

Diffie Helman, Successive Square, Modulo Arithmetic

Explained

eCommerce couldn't exist without the ability for two computers to share secret information. When eCommerce first began, there was a pervasive concern that credit cards would be compromised, that buying online wouldn't be "safe."

The secret to keeping things secret is encryption. And the secret to encryption is having a shared secret, something that only the sender and receiver know. It's the "key." In the world of espionage spies could meet at the secret meeting place and exchange a code book, but that's hard to do when it's you and Amazon. No place to meet.

Enter the Diffie-Helman Key Exchange Protocol. This piece of math magic lets two people communicate in the clear (or, in plain English – two computers send messages that are available to everyone), and at the end of the exchange, the two computers know a secret key that others can't figure out.

There are three parts to this bit of magic: modular arithmetic, raising numbers to a power with successive squaring, and last, but not least, the Diffie-Helman exchange.

Part 1: Modular Arithmetic.

It's not as complicated as it seems. In modular arithmetic, numbers are never bigger than the "modulus." For example, for "mod 12" numbers are never bigger than 11. You can think of a clock. There's no 13 or 14.

The easiest way to convert numbers in modular arithmetic is by dividing and taking the remainder. For those of you who are calculator slaves you may have forgotten what remainders are. It's the integers left over after you divide. Take $17 / 3$. That's 5 with a remainder of 2 (because 3 goes into 17 5 times – $3 * 5 = 15$ – and there are 2 left over). On a calculator you get 5.666666. The remainder is NOT .66666.

One more example. $435 \text{ mod } 17$ is 10 because $435 / 17 = 25$ with 10 left over.

A word about notation. When we say "mod 17" that means that the whole expression is modular, not just the last number.

There's one more critical piece to modular arithmetic. You can do the reduction at whenever the numbers are bigger than the modulus. Again, this concept is simpler than it sounds.

We'll do some examples.

$$12 * 29 * 408 \text{ mod } 13$$

Remember that the phrase "mod 13" applies to the whole expression. We can reduce the parts before we do the multiplication. This is VERY important as we shall soon see.

$$12 \text{ mod } 13 = 12$$

$$29 \bmod 13 = 3$$

$$408 \bmod 13 = 5$$

Now do the multiplication. $12 * 3 = 36$, but “mod 13” it is 10

Then $10 * 5 = 50$, but “mod 13” that’s 11 – which is our answer.

Just for fun, we can do the mod reduction at some other point.

$$12 * 29 = 348 \quad 348 * 408 = 141,984$$

$$141,984 \bmod 13 = 11$$

See – same result. That’s not a proof at all, but it serves to demonstrate the point.

The beauty of modular arithmetic is that the numbers stay manageable.

Part 2: Successive Squaring

Let’s say I want to calculate 3^9 (3 raised to the 9th power). That’s $3 * 3 * 3 * 3 * 3 * 3 * 3 * 3 * 3$.

It’s the same as $3^7 * 3$, which is the same as $3^4 * 3^4 * 3$, or even $3^2 * 3^2 * 3^2 * 3^2 * 3$. Remember, we add exponents when we multiply. Either one of these has 9 3’s multiplied together.

That’s all there is to successive squares.

Let’s do the example:

$$3^1 = 3$$

$$3^2 = 9$$

$$3^4 = 81$$

$$3^8 = 6561$$

$$3^9 = 3^8 * 3 = 6561 * 3 = 19,683$$

We only had to do 4 multiplications, not 9.

Consider what happens if the exponents get bigger. What if we wanted to do, say, 3^{4098} ?

For starters, the numbers are enormous. 3^{32} is 1,853,020,188,851,840. And we’d need to do 5831 multiplications. With successive squaring though, twelve multiplications get us to 3^{4096} , then one more and we’re there ($3^{4096} * 3^2$).

It’s time to combine Part 1 and Part 2. The problem with raising things to big powers is that the numbers get huge fast. Remember the tale of the beggar who asked the king to put one grain of sand on the first square of the chessboard, two on the next, four on the third. The universe doesn’t have 2^{64} grains of sand.

Let’s do 3^{4098} say, mod 11. Now the number won’t ever get big.

$$3^1 = 3 \quad \bmod 11 = 3$$

$$3^2 = 9 \quad \bmod 11 = 9$$

$$3^4 = 81 \pmod{11} = 4$$

OK. Stop right here. I'm not going to do $81 * 81$. We already know that $81 \pmod{11} = 4$.

$$\text{SO } 3^8 = 4 * 4 = 16 \pmod{11} = 5$$

$$3^{16} = 5 * 5 = 25 \pmod{11} = 3$$

3^{32} you've got the picture

$$3^{4096} \pmod{11} = 3$$

$3^{4098} = 3 * 9 = 27 \pmod{11} = 5!$ And we only had to do 13 multiplications.

Part 3: Diffie Helman

This really does seem like magic. Two people talk, everyone listens, and in the end, they share a secret number.

Here's how it works. We start with a number, "g" that everyone in the whole world knows.

Next, you and I each pick a secret number. Call mine "a" and yours "b."

I'll calculate g^a and tell you. Let's call that "A." You calculate g^b and tell me. We'll call that "B."

Finally, I'll calculate B^a and you calculate A^b . Presto - we have a secret number because:

$$A = g^a \text{ so } A^b = (g^a)^b = g^{(a*b)}.$$

And

$$B = g^b \text{ so } B^a = (g^b)^a = g^{(b*a)}$$

What makes it really secret is that we do all of this calculation using modular arithmetic. If we all know what g is, and I tell you what A is, you can't possibly figure out a. Trust me on that one.

That's all there is to it.