

Re: two of three

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-01/2251.html>

From: Michael Brown (*see_at_signature_below*)

Date: 01/28/05

Date: Sat, 29 Jan 2005 02:05:11 +1100

Bob Harris wrote:

> *Suppose I have a value x (chosen from some range) and I want to*
> *encrypt it with three value a , b , and c (each from the same range as*
> *x) such that x can be recovered from any two of those values. In*
> *other words, we have functions f , g , and h such that $f(a,b) = g(b,c)$*
> *$= h(c,a) = x$.*

The term to look for is "secret splitting" A primitive approach in this case would be encrypt it with a single key, call it K , and let it be n bits long. Then, split K into 3 equal portions, called K_1 , K_2 , K_3 . K_1 is $n/3$ bits long, etc.

The first "metavalue" a contains K_1 and K_2 , b contains K_2 and K_3 , and c contains K_3 and K_1 . From any two of these values, the original key can be found. The downside to this approach is that you have dramatically reduced the brute-force key space if you have only one of the "metavalues", something which better methods avoid.

[...]

--

Michael Brown

www.emboss.co.nz : OOS/RSI software and more :)

Add michael@ to [emboss.co.nz](http://www.emboss.co.nz) ---+--- My inbox is always open