MATH 314 Spring 2019 - Class Notes

2/21/2019

Scribe: Matthew Oberteuffer

Summary: In this class, we discussed solving an equation involving exponents by making use of the Basic Principle, and how the Basic Principle could be applied to cryptography in the form of the 3-pass protocol.

Basic Principle:

- Say we want to solve an equation like: $x^3 = 7 \pmod{11}$.
- To solve, we would need to take the cube root of both sides of the equation. In modular arithmetic, the equivalent would be raising both sides by the modular inverse of 3.
- Basic Principle is that all that matters in the exponent is what happens $\pmod{p-1}$.
- So, to find the modular inverse of 3, both sides of the equation would be raised to some power b such that $x^{3^b} = 7^b \pmod{11}$ and $3b = 1 \pmod{10}$.
- In other words, to undo raising a number to a power $\pmod{p}$, raise the equation to the inverse of that power $\pmod{p-1}$

Example: Solution for $x^3 = 7 \pmod{11}$

1. Raise both sides to some power b: $x^{3^b} = 7^b \pmod{11}$
2. Apply Basic Principle to solve for exponent's inverse: $3b = 1 \pmod{10}$
3. Apply Extended Euclid's algorithm:

   GCD(10, 3)
   $10 = 3(3) + 1$
   $1 = 10 - 3(3)$
   So, $3^{-1} \pmod{10} = -3 \pmod{10}$, resolving to $3^{-1} \pmod{10} = 7 \pmod{10}$

4. $b = 7$, so $x^{3^7} = 7^7 \pmod{11}$ is equivalent to $x = 7^7 \pmod{11}$ which gives $x = 6 \pmod{11}$

Three-Time Pass

- Real world version of three-time pass:

- Alice wants to send a box to Bob securely through the mail, but Bob does not share a key with Alice. To circumvent this, Alice locks the box with her padlock, and sends it to Bob. Bob receives the box, locks the box with his own padlock, and sends it back to Alice. Alice removes her lock and sends it to Bob. Bob completes the process by removing his own lock.

- Math version:

1. Alice has a message m, where m is some number. A large prime number $p > m$ is picked. p is not a secret.

2. Alice picks a secret number $a < p - 1$ such that GCD(a, p-1) $= 1$

3. Bob picks a secret number $b < p - 1$ such that GCD(b, p-1) $= 1$ (Both a and b must be coprime to p.)

4. The encryption functions would then be given by:
   $E_A(x) = x^a \pmod{p}$
   $E_B(x) = x^b \pmod{p}$

5. Alice computes $a' = a^{-1} \pmod{p-1}$
   Bob computes $b' = b^{-1} \pmod{p-1}$
   The decryption functions would be given by:
   $D_A(y) = y^{a'} \pmod{p}$
   $D_B(y) = y^{b'} \pmod{p}$

6. Alice encrypts m such that $C_1 = E_A(m) = m^a \pmod{p}$, and sends it to Bob.

7. Bob computes $C_2 = E_B(C_1) = C_1^b \pmod{p}$, and sends this to Alice.

8. Alice computes $C_3 = D_A(C_2) = C_1^{a'} \pmod{p}$, sends this to Bob.

9. Bob computes $C_3^{b'} = (C_2^{a'})^b = (((C_1^b)^{a'})^{b'}) = (((m^a)^b)^{a'})^{b'}$, which becomes m after applying the Basic Principle.

- Some drawbacks to the Three-Pass protocol include being exceptionally vulnerable to man-in-the-middle attacks and requiring three times the traffic, significantly slowing down communications.