik), a public data channel and two publicly available numbers: g and n (yellow).

g and n are either agreed upon before hand, using some industry standard, or are agreed upon in public before the process starts.

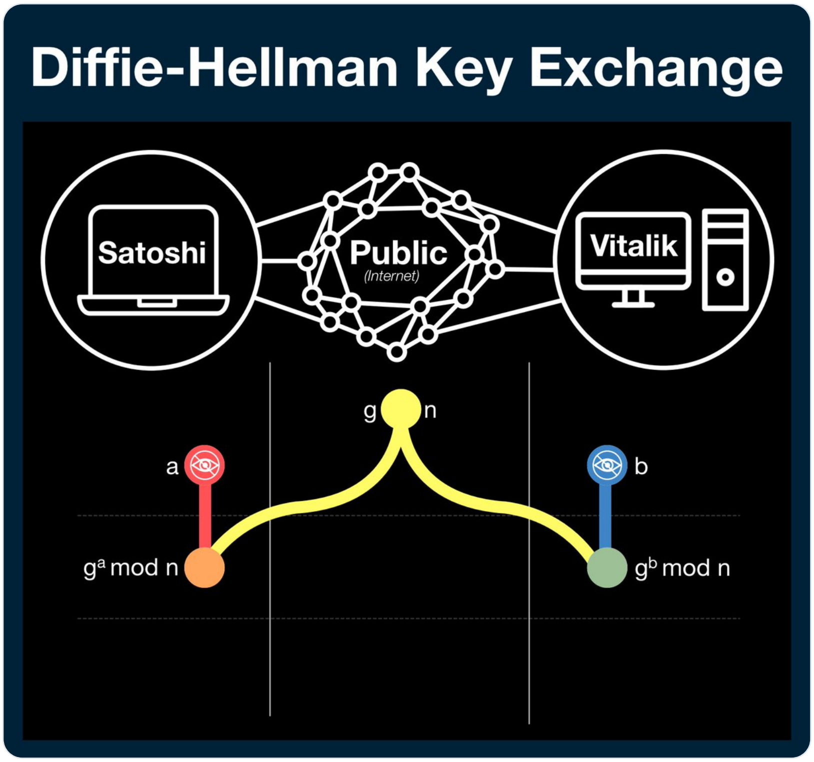


(12/21) Both parties have a secret number (Satoshi - a, red) (Vitalik - b, blue). These numbers are the keys to every message sent by their owner; their privacy is paramount.

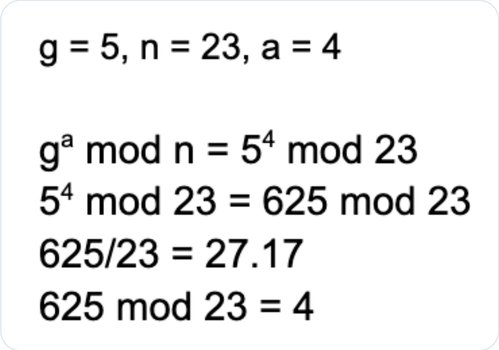
(13/21) To begin the process, both parties import the publicly available data (g and n - yellow) and apply their secret number.

The formula below is a little scary; let me break it down.

All we are doing is multiplying g by itself a/b times and then applying mod n.

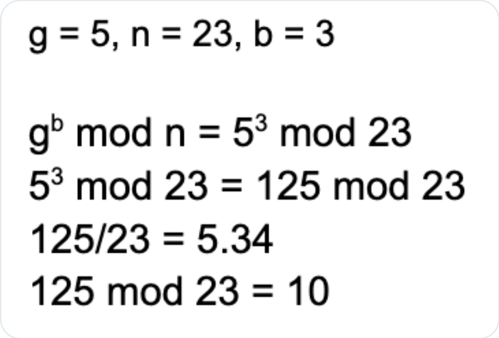


(14/21) Here is a concrete example:



$g = 5, n = 23, a = 4$

$g^a \bmod n = 5^4 \bmod 23$
$5^4 \bmod 23 = 625 \bmod 23$
$625/23 = 27.17$
$625 \bmod 23 = 4$

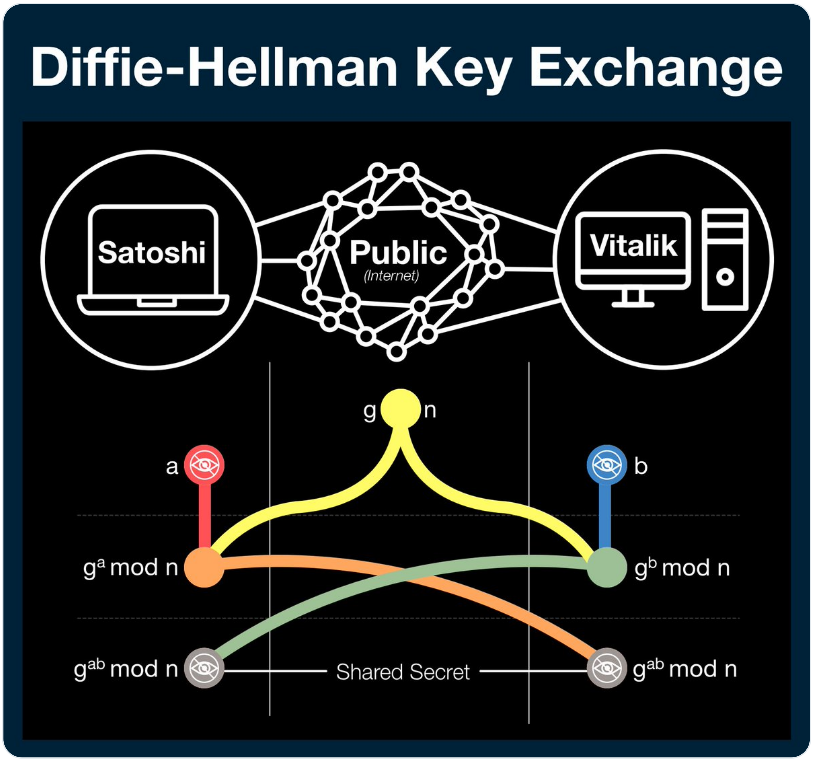


$g = 5, n = 23, b = 3$

$g^b \bmod n = 5^3 \bmod 23$
$5^3 \bmod 23 = 125 \bmod 23$
$125/23 = 5.34$
$125 \bmod 23 = 10$

(15/21) Next, both parties will send this new value back across the public channel.

At this point both values become public, however no observer can recover the original data. The critical piece is the modulo function.



(16/21) Let's think about a clock as a system with mod 12.

Just because you know we start at 4 (g) and where we end at 6 (g^a mod n) doesn't give you enough information to know how long we lasted: 2 hours? 14 hours? 26 hours?

g^a mod n is the same problem!

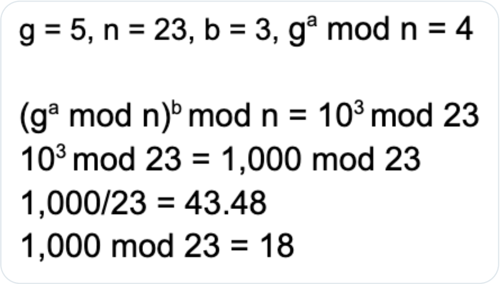
(17/21) It turns out there isn't a great way to do this other to just start guessing. Our examples are using tiny numbers, but in practice these values would be hundreds of digits long.

Guessing is not just difficult, its nearly impossible (although that's becoming less true).

(18/21) Once both parties have this intermediate value, they can repeat the process they used to make it: multiply the new value a/b times and take the remainder when you divide by n.

Here's where the magic happens: Now you both have the same number; a number no one else knows.

(19/21) Here is a concrete example:



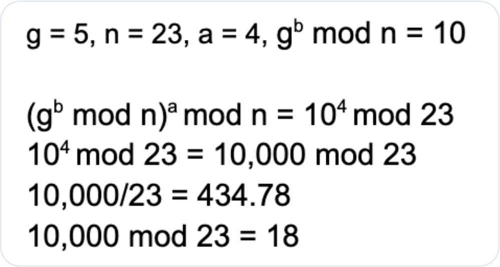
$g = 5$, $n = 23$, $b = 3$, $g^a \bmod n = 4$

$(g^a \bmod n)^b \bmod n = 10^3 \bmod 23$

$10^3 \bmod 23 = 1{,}000 \bmod 23$

$1{,}000/23 = 43.48$

$1{,}000 \bmod 23 = 18$



$g = 5$, $n = 23$, $a = 4$, $g^b \bmod n = 10$

$(g^b \bmod n)^a \bmod n = 10^4 \bmod 23$

$10^4 \bmod 23 = 10{,}000 \bmod 23$

$10{,}000/23 = 434.78$

$10{,}000 \bmod 23 = 18$

(20/21) And so, after you complete the Diffie-Hellman key exchange process, both parties have a shared secret. They both can be confident that they (and only they) will the only ones able to read messages that use that value as an encryption key.

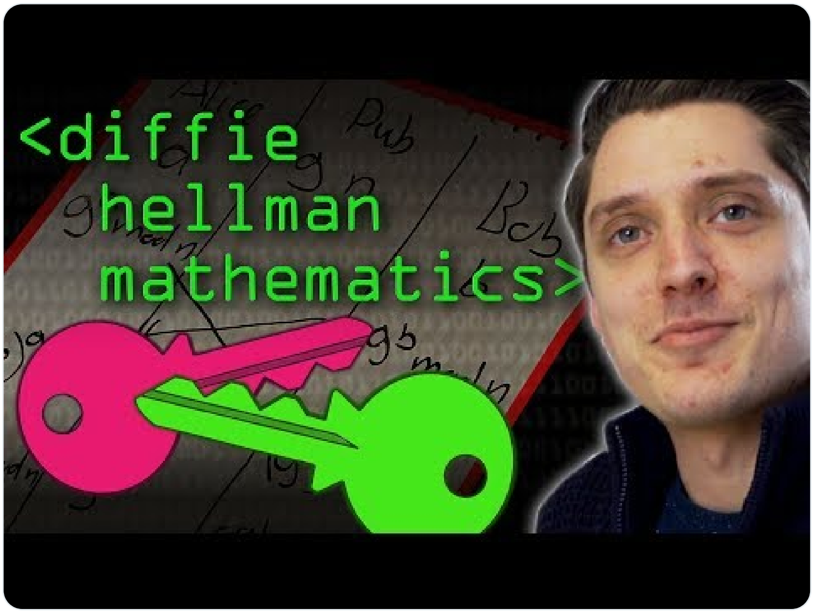
A public secret!

(21/21) Audio/video learner? No problem! @computer_phile has got you covered!

Classic paint metaphor:

https://www.youtube.com/embed/NmM9HA2MQGI

Actual math:



https://www.youtube.com/embed/Yjrfm_oRO0w

Like what you read? Help me spread the word by retweeting the thread (linked below).

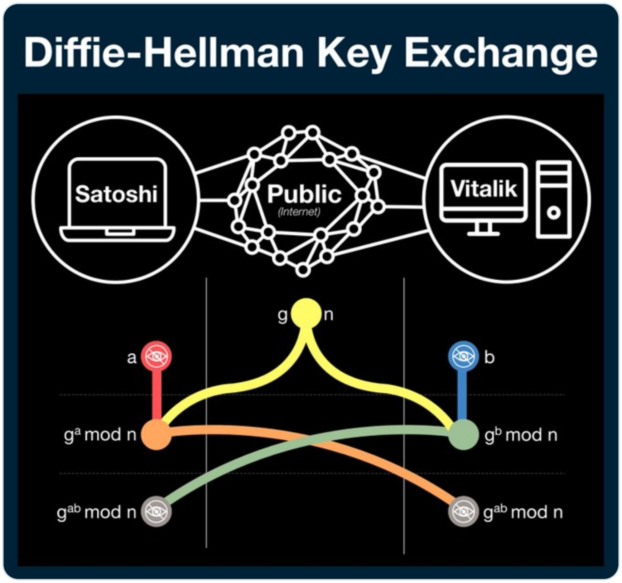
Follow me for more explainers and as much alpha as I can possibly serve.

Haym
@SalomonCrypto · **Follow**

(1/21) Cryptography Fundamentals: Diffie-Hellman Key Exchange

How do you share private information over public networks? How can we create mathematically secure secrets? What actually is an encryption key?

A public guide for private communication.



2:43 AM · Oct 13, 2022

Read the full conversation on Twitter

433 Reply Copy link

Read 26 replies

• • •