Two studies in explanation – Annotated

Below are transcripts of two explanations of the same difficult concept. How are they different? Mark areas where the author provides **motivation**, **bridging** from familiar to unfamiliar, and **signposting** of structure. Links to the videos are below.

"Imagine two people who have never met who can do an amazing trick. Alice and Bob are allowed to communicate over a line which is tapped, so any message they pass will be intercepted by Eve, who is always listening. The trick is to agree on a secret numerical key, without Eve also obtaining a copy. How is this possible?

First, let's explore how this trick is done using colors. How could Alice and Bob agree on a secret color without Eve finding it out? The trick is based on two facts:

1. It's easy to mix two colors together to make a third color. And 2. given a mixed color, it's hard to reverse it in order to find the exact original colors.

This is the basis for a lock: easy in one direction, hard in the reverse direction. This is known as a *one way function*.

Now the solution works as follows:

First, they publicly agree on a starting color, say yellow.

Next, Alice and Bob both randomly select private colors and mix them into the public yellow in order to disguise their private colors.

Now, Alice keeps her private color and sends her *mixture* to Bob.

And Bob keeps his private color and sends his *mixture* to Alice.

Now the heart of the trick: Alice and Bob add their private colors to the other persons mixture and arrive at a shared secret color. Notice how Eve is unable to determine this color since she needs one of the private colors to do so. And that is the trick.

Motivate why things are happening

Bridge from familiar to unfamiliar

Signpost your structure

Transition to metaphor. Restate the problem in metaphorical terms.

What they do + ***why*** they do it.

11 Now to do this with numbers, we need a numerical procedure which is easy in one direction and hard in the reverse direction. This brings us to *modular arithmetic*, which is known as clock arithmetic.

Transition back from the metaphor domain; parallel restatement of the problem.

For example, to find 46 mod 12, we take a rope of length 46 units and wrap it around the clock of 12 units – which is called the *modulus* – and wherever the rope ends is the solution. So we say 46 mod 12 is congruent to 10. Easy!

"Easy" and "hard" are not normally structural flags. Their emphasis prepares the listener to map the insight from the metaphor domain onto processes in the numerical domain.

Now to make this work we need a prime modulus such as 17 instead of 12. Then we find the primitive root of 17, which is a number that has no factors in common – in this case 3. And it has this important property that when raised to different exponents, the solution distributes uniformly around the clock. 3 is known as the *generator*. So if we raise 3 to any exponent x, the solution is equally likely to be any integer between 0 and 17. Now the reverse procedure is hard. Say, given 12, find the exponent 3 needs to be raised to. This is called *the discrete logarithm problem*.

These exact words return to make sure the listener mapped correctly.

And now we have our one-way function. Easy to perform, but hard to reverse. Given 12, you would have to resort to trial and error in order to find the matching exponent.

15 How hard is this? Well with small numbers, it's easy. But if we use a prime modulus which is 100s of digits long, it starts to get seriously hard. Even if you had access to all of the computational power on Earth, it could take thousands of years or more to find the answer. So the strength of the one-way function is based on the time needed to reverse it.

Complications and complexity are added only afterwards, once the core intuition has been established; not as a disclaimer.

Now this is our solution: First Alice and Bob publicly agree on a prime modulus and a generator. For example, 17 and 3. Then Alice selects a private random number, say 54, and calculates 3^{54} mod 17, and sends this result publicly to Bob. Then Bob selects his private random number, say 24, and calculates 3^{24} mod 17 and sends this result publicly to Alice. And now the heart of the trick: Alice takes Bob's public result and raises it to the power of her private number, which gives 3^{24*54}, and she obtains the shared secret, which in this case, is 1. Bob takes Alice's public result and raises it to the power of his private number, which gives 3^{54*24}, resulting in the same shared secret. Notice they did the same calculation with the exponents in a different order: 24*54 = 54*24. Without one of the private numbers, Eve will not be able to find the solution. And this is how it's done."

Diffie-Hellman Key Exchange
by Art of the Problem

Diffie-Hellman Key Exchange
by ZemediaTube

"Encryption requires two parties to share a secret random number known as a key. But how can two people who've never met agree on this number without letting anyone else know?

In the mid 1970's, 3 research scientists, Whitfield Diffie, Martin Hellman, and Ralph Merkle devised a brilliant method to do this using a numerical procedure. So how is it done?

For this example, we'll use prime numbers with values under 30.

This disclaimer is not for the audience's benefit.

First, Ada and Bill agree on two numbers in public. In this case 11 and 29. Which anyone can listen in on. Then Ada selects a private random number, say 3, and Bill selects his private number, say 5. Ada then uses modular arithmetic to calculate 11^3 mod 29.

These are structural signposting words, in a way, but they do not reduce complexity. The structure is "a series of events happen."

Modular arithmetic finds the remainder of the number to the left of the word mod when divided by the number to the right of it. So, 10 mod 3 is 1, as 10 divided by 3 leaves a remainder of 1.

Now 11 to the power of 3 is 1331. To calculate the remainder, divide this by 29 and disregard the decimal place to get 45, then multiply this whole number by 29 – giving 1305 – and subtract this result from your first value. This gives Ada 26.

What follows is a stepwise description of ***what*** they do in chronological order, with no mention at all of ***why*** they're doing it.

We've motivated the big picture, but failed to show how these steps contribute to solving it.

While Ada's doing this, Bill calculates 11^5 mod 29. 11 to the power of 5 is 161051. Bill calculates the remainder by finding the whole number through dividing this by 29. He then multiplies this whole number – 5553 by 29 – to get 161037, and subtracts this from his first value, to get 14.

We spend nearly 2 full minutes on arithmetic to find remainders. Is the ***goal*** of this video to show the mechanics of calculating remainders or to explain Diffie-Hellman key exchange?

Then Ada and Bill publicly exchange their numbers. Now, this is where the important stuff happens. Ada takes Bill's public result and raises it to the power of her private number to obtain their shared secret number, which in this case, is 18. Then Bill takes Ada's public result and raises it to the power of his private number, which results in the same shared secret.

So they both used the algorithm to calculate the same shared private number. Without one of these private numbers, 3 or 5, someone listening in will have great difficulty finding the solution."

Note there was never any explanation of ***why*** someone listening in won't be able to figure out the solution. This is simply asserted at the end.