Área: CIENCIAS EXATAS E DA TERRA

Projeto: CRIPTOGRAFIA E CURVAS ELÍPTICAS

Autores: MARCOS HENRIQUE SILVA ALMEIDA (XXII PIBIC/XXVI BIC/UFJF); ÍTALO ZANELLI DE MELO (XXII PIBIC/XXVI BIC/UFJF); BEATRIZ CASULARI DA MOTTA RIBEIRO (ORIENTADOR);

Resumo:

A criptografia moderna teve início com a necessidade de proteção de segredos de guerra. Porém, cada vez mais a proteção de informações é uma necessidade cotidiana. Assim, a procura por métodos cada vez mais seguros de troca de informação, tornou-se uma necessidade para a vida cotidiana.

Nesse sentido, foi criada a criptografia de chave pública. O método mais conhecido é a criptografia RSA, proposta em 1977 por Rivest, Shamir e Adleman (daí o nome). Para seu funcionamento, é necessário trabalhar com números primos da ordem de cem dígitos, que são multiplicados de forma a obter um número ainda maior. Esses números primos são chaves secretas (apenas o codificador os conhece) e o número obtido na multiplicação é a chave pública. A questão da segurança se baseia no fato de que ainda é muito caro computacionalmente fatorar grandes números em produto de primos. O problema que surgiu há pouco tempo foi: com o avanço rápido da computação, pode ser que, mesmo métodos de força bruta possam, com alguma rapidez, fatorar números e, assim, descobrir as chaves secretas a partir apenas da chave pública, em algum futuro mais ou menos próximo. Tornou-se necessário, então, o estudo de novos métodos cuja segurança não se baseie em fatoração em produto de primos.

Por volta de 1985, Koblitz e Miller (separadamente) propuseram a exploração de uma nova técnica de criptografia de chave pública baseada em uma teoria de curvas algébricas já bastante conhecia, a teoria de curvas elípticas. A ideia é, em vez de usar produto de números primos, usar operações com pontos de uma certa curva elíptica pré-determinada.

Nesse projeto, estudamos a base e a história da criptografia moderna, bem como os avanços da criptografia baseada em curvas. Assim, o bolsista Ítalo apresentará a base da criptografia RSA e o bolsista Marcos apresentará as técnicas e definições da teoria de curvas elípticas, que formam base para esse novo método de criptografia.