MATH 314 Fall 2019 - Class Notes

11/25/2019

Scribe: Tho Man

Summary: Continue with hash functions. Elliptic curves.

Hash functions (Cont.)

- Don't store pass words in plaintext on a server
- Use a has function (if someone accesses the password file reversing a hash to find a specific password is hard).
- Attack against a hashed password file:
  Take common passwords and hash them all
  Look for these digests among the list of passwords
- Solutions:
  Salt passwords by adding some random string to them before hashing
- Hash password combined with the random salt string.

Elliptic Curves

$(1 - \frac{1}{365})(1 - \frac{2}{365})...(1 - \frac{k+1}{365}) \approx e^{-\frac{k^2}{2(N)}}$

- An elliptic curve is an equation of the form

$\boxed{y^2 = x^3 + ax + b}$ **w**here $\underbrace{4a^3 + 27b^2}_{Discriminant} \neq 0$

- Always symmetric across the x-axis
- If we pick two points on elliptic curve and draw the line connecting them
  That line will always go through exactly one more third point
  Unless the line is vertical or is tangent to the elliptic curve
- This fact lets us define "arithnetic" on points of an elliptic curve
- Define P + Q to be the point obtained by drawing a line from P to Q, finding the thrid point on that line and then reflecting across the x-axis.

- Lets find this third point
  Suppose
  $P = (x_1, y_1)$
  $Q = (x_2, y_2)$
- Slope of this line is $m = \frac{y_2 - y_1}{x_2 - x_1}$
- $R = (x_3, y_3)$ is a point on the elliptic curve
  $y^2 = x^3 + ax + b$
  and
  y = mx + d

  $(mx + d)^2 = x^3 + ax + b$
  $m^2x^2 + 2dmx + d^2 = x^3 + ax + b$
  $0 = \underline{x^3 - m^2x^2 + (-2dm + a)x + b - d^2}$
  Since P,Q,R are all on both curves all 3 x-coordinates satisfy this equation.
  $(x - x_1)(x - x_2)(x - x_3)$
  $= \underline{x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_1x_3)x - (x_1x_2x_3)}$
- Equate x^2 terms
  $-m^2 = -(x_1 + x_2 + x_3)$
  $m^2 = x_1 + x_2 + x3$
  $\boxed{x_3 = m^2 - x_1 - x_2}$
  $y_3 = -(y_1 + m(x_3 - x_1))$
- Coordinates of P + Q are $(\bar{x_3}, \bar{y_3})$
  $\boxed{\begin{array}{l} \bar{x_3} = x_3 = m^2 - x_1 - x_2 \\ \bar{y_3} = m(x_1 - x_3) - y_1 \text{ (updated)} \end{array}}$
- Tangent lines:
  Add P + P
  line = tangent line at P

  Find slope of line using calculus
  $m = \frac{3{x_1}^2 + a}{2y_1}$

  $\boxed{\begin{array}{l} \bar{x_3} = m^2 - 2x_1 \\ \bar{y_3} = m(x_1 - x_3) - y_1 \text{ (updated)} \end{array}}$

  What is P + Q?
  If P and Q are opposites, we define P + Q = ∞

  what is P + ∞ = P
  ∞ is the identity element