Maths Modelling and Problem Solving: Cryptography Project

Ricardo Jesús Palomino Piepenborn

The University of Manchester

Wednesday 23rd of June, 2021

Who is Ricardo?

- Originally from Spain.
- Finished a 4 year MMath degree at The University of Manchester in 2020.
- Currently a PhD student in Mathematical Logic also at The University of Manchester.
- Research on deploying tools from Model Theory (and area of Mathematical Logic) to understand certain objects (real closed rings) appearing in Algebra.

What is Cryptography?

- Cryptography (or cryptology) is the scientific study of sending secret information.
- Various methods have been used throughout history to code secret information with varying degrees of security: from the Caesar cipher (used by the Roman emperor Julius Caesar in his private correspondence), to the Enigma code (used by the German military to encode messages before and during World War II).
- Most coding schemes rely on sharing “keys” (strings of data, usually numbers, letters or a combination of both) which have to be shared before sending any information.

What is Cryptography?

- A modern scheme is the RSA cipher (RSA standing for Rivest, Shamir and Aldeman, the surnames of their inventors). It used to encode information used in internet communication, and also by banks and military.
- The RSA cipher uses a public key (i.e., it shared with everyone) and a private key, which gives it added security.
- This scheme relies on mathematics that has been known for hundreds of years. In particular, it uses notions from Number Theory such as prime numbers and modular arithmetic, and some results from the area such as the Fundamental Theory of Arithmetic and Fermat's Little Theorem.

Caesar Ciphers: an example

Suppose **Alice** has a message (call it *plaintext*) which she wants to send to **Bob**. **Eve** is able to listen in on the message, but Alice doesn't want Eve to know what the message means; to do so Alice uses a Caesar cipher:

- Alice and Bob make sure they have agreed in advance on an integer α between 1 and 25. This is called the *key*.
- Encryption: Alice takes each letter of the plaintext, and advances it α letters through the alphabet (if she reaches `Z`, she wraps back around to `A`). She sends the resulting *ciphertext* to Bob.
- Decryption: Bob takes each letter of the ciphertext, and advances it $26 - \alpha$ letters through the alphabet. Since every letter has now been advanced by $\alpha + (26 - \alpha) = 26$ places through the alphabet, each letter is back where it started. So the result is the plaintext again!
- Eve cannot do the same as Bob, because she doesn't know the key α.

Caesar Ciphers: some practice

Activity 1. Encrypt the plaintext `HELLO` with key 6.

Activity 2. Decrypt the ciphertext `KGYE`, which was encrypted with key 6.

Questions. What can Eve do to try to decrypt the message? Why is the Caesar cipher not really very secure?

Answers. Eve can decrypt the massage using a *brute force attack*, this is, trying all possible advances of the letters of the alphabet. First she tries to advance the letters by 1, then by 2, then by 3, and so on; since the alphabet is finite, at some point Eve will advance the letters exactly as many places as Bob needed to advance them to decrypt the ciphertext. For this reason, Caesar ciphers are not very secure, since messages can always be decrypted in a reasonable amount of time.

Some Number Theory: prime numbers and remainders

Number Theory is a branch of Pure Mathematics that concerns the study of integers. We will now present and work with some basic number-theoretic notions that will enable us to construct a ciphering scheme more involved (and more secure!) than Caesar ciphers.

Amongst all integers, there are some which are of particular importance in Number Theory and all Mathematics:

Definition

A positive integer $p \geq 2$ is *prime* if it is only divisible by itself and 1.

Theorem (The Fundamental Theorem of Arithmetic)

Every positive integer can be written uniquely (up to ordering of the factors) as a product of prime numbers.

Some Number Theory: prime numbers and remainders

For example, $45 = 3 \times 3 \times 5 = 3 \times 5 \times 3 = 5 \times 3 \times 3$, and there are no other ways to write 45 as a product of primes.

Activity. Write 50 and 31 as products of primes.

Notation

We write $a \bmod b$ for the remainder of a on division by b.

For example, $7 \bmod 4 = 3$ and $100 \bmod 10 = 0$.

Question. What are the possible remainders on division by 4? What about the possible remainders on division by n, for some positive integer n?
Answer. Remainders on division by 4 are $0, 1, 2, 3$. Remainders on division by n are $0, 1, 2, \ldots, n-1$.

Some Number Theory: modular arithmetic

Throughout, fix a positive integer n; we will call this integer the *modulus*. Modular arithmetic is about doing arithmetic using the n numbers

$$0, 1, 2, \ldots, n-1.$$

The problem we encounter is that if we add or multiply two of these numbers we might get one which is too big to be on this list. However, we've seen that the numbers above are exactly the remainders on division by n, so what we do is to do the usual arithmetic operations with numbers and then take the answer mod n (in other words, the remainder on division by n).

Some Number Theory: addition in modular arithmetic

Addition. To add a and b modulo n we just work out $a + b \bmod n$; this is, we add a and b and then take the remainder on division by n.

For example,

$$2 + 1 \bmod 4 = 3 \bmod 4 = 3,$$

and

$$3 + 2 \bmod 4 = 5 \bmod 4 = 1.$$

Activity. Calculate $2 + 3 \bmod 5$ and $8 + 9 \bmod 12$.

Question. Can you think of any situation where you have used modular arithmetic? (Hint: you know such situations for modulus 12 and 26.)
Answer. In telling the time in a 12-hour clock we use modular arithmetic with modulus 12. In encrypting and decrypting messages using a Caesar cipher we use modular arithmetic with modulus 26.

Some Number Theory: multiplication and powers in modular arithmetic

Multiplication and Powers. In a similar way, to multiply a and b modulo n we multiply a and b and then take the remainder on division by n; to compute a^b modulo n we compute a^b and then take the remainder on division by n.

For example,

$$5 \times 3 \bmod 6 = 15 \bmod 6 = 3,$$

and

$$5^2 \bmod 6 = 25 \bmod 6 = 1.$$

Some Number Theory: a useful fact

So far, to do modular arithmetic we were doing the standard arithmetic operations and then taking remainders. The following fact tells us that we can take remainders at any step of the computation that we want.

Useful Fact

For every integer a and b we have

$$\begin{aligned} a + b \bmod n &= (a \bmod n) + (b \bmod n) \bmod n \\ a \times b \bmod n &= (a \bmod n) \times (b \bmod n) \bmod n \\ a^b \bmod n &= (a \bmod n)^b \bmod n \end{aligned}$$

Some Number Theory: an example of the useful fact

For example,

$$[(3+4)\times 5]^2 \bmod 6 = (7\times 5)^2 \bmod 6 = (35)^2 \bmod 6 = 1225 \bmod 6 = 1.$$

Alternatively, we can take the remainder after every part of the computation:

$$[(3+4)\times 5]^2 \bmod 6 = (1\times 5)^2 \bmod 6 = 5^2 \bmod 6 = 25 \bmod 6 = 1,$$

or just take remainders whenever it suits us:

$$[(3+4)\times 5]^2 \bmod 6 = (35)^2 \bmod 6 = 5^2 \bmod 6 = 25 \bmod 6 = 1.$$

Activity. Use the useful fact to work out $((5+4)\times 5\times 8)^6 \bmod 10$.

Key Exchange: the Diffie-Hellman protocol

Recall that with the Caesar cipher Alice and Bob needed to have agreed their key in advance. But what if they have had not opportunity to do so? Can they establish a common key entirely in public, with Eve listening in, but still not knowing what the key is?

The Diffie-Hellman protocol allows Alice and Bob to carry this out; this system was announced by Diffie and Hellman in 1976, but the GCHQ had already discovered it in 1974 and kept it secret!

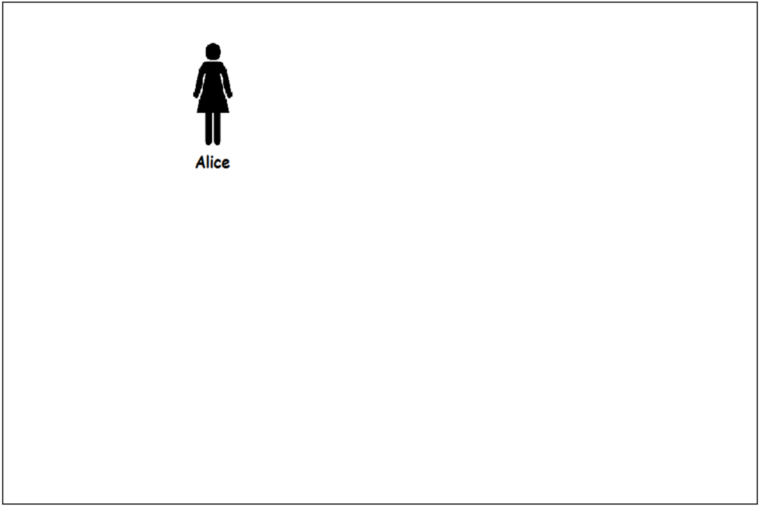
We are now equipped with the mathematical notions needed to understand the workings of this scheme, so let us do so in several steps.

Key Exchange: the Diffie-Hellman protocol

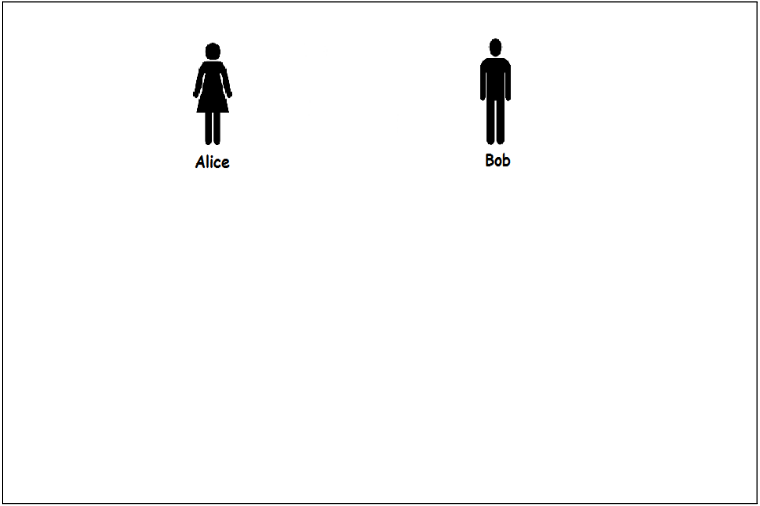
- Alice chooses a prime p, a smaller number g, and sends them (unencrypted) to Bob.
- She also chooses a secret number a. She keeps a secret but works out $g^a \bmod p$ (call this number A), and sends it to Bob.
- Bob chooses a secret number b. He keeps it secret but works out $g^b \bmod p$ (call this number B), and sends it to Alice.
- Alice knows a, B and p. She works out $B^a \bmod p$ and uses it as a key.
- Bob knows b, A and p. He works out $A^b \bmod p$ and uses it as a key.

We claim that the two keys obtained by Alice and Bob are in fact equal. Before we see this, let us review the system with the aid of a diagram.

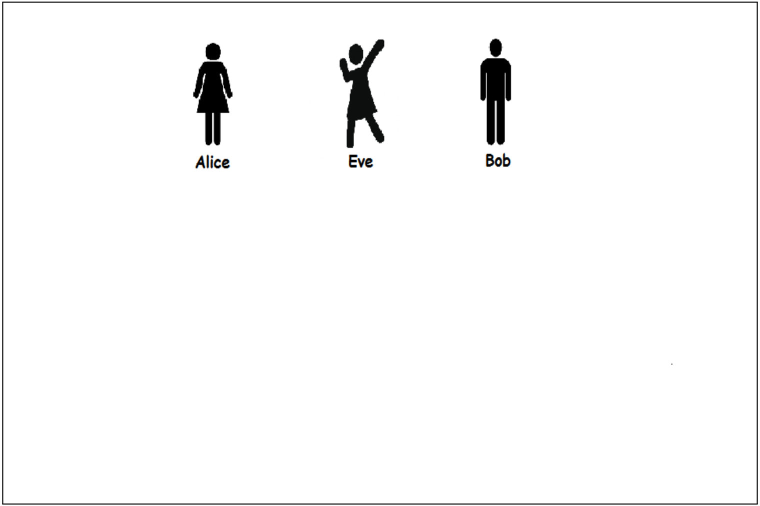
Key Exchange: the Diffie-Hellman protocol



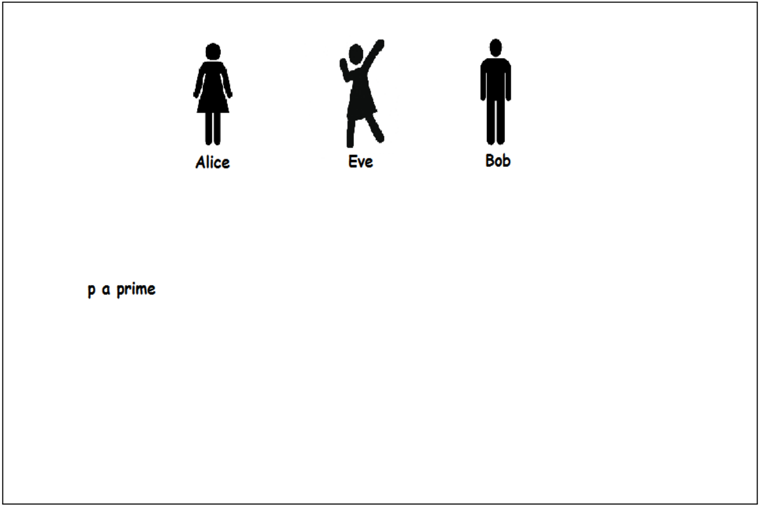
Key Exchange: the Diffie-Hellman protocol



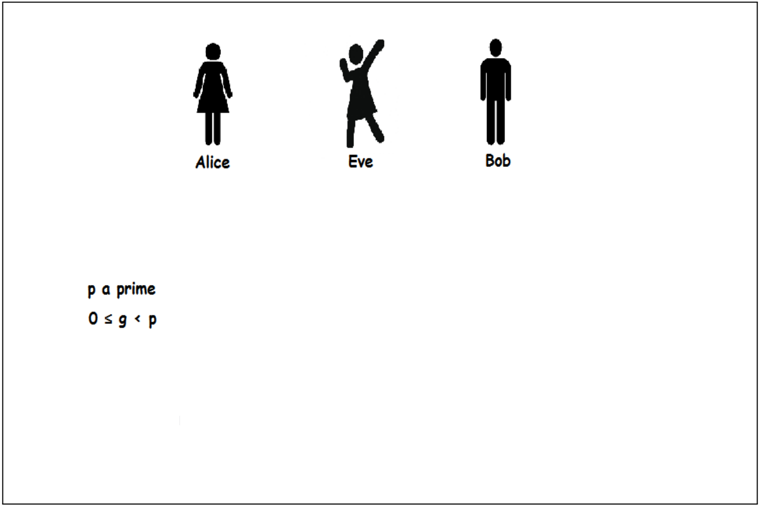
Key Exchange: the Diffie-Hellman protocol



Key Exchange: the Diffie-Hellman protocol



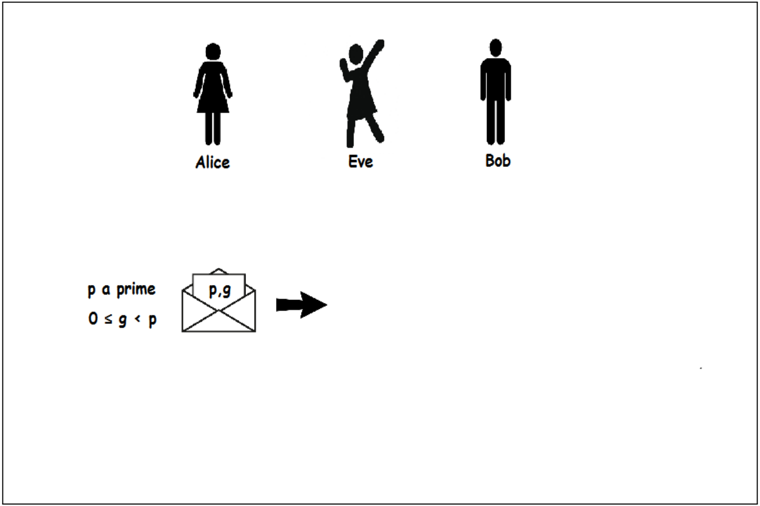
Key Exchange: the Diffie-Hellman protocol



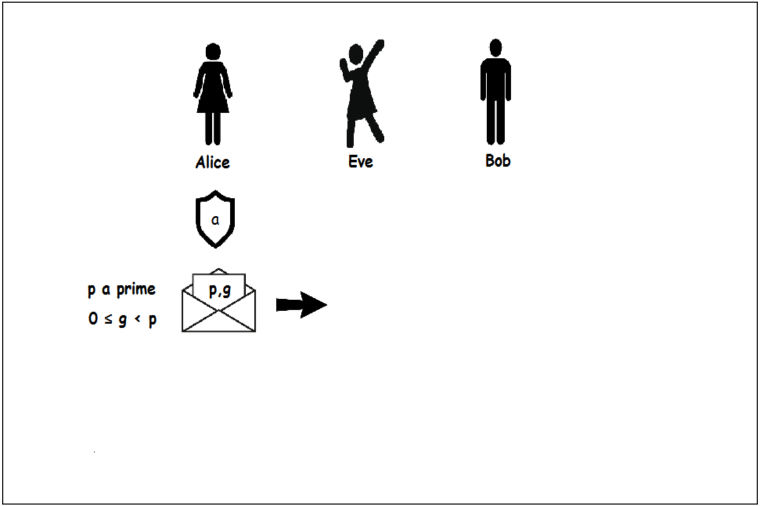
p a prime

$0 \leq g < p$

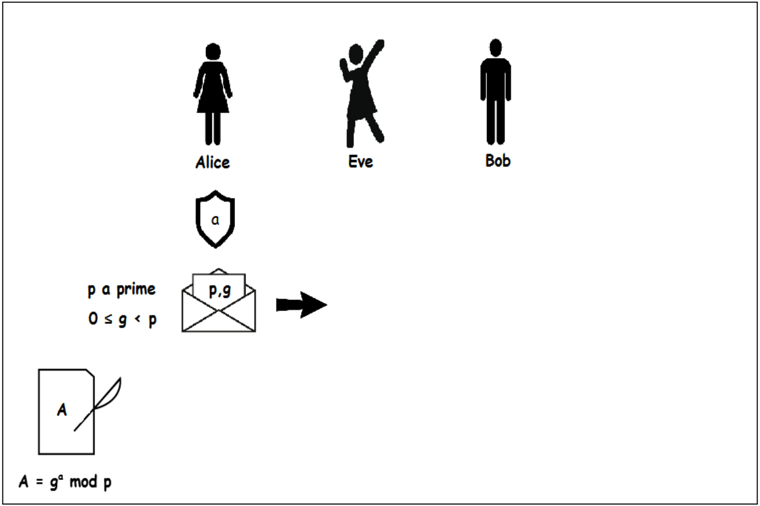
Key Exchange: the Diffie-Hellman protocol



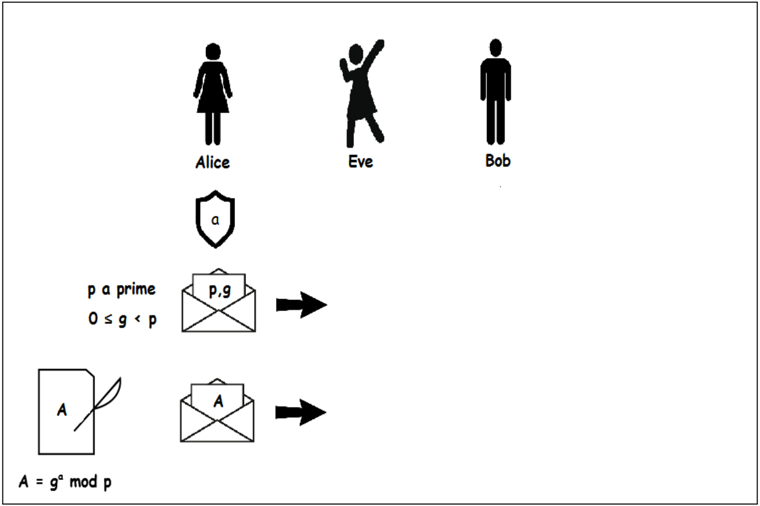
Key Exchange: the Diffie-Hellman protocol



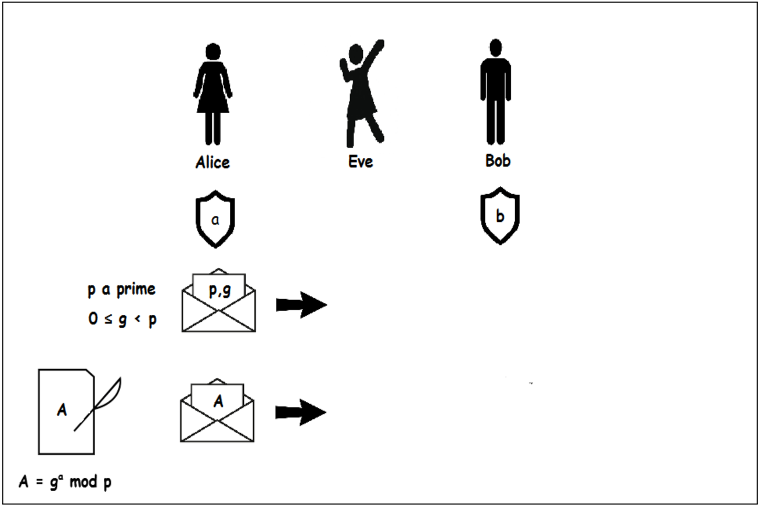
Key Exchange: the Diffie-Hellman protocol



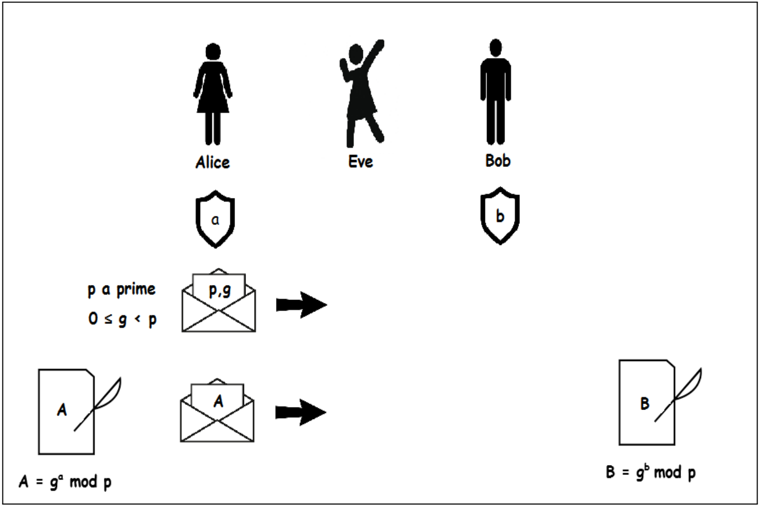
Key Exchange: the Diffie-Hellman protocol



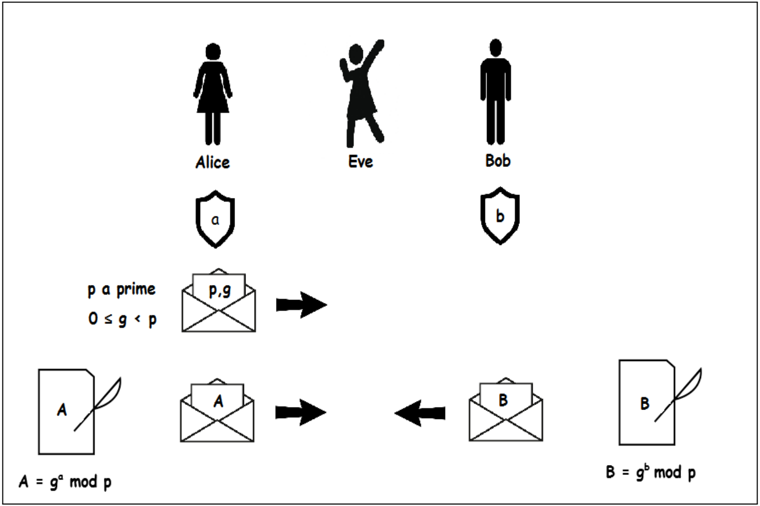
Key Exchange: the Diffie-Hellman protocol



Key Exchange: the Diffie-Hellman protocol



Key Exchange: the Diffie-Hellman protocol



Key Exchange: the Diffie-Hellman protocol

So Alice has key $B^a \bmod p$ and Bob has key $A^b \bmod p$; but now, modular arithmetic (and using the useful fact, marked with $*$) gives that:

$$\begin{aligned} B^a \bmod p = (g^b \bmod p)^a \bmod p &\overset{*}{=} (g^b)^a \bmod p \\ &= g^{ba} \bmod p \\ &= g^{ab} \bmod p \\ &= (g^a)^b \bmod p \\ &\overset{*}{=} (g^a \bmod p)^b \bmod p \\ &= A^b \bmod p. \end{aligned}$$

So their keys are the same! Now they can turn their key into a form suitable for the cipher system they want to use. For example, they could take the key modulo 26 and use it as a key for the Caesar cipher.

Key Exchange: the Diffie-Hellman protocol

Activity. Suppose Alice chooses $p = 13$, $g = 6$, $a = 5$, and Bob chooses $b = 7$. Work out A and B. Now work out the keys $A^b \bmod p$ and $B^a \bmod p$ and check that they coincide.

The End

Thank you for your attention.