

# Questions about Shamir secret sharing

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-09/msg01005.html>

---

- *From:* "Dro Kulix" <[peter.s.may@xxxxxxxxx](mailto:peter.s.may@xxxxxxxxx)>
  - *Date:* 28 Sep 2006 09:15:43 -0700
- 

I've written a conceptual overview of a particular form of Shamir's polynomial scheme from "How to Share a Secret", but I have some questions regarding which liberties I can take and still get away with it. I've copied the introduction here; the full document is at <http://halfgeek.org/ss10001/ss10001.html> . If I've made any incorrect assumptions, or if you have any answers to my questions, please reply.

Thanks a zillion --- PSM

The intro:

ss10001 is an experiment in implementing secret sharing as proposed by Shamir[SHAMIR] by using 16-bit blocks of the secret to be shared and evaluating polynomials modulo 65537. The goal is to provide a speed-efficient (and hopefully, at some point, memory-efficient) implementation of the sharing scheme while providing a level of theoretical security at or near the number of bits of the secret itself.

This version of the document is a request for commentary by those better versed in cryptanalysis than I am, having ever had only two classes on the topic and no graduate study. I think I may be onto something useful, but I would not be so presumptuous as to consider it secure without first having it reviewed by expert eyes. I have written an encrypter and a decrypter for this scheme, both in C, but have not released either. The decrypter is suitable for solving shares generated from any of the modes described below; the encrypter is currently designed to run in OC mode. My intuition about the Shamir algorithm is not sufficient to tell me whether OC mode provides sufficient security, or whether the more conservative AC or the less intensive SR modes should be used instead.

This is not (yet) intended to be a formal paper; I'm really just trying to ask some questions.

.