Cryptography notes

James Edwards

11/28/2023

Hash Functions, not on final
-take in very large inputs to produce smaller outputs
- whenever 2 inputs produce digests, its called collision properties
1. Hard to reverse hash digest
2. Weak collision, find message that hashes to predetermine digest
3. Strong collision resistance, you create 2 messages to collide

Hash messages signature and send along side it
Elliptic Curves
Elliptic Curves are a variation to do instead of discrete log
They are the points of x and y that satisfy an equation in the form:
$y^2 = x^3 + ax + b$
where a and b are ints and if you draw 2 points on an eliptic curve and draw a line between them, there will be a third point that intersects the curve and the line.

1 DSA- digital Signature Algorithm

q = medium sized prime number (80 digits)
p = large prime number (200 digits)
p is chose so that p -1 = ql, this means that p - 1 must be a multiple of q

Example.
q = 11, p = 67 = (6 x 11) + 1
More Info
g = primitive root (mod p)
$\alpha = g((p-1)/q) = g^l(modp)$
a = private exponent, must be $0 < a < p - 1$
$\beta = \alpha^a(modp)$
public key (p, q, α, β)

Signature Step (DSA)
Pick an ephemeral key $0 < k < p - 1$, and the gcd(k,p-1) =1
r = $(\alpha^k(modp)(modq))$
s = $(m + ar)k^{-1}(modq)$
(r,s) is the signature for message m so (m,(r,s)) is sent

Verification Step
Bob receives this message (m,(r,s)) and wants to check if it is valid
Bob computes:
$U1 = s^{-1}m(modq)$
$U2 = s^{-1}r(modq)$
$\alpha^{U1}\beta^{U2}(modp)(modq)$
This is valid if it equals r
Note, $k = s^{-1}(m + ar)(modq)$