Cryptography Research

Dr. Hagedorn and Dr. Schmoyer

Cryptography is the art and science of keeping secrets.

Most modern cryptography is based on number theory and abstract algebra.

- RSA is based on Euler's Theorem:
  If $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \bmod n$$

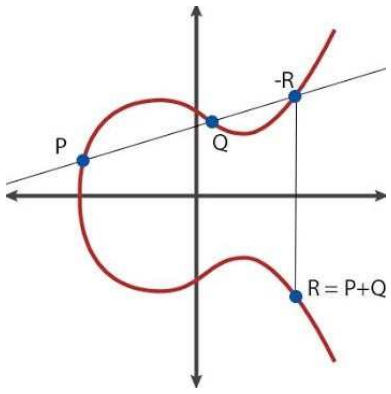
  where $\phi(n)$ is the number of integers $1 \leq b \leq n$ so that $\gcd(b, n) = 1$.

  In RSA, n is the product of two large prime numbers.

- Other modern cryptography systems are based on discrete logarithm problems in abelian groups.

  For example, suppose you know integers α and β and a prime number p, and you know that $\beta \equiv \alpha^x \bmod p$.
  Find x.

- Elliptic Curves and Hyperelliptic Curves have their own version of the discrete logarithm problem and are used in cryptography. They are the topic of a lot of current research.



- Every cryptosystem that is used incorrectly is vulnerable to attacks. Often, cryptography depends on choosing a number that is secret and random. Interesting questions arise when we wonder what happens if we make bad choices. For example,

  What if we choose bad prime numbers?
  What if we choose numbers that are secret, but not random?
  What if we encrypt or decrypt 'the wrong thing'?

- Many of our current cryptosystems will be broken by Quantum Computers.

  The future of cryptography is "Post Quantum". What will it look like?