Jacob Martens
Jeff Ondich
Computer Security
13 April 2021

Diffie Hellman

Alice and Bob's shared secret is 12. The steps below show how I reached this conclusion:

1. I intercept that g=17, p=61, A=46, and B=5.
2. Now let A=46=g^Xmod p=17^Xmod 61. It follows that X=14.
3. Similarly, let B=5=g^Ymod p=17^Ymod 61. It follows that Y=26.
4. Now Alice computes that B^Xmod p=5^{14}mod 61=12.
5. Finally Bob computes that A^Ymod p=46^{26}mod 61=12, as expected.

For finding the values of X and Y, I guessed and checked until I found values that worked using an online power modulo calculator, which is linked at the end. For integers much larger, this process is too inefficient for an interloper to learn the secret. Thus, the failure would occur at steps 2 and 3.

RSA

The unencrypted message is below, as well as its translation into letters from the ASCII values I found.

068 101 097 114 032 066 111 098 044 032 067 104 101 099 107 032 116 104 105 115 032 111 117 116 046 032 032 104 116 116 112 115 058 047 047 119 119 119 046 115 099 104 110 101 105 101 114 046 099 111 109 047 098 108 111 103 047 097 114 099 104 105 118 101 115 047 050 048 049 055 047 049 050 047 101 045 109 097 105 108 095 116 114 097 099 107 105 110 103 095 049 046 104 116 109 108 032 089 105 107 101 115 033 032 089 111 117 114 032 102 114 105 101 110 100 044 032 065 108 105 099 101

Dear Bob, Check this out. https://www.schneier.com/blog/archives/2017/12/e-mail_tracking_1.html Yikes! Your friend, Alice

The process is as follows:

1. I know Bob's public key: (31, 4661).
2. Using an online calculator linked below, I found that the prime factors of 4661 are 59 and 79.

3. Now I find a value d such that $e \times d = 31 \times d \equiv 1\, mod\, 58 \times 78 = 4524$. Using an online calculator linked below, I found that $d = 2335$.
4. Now we raise each integer in the encrypted data to the power of d modulo 4661.
5. I then passed the decrypted numbers through an online ASCII translator to uncover the final message. This translator is linked below.

Similar to the Diffie-Hellman process above, this method is inefficient if the second value in the public key is very large. This is because there is no efficient way for finding the prime factors of this number n besides checking the combinations of every prime number less than n. While I was able to use an online calculator in step 2, it would hypothetically take many thousands of years to do the same for a number on the scale of 600 digits unless I made a really lucky guess.

Online Resources

This is the tool for finding powers modulo a number referenced in the Diffie-Hellman section:
https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html

This is the tool I used for prime factorization, referenced in RSA, step 2:
https://www.calculatorsoup.com/calculators/math/prime-factors.php

This is the tool I used for finding the multiplicative inverse of e in RSA, step 3:
https://planetcalc.com/3311/

This is the ASCII translation tool I used in RSA, step 5:
http://www.unit-conversion.info/texttools/ascii/