Fall 2020 CIS 3362 Quiz #5 Part A: Diffie-Hellman, RSA Solutions

Date: 11/13/2020

1) (5 pts) Consider the situation where Alice and Bob attempt the Diffie-Hellman Key Exchange, but their modulus value, *p*, is NOT a prime number, and *a* (the base) is not a generator of *p*. If they perform the protocol as otherwise specified, are they guaranteed to calculate a shared key?

Solution

Yes, both will still calculate the same shared key. Both calculate a^{xy} mod p, where x and y are the secret values they choose on their own, and mathematically, no matter what p is, they will calculate the same thing. If p isn't prime and a isn't a generator, there are potentially a lot fewer values that a^{xy} could be equivalent to, mod p, thus, not using a prime number and generator reduces the security of the key exchange protocol.

Grading: 3 pts for clearly stating that both will calculate the same shared key. 2 pts for the reasoning.

2) (8 pts) Bob is using *p* = 23 as his prime number and *a* =5 for the Diffie-Hellman Key Exchange. Talia would like to use a different generator mod 23. Unfortunately, Talia is lazy and wants to do the least amount of arithmetic (multiplication and modding) possible, and she knows an efficient way to calculate a different generator mod 23, given that 5 is a generator mod 23. Determine the generator (**by hand**) that Talia is going to calculate.

Solution

Raising any generator, a, of a prime p, to the power k, where gcd(k, p-1) = 1, will yield another generator, as shown on homework #6. In this case p-1 = 22. The first few values relatively prime to 22 are 1, 3, and 5. Note that 5^1 is 5 and Talia wants ***a different generator***, so if she's lazy, she'll use the generator $5^3 \equiv 125 \equiv$ **10 (mod 23).**

Grading: 4 pts for stating the fact about which powers to raise a generator to, to create another generator, 1 pt for throwing away 1, 2 pts for choosing 3, 1 pt for obtaining the correct answer of 5^3 reduced mod 23.

3) (12 pts) In an RSA system n = 713 and e = 119. What is d? (In order to get credit, please do the following: you may use a calculator to factor any numbers necessary, but you **must show** each step of the Extended Euclidean Algorithm to earn full credit. You may plug into the calculator for the EEA, but you must write down/type out each step as shown in class. If you would like, you can gather terms quickly, to reduce the amount of writing.)

Solution

713 = 23 x 31, which was obtained by trial and error. Since it's an RSA system, I knew that two primes were to be multiplied. Also, to create an ending digit of 3, we can multiply 1 x 3 or 7 x 9. Quickly, we see that 2, 3, 5 and 7 don't work. So since we must have one number ending in 3 or 9, we can just try 13, 19, both which fail, and then get to 23, which succeeds.

$\Phi(713) = (23 - 1)(31 - 1) = 22 \times 30 = 660$

$d = 119^{-1} \bmod 660$

Now, let's do the Extended Euclidean Algorithm:

660 = 5 x 119 + 65
119 = 1 x 65 + 54
65 = 1 x 54 + 11
54 = 4 x 11 + 10
11 = 1 x 10 + 1

11 - 1 x 10 = 1
11 - (54 - 4 x 11) = 1
5 x 11 - 1 x 54 = 1
5(65 - 54) - 1 x 54 = 1
5 x 65 - 6 x 54 = 1
5 x 65 - 6(119 - 65) = 1
11 x 65 - 6 x119 = 1
11(660 - 5 x 119) - 6 x 119 = 1
11 x 660 - 61 x 119 = 1

Take this equation mod 660 to yield

$-61 \times 119 \equiv 1 \pmod{660}$

Thus, $119^{-1} \equiv -61 = 599 \pmod{660}$.

Thus, **d = 599.**

Grading: 2 pts factorization 713 (no work needed), 1 pt phi(n), 3 pts Euclidean, 5 pts Extended Euclidean, 1 pt extracting the positive answer