

# Re: Public Key, Symbolic Calculation

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/1493.html>

---

*tomstdenis\_at\_gmail.com*

**Date:** 02/08/05

Date: 8 Feb 2005 08:18:22 -0800

Kiuhnm wrote:

> *David Wagner wrote:*

> > *But even this is not precise enough. What field does the polynomial*

> > *lie in, and how is it specified? If you say that the polynomial lies*

> > *in C, we're back to trouble again, because you can't specify arbitrary*

> > *elements of C in finite length. Perhaps you meant that the polynomial*

> > *p has integral, or rational, coefficients? In that case the polynomial*

> > *can be specified in finite length using any standard encoding.*

>

> *The polynomial has "algebraic" coefficients, but I am afraid that if the*

> *"algebraic form" of the solution is known, the problem is simple.*

What does "algebraic coefficients" mean anyways? The coefficients of a polynomial must belong to a group, ring or field to be representable. I'm afraid I don't know what group "algebraic" is... [punk or ska?]

To put it another way. If I were to write a program to store/load your "algebraic polynomial" ... what format would it be reading/writing? More importantly how do you map raw binary messages [e.g. plaintext] to the "algebraic group"?

Tom