MATH 314 Spring 2018 - Class Notes

2/15/2018

Scribe: James Waugh

Summary: Perfect Secrecy, and working with Euclid's Algorithm and gcd's

Example of Perfect Secrecy:

- *Perfect Secrecy Recap:*

  For any message p and ciphertext c, P(a message sent p) = P(a message sent p | ciphertext is c)

- *Example: Eve's Attack on Alice and Bob*

  Suppose that Alice and Bob send "yes", "no", or "maybe", with frequencies:

  5/10 for "yes"

  3/10 for "no"

  2/10 for "maybe"

  They encrypt using three keys, where

	k1	k2	k3
"yes"	a	b	c
"no"	b	c	d
"maybe"	c	d	a

  Every day they pick one key at random with probability 1/3, and use that key to send their message for that day

  Suppose that Eve captures the ciphertext "c". Her goal is to find how likely the corresponding message is "yes"

  We know that P(message sent is "yes") = 1/2

  We know that P(today's key is k3) = 1/3

Eve computes:

P(message sent is "yes" | the ciphertext is "c") = P(message sent is "yes" and the message's ciphertext is "c") / P(the ciphertext is "c")

= ((1/2)(1/3)) / (P(the ciphertext is "c"))

=

$$\frac{(1/2)(1/3)}{(5/10) * (1/3) + (3/10)(1/3) + (2/10)(1/3)} = \frac{(1/6)}{(1/3)} = 1/2$$

Eve doesn't learn anything from the ciphertext through this computation

Now suppose Eve capture ciphertext "b" the next day

We know that P(message sent is "yes") = 1/2

P(message sent is "yes" | the ciphertext is "b") = P(message sent is "yes" and the message's ciphertext is "b") / P(the ciphertext is "b")

=

$$\frac{(1/2)(1/3)}{(5/10) * (1/3) + (3/10)(1/3)} = \frac{(1/6)}{4/15)} = 15/4 = 5/8$$

Because 5/8 does not equal 1/2, Eve has better than a half-chance that the message is "yes", and thus has a more accurate prediction. This answer shows that the cryptosystem does not have Perfect Secrecy

- *Theorem: The One-Time-Pad has Perfect Secrecy.*

  Disadvantages of the one-time-pad:

  1. Very long key that has to be shared
  2. Difficult to figure out what it looks like in a modern setting
  3. using a key one time only is cumbersome

Tools from Elementary Number Theory:

- *Euclid's Algorithm:*

  Compute greatest common divisors (gcd's)

  Example:

  $\gcd(6, 10) = 2$

  One method for computing gcd's is to factor both of the numbers and take the largest factor of both

  Euclid's Algorithm lets us compute gcd's without factoring the numbers

  Idea; Division With Remainder:

  There exists a remainder after division between two numbers, which is key to Euclid's Algorithm

  $$\frac{b}{a} = mRr$$

  Crafting the Algorithm:

  $a = mb + r$, where r is some number less than b, and a, b, m, r are integers

  $\gcd(a, b) = c$

  $\gcd(a, b) = \gcd(b, r)$

  Repeat this division with remainder until we get a remainder of 0. Then the gcgd is the remainder from the most previous step

Example:

$\gcd(79, 19)$

$$\frac{79}{19} = 4R3$$

$79 = 4 * 19 + 3$

$\gcd(79, 19) = \gcd(19, 3)$

$19 = 6 * 3 + 1$

$\gcd(19, 3) = \gcd(3, 1)$

$3 = 3 * 1 + 0$

Here, the algorithm stops, we have reached the remainder of 0. Therefore, we look at the most previous step and observe its remainder

The most previous step is $19 = 6 * 3 + 1$, and so the remainder is 1

1 is our gcd

$\gcd(79, 19) = \gcd(19, 3) = \gcd(3, 1) = 1$

Factoring Method:

Computes $\gcd(a, b)$ in $O(a + b)$ time

This is exponential time

Euclid's Algorithm computes in $O(\log a + \log b)$ time

- *Extended Euclid's Algorithm:*

  Computes inverses of numbers in modular arithmetic

  Theorem:

  If $\gcd(a, b) = c$, then there exists integers m, n such that $am + bn = c$

  Extending Euclid's Algorithm:

  First do Euclid's Algorithm forward to find the gcd

  Then use the division with remainder equations, solving them for the remainder

Example:

$1 = 1 * (19) - 6 * (3)$

For $\gcd(19, 3) = 1$, trying to find $\gcd(79, 19)$

$3 = 79 - 4 * (19)$

Now we substitute in the 3 from the equation above into the first equation

$1 = 1 * (19) - 6 * (79 - 4 * (19))$

$1 = 1 * (19) - 6 * (79) + 24 * (19)$

$1 = 25 * (19) - 6 * (79)$

Suppose we wanted

$19^{-1} \pmod{79}$

We use

$1 \equiv 25 * (19) \pmod{79}$

To find that

$19^{-1} \pmod{79} \equiv 25 \pmod{79}$

Way to Compute Inverses (mod m):

- *Finding* $a^{-1} \pmod{m}$

  Use the Extended Euclid's Algorithm to find the linear combination that equals 1

  The inverse is the thing multiplying a

- *Example: Compute* $7^{-1} \pmod{26}$

  $\gcd(7, 26)$

  $26 = 3 * (7) + 5$

  $\gcd(7, 5)$

  $7 = 1 * (5) + 2$

  $\gcd(5, 2)$

  $5 = 2 * (2) + 1$

  $\gcd(2, 1)$

  $2 = 1 * (2) + 0$

  The most previous step is $5 = 2 * (2) + 1$, and so the remainder is 1, 1 is our gcd

  Now we use Extended Euclid's Algorithm. We have the following:

  $1 = 5 - 2 * (2)$

  $2 = 7 - 1 * (5)$

  $5 = 26 - 3 * (7)$

  We substitute in the 2 from the equation $2 = 7 - 1 * (5)$ into the equation $1 = 5 - 2 * (2)$

  $1 = 5 - 2 * (7 - 1 * (5))$

  $1 = 3 * (5) - 2 * (7)$

  We substitute in the 5 from the equation $5 = 26 - 3 * (7)$ into the equation $1 = 3 * (5) - 2 * (7)$

  $1 = 3 * (26 - 3 * (7)) - 2 * (7)$

  $1 = 3 * (26) - 11 * (7)$

  Now we introduce (mod 26)

$$1 \equiv -11 * (7) \pmod{26}$$

$$7^{-1} = 15 \pmod{26}$$

  Which is the inverse we are trying to find