Irreducible Polynomials Over Finite Fields as Cryptographical Frameworks for Cybersecurity

Lee, Jiseop (School: BASIS San Antonio Shavano Campus)

This project investigated a cryptographic framework for cybersecurity utilizing a pair of a field-defining monic irreducible polynomial f(x) and an associated multiplier polynomial k(x) as a private key. Constructed over GF(p^n) for some prime p and degree n, the encryption algorithm involved multiplying a message polynomial by k(x) modulo f(x) and the decryption algorithm involved multiplying the ciphertext by the modular inverse of k(x) modulo f(x). Mathematical theorems on irreducible polynomials over finite fields were used to estimate the search space for brute-force attacks, the expected runtime of the decryption algorithm, and ensured that only the correct key recovered the original message. Mathematical analysis predicted a brute-force time complexity, charaterized as the relationship of the values p and n to the time spent to successfully brute force the cryptosystem: O(p^n n log^2(p)) when only the irreducible polynomial was unknown, and O(p^(2n) n log^2(p)) when both polynomials were secret. The cryptosystem and a brute-force method were implemented in Python. Assuming that k(x) was known, testing across various values of p and n confirmed that cracking times were consistent with the theoretical time complexity. To secure against linear/algebraic attacks, the study mathematically investigated the integration of a nonlinear substitution layer (S-box) and additional encryption layers. The findings demonstrated that the cryptosystem achieved secure brute-force complexity and provided a foundation for future development in nonlinear and layered cryptographic designs.

Awards Won: