Prime Numbers in Cryptology

Leon Bykov, Lisa Stelmarski, Daniel Arraj

Advisor: Dr. Luiz Felipe Martins

History

- One of the first encryption systems was the Caesar cipher.
- Example: shift each letter to the right by three spaces, so A→D
- Used for hundreds of years until it was discovered how to break the code by using frequency analysis.
- Most famous encryption system was the Enigma machine.
- Used in WWII by the Nazis to encrypt codes; seemed impossible to break and had a code that was changed often.

The Enigma.

Modern Encryption

- Asymmetrical processes
- Very dependent on primes and their behavior.
- Primes defy simple attempts at cracking. (How does a hacker find the “key”?)

Primes in Action: Key Exchange

- Alice and Bob pick a prime *p*—say, 13—and a *primitive root mod p*, *r*—say, 2. (A primitive root’s powers modulo *p* give all values from 1 to *p* – 1.)
- Alice picks a secret integer—say, 4—and computes 2^4 mod 13 (3). Bob picks a secret integer—say, 5—and computes 2^5 mod 17 (6). They exchange 3 and 6.
- Alice computes 6^4 mod 13 and Bob computes 3^5 mod 13—both 9.
- Alice and Bob got the same key without actually revealing it!
- Although not an encryption method per se, this does answer another question: how do we decide on keys without revealing them to eavesdroppers?

Why primes?

- Modular arithmetic modulo a prime is a *field*. Notably, if you multiply two nonzero numbers modulo a prime, you cannot get zero. This prevents data loss.
- Composites usually lack primitive roots.
- However, *factoring* products of two primes (which are also used) is very time-consuming.

Prime Factorization

- The RSA cryptosystem also uses products of two primes.
- Breaking RSA involves factoring this number, a very long process!
- Assuming a million operations per second, it would take a computer 4.9×10^{15} years to check all possible prime factors!
- Factorization is often used as a benchmark for computer performance.

Conclusion

- Cryptosystems have become ever more complicated, from Caesar shift to Enigma to public-key cryptography.
- Earlier ciphers were symmetric and had no “deep” mathematics. Today, ciphers depend on and special numbers and functions.
- This has led to greater interest in these numbers and functions. For example:
  - Can we easily factor large numbers?
  - Are there general patterns in primes?
  - Can we develop a quick test for primality that does not depend on factorization?