MATH 314 Fall 2023 - Class Notes

11/21/2023

Scribe: Andrew Heller

Summary: Todays class covered Hash functions and began to dive into Digital signatures. Hash functions take in large inputs and output much smaller digests. Any time two different inputs result in the same output, it is called a **collision**. Cryptographic hash functions should ideally satisfy the following properties:

1. **Preimage resistance**: It should be hard to find a message with a given digest. That is, given $H(x) = y$, it should be hard to solve for x.
2. **Weak collision resistance**: For a fixed input x_1, it should be hard to find another input x_2 such that $H(x_1) = H(x_2)$.
3. **Strong collision resistance**: It should be hard to find any two inputs x_1 and x_2 such that $H(x_1) = H(x_2)$.

The RSA signature algorithm has the same setup as regular RSA. Alice creates a public key using prime numbers p and q, and a public exponent e. The public key is represented as (n, e) where $n = p \cdot q$. The private key d is calculated as $d = e^{-1} \mod \phi(n)$.

RSA Signature Function: The signature function s for a message m is defined as:

$$s(m) = m^d \mod n$$

Alice sends the pair (m, s) to Bob.

Upon receiving the message, Bob computes:

$$v = s^e \mod n$$

If $v = m \mod n$, then the signature is considered valid.