MATH 314 Spring 2018 - Class Notes

10/14/2015

Scribe: Samuel Naranjo

Summary: This class covered the Digital Signature Algorithm (DSA). There was also an introduction to Elliptic Curves.

Notes: Alice wants to create a public key:

- 2 primes, p(200 digits), and q(50 digits) where $q \mid (p-1)$
- let g be a primitive root (mod p)
- let $\alpha = g^{(p-1)/q}$
- Note: $\alpha^q = (g^{(p-1)/q})^q \equiv 1(modp)$, alpha is not a primitive root. Alice picks a secret number q $\beta \equiv \alpha^q(modp)$.
- Thus, the public key is (p,q,α, β).

Suppose Alice wants to sign the message m. To sign the m, Alice picks a new random number k, where k is $2 \leq k < q-1$.

- $r = (\alpha^k(modp))(modq)$
- $s = k^{-1}(m+ar)(modq)$

She sends (m,(r,s)).

Bob receives (m,(r,s)) and wants to verify the signature. He computes

- $U_1 = s^{-1} \times m(modq)$
- $U_2 = s^{-1} \times r(modq)$
- He computes $V = (\alpha^{U_1} \times \beta^{U_2}(modp))(modq)$.

If $V \equiv R$ then Bob accepts the signature, else Bob rejects it.

Why should V=R?

1. $S = k^{-1}(m+ar)(modq)$
2. $kS = m + ar(modq)$
3. $k = s^{-1} \times m + (aS^{-1}r)(modq)$
4. $r = \alpha^k = \alpha^{U_1+a} \times U_2$

5. $\equiv \alpha^{U_1}(\alpha^a)^{U_2}$

6. $\equiv \alpha^{U_1} \times \beta^{U_2} \equiv (v(modp)(modq))$

Nifty Fact: Pick two points on an elliptic curve and draw the line between them. It always* intersects the curve at a third point.

- Define arithmetic of points on an elliptic curve to be i.
- Draw the line between points to get a third point (R), reflect this point across the x-axis.
- Suppose $p = (x_1, y_1) andq = (x_2, y_2)$ and we want to find the third point $r(X_3, y_3)$. Find the equation for the line y = mx + c
- Want to find (x_3, y_3) on both $y = mx + c$ and $y^2 = x^3 + ax + b$
- $(mx + c)^2 = x^3 + ax + b$
- $m^2 + x^2 + 2mc + c^2 = x^3 + ax + b$
- $0 = x^3 - m^2x^2 + (a - 2mc)x + (b - c^2)$
- $= (x - x_1)(x - x_2)(x - x_3)$