Diffie-Hellman Key Exchange

Wednesday, October 28, 2020 11:32 AM

Two ways to tell the story:
a) real chronological order
b) the order in which it was reported…

We will do (a)

The year is 1972…
British Intelligence Agency is working on a problem…

The norm, ie the paradigm for encryption was what we today call "Private Key Cryptography"

In order for you and I to communicate, we must **first exchange a secret key that no one else knows. So we must meet securely to do this.**

In every single cipher we've looked at…knowledge of the encryption key gives away the decryption key…

a) Can we exchange a secret key without ever meeting, so everyone hears our conversation, but at the end of it, you and I have a secret key that no one else who listened has.
b) Can we do this with arbitrary message, where I post a public key, you use that to encrypt a message to send to me, and then I am the only one who can decrypt it…even though others know the public key, that does not compromise the value of the private key used to decrypt.

In 1972…the British Intelligence Agency hires Clifford Cocks, a young mathematician. In high school, he represented Great Britain in the International Math Olympiad (IMO).

The group that he joined posed these problems to him and he thought they were interesting…they told him, "hey we've been working on these for a while and haven't gotten anywhere."

In less than 3 weeks, he came up with an idea to solve (b). He approached his colleagues, showed them on paper what he did, and they

were stunned…they couldn't figure out how to break it and they eventually agreed that he solved the problem….But…because he was doing this for intelligence, he couldn't tell anyone he solved this problem…In fact, as it turns out what he invented is currently called RSA encryption named after 3 people who "invented" it five years later.

But, Clifford wasn't done…

In another couple weeks, he told colleagues that he had figured out how to do (a) as well…and again, he was right, he really did solve the problem…and this time, the thing he invented is currently called, "The Diffie-Hellman Key Exchange"

In fact, Clifford wasn't allowed to talk about his discoveries until 1997, and which point the RSA company had already been sold for many millions of dollars!

Go ahead to 1976…
In public domain, some researchers were wondering whether problem (a) was possible to solve?

Most researchers thought this was impossible!!!

But a few, thought there might a way, and if so, it would rely on what we call a "trap door function" or "one way function"

A function easy to calculate forwards, but hard to calculate backwards…

(a) Multiplication vs Factoring 5 x 7 = 35, a x b = 35, what are a a and b?

(b) Modular Expo vs. Discrete Log Problem: Given an base a, exponent b and a mod value p, calculate a^b mod p…(easy)…to do backwards, I give you the answer, I give you a and I give you p, you figure out b.

Diffie gave a talk somewhere about his ideas and wanted someone to work with and Hellman thought his ideas had merit and so they started working together…It took them about a year…but, utilizing the difficulty of the discrete log problem (kind of), they were able to find a

way to exchange a secret key with only public communication.
=

Diffie-Hellman Key Exchange

We pick a large prime number p, and this will be a public value. We pick a generator/primitive root for the prime, a, and this will also be a public value.

Alice	Bob
1. Picks a random private key, k_A. ($1 < k_A < p$)	1. Bob picks a random private key, k_B. ($1 < k_B < p$)
2. Calculates $C1 = a^{kA} \bmod p$	2. Calculates $C2 = a^{kB} \bmod p$
3. Alice sends Bob C1	3. Bob sends Alice C2

Note: EVERYONE SEES C1, C2 and knows p and a. They don't know k_A or k_B. Due to the discrete log problem, these are not easy to figure out given only C1 and C2.

4. Alice calculates $C2^{kA} \bmod p$	4. Bob calculates $C1^{kB} \bmod p$

The value in step 4 that both calculate is the same and is their shared key.

$C1^{kB} = (a^{kA})^{kB} = a^{kA*kB} \bmod p$

$C2^{kA} = (a^{kB})^{kA} = a^{kB*kA} = a^{kA*kB} \bmod p$

Thus, the two values are equal.

We can't use C1 and C2 to calculate the secret key…

Try it…

$C1 \times C2 = a^{kA} * a^{kB} = a^{kA + kB}$, not what we want…

$C1^{C2} = a^{(kA)(a\text{^}kB)}$ so exponent is "way bigger"

Anyway, we get stuck…

Let's try with small numbers:

p = 13, try a = 2

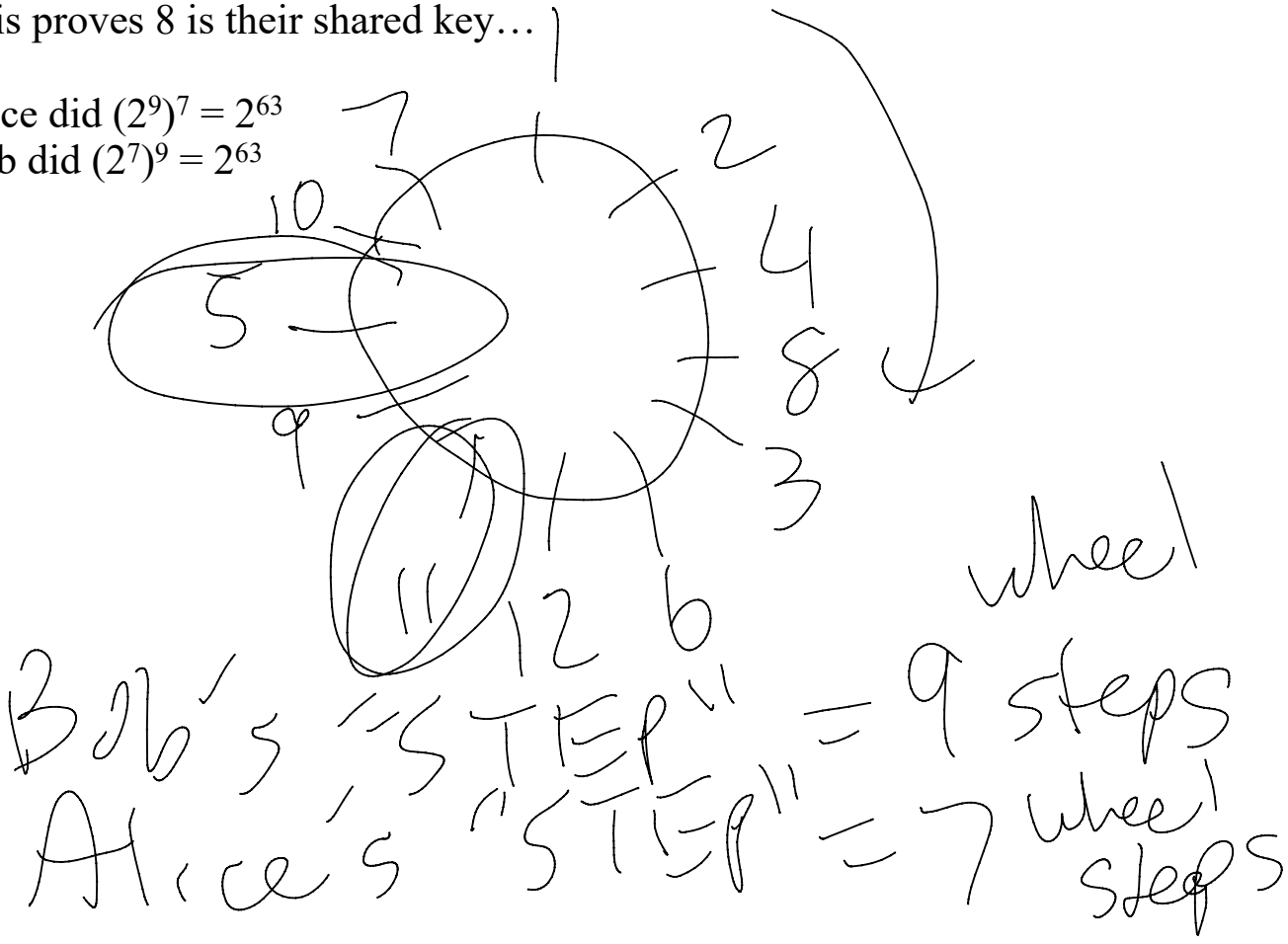
Alice generates kA = 7, Alice sends bob $2^7 = 128 = 11 \pmod{13}$
Bob generates kA = 9, Bob sends Alice $2^9 = 512 = 5 \pmod{13}$

Now, Alice receives 5, then calculates $5^7 \bmod 13 = 125 \times 125 \times 5 = (-5)$
$(-5)(5) = 125 = 8 \pmod{13}$

Bob receives 11, then calculates $11^9 = (-2)^9 = -512 = 8 \pmod{13}$

This proves 8 is their shared key…

Alice did $(2^9)^7 = 2^{63}$
Bob did $(2^7)^9 = 2^{63}$



When Alice gets her final answer, what she is doing is taking 7 Bob SIZED steps around this wheel.

When Bob gets his final answer, what he is doing is taking 9 Alice SIZED steps around this wheel.

So, when both are done, they have spun around the wheel the exact same amount and will end up at the same place.

H1 is worth 1% and was 25 pts
H2 is worth 4% and was 100 pts
H3 is worth 4% and was 100 pts
H4 is worth 4% and was 100 pts
Q1A+Q1B is worth 10% and was 50 pts
Q2A+Q2B is worth 10% and was 50 pts
Q3A+Q3B is worth 10% and was 50 pts
Q4A+Q4B is worth 10% and was 50 pts

(H1+H2+H3+H4)/25

max of sum H1 to H4 is 325, when we divide by 25 we get 13 as the max since this is supposed to be 13% of the grade…so the most you can earn from these is 13, which is why we divide by 25, since 25 points = 1% of the course grade for all homeworks

If 50 quiz pts = 10% course grade, 5 quiz pts = 1% of the course grade, so divide the sum of the quiz pts by 5 to get their contribution.

(Q1+Q2+Q3+Q4)/5

in total, all of this represents 13+40 = 53 53% of the course grade. To scale this out of 100, we divide this sum by .53

So the final formula is

((H1+H2+H3+H4)/25 + (Q1+Q2+Q3+Q4)/5)/.53

HERE IS WHAT WEBCOURSES DOES DIFFERENTLY!!!

IT ASSUMES THAT THERE ARE AN UNKNOWN NUMBER OF FUTURE ASSIGNMENTS AND IT ASSUMES THAT YOU WILL CONTINUE, IN EACH GRADE CATEGORY, TO GET THE SAME PERCENTAGE IN THE FUTURE…WEBCOURSES DOESN'T KNOW THAT MOST OF THE QUIZZES ARE DONE BUT THERE IS MORE REMAINING HOMEWORK,

RELATIVELY SPEAKING…

Homework in the course is worth 25%
Quizzes are worth 50%

[(4*(H1+H2+H3+H4)/13)*.25 + (Q1+Q2+Q3+Q4)/2)*.50]/ .75

At the end of the day, your Real grade is of the form

c1*(H1+H2+H3+H4) + c2*(Q1+Q2+Q3+Q4)

Webcourses calculates your grade as

d1*(H1+H2+H3+H4) + d2*(Q1+Q2+Q3+Q4)

Due to the dynamics of the calculation, if c1 > d1 then c2 < d2
if c1 < d1 then c2 > d2

So it's a difference of how much the two categories are weighted, because I **KNOW** how mcuh of each category is finished, and Webcourses assumes that the same percentage of each category is finished so far…

At the end of the course, is the only time c1 = d1 and c2 = d2, so at the very end, once the very last grades are entered, they both converge to your correct class grade.

This is true in ALL of your classes…so you should be in the habit of calculating your own grades
The only issue would be if a teacher implements incorrectly in Webcourses what their syllabus says, which I have seen happen…