

# Re: triple algorithms

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2008-02/msg00926.html>

---

- *From:* "Antony Clements" <[antony.clements@xxxxxxxxxxx](mailto:antony.clements@xxxxxxxxxxx)>
  - *Date:* Wed, 27 Feb 2008 20:47:54 GMT
- 

the layer i wrote uses a passphrase which is used to generate a passcode equal to the length of m, i wont go into detail on how this passcode is produced because it's long and boring.

[http://en.wikipedia.org/wiki/Key\\_strengthening](http://en.wikipedia.org/wiki/Key_strengthening)

<http://www.google.com/search?q=key+strengthening+passphrase>

yes i know about key stretching, but that's the least significant part of the KDF that i mashed together.

essentially all i am doing for my KDF to produce  $l(\text{passcode}) == l(m)$ , where  $l(m)$  is always a multiple of 64

```
s = hex(random salt)
permutate s
salt = hex to decimal(s)
K' = sha512(passphrase & salt)
```

```
for i = 1 to n
if K' is unique
perumate K'
K= K & K'
sbox(salt)
K' = sha512(K' & salt)
else
s = hex(salt)
permutate s
salt = hex to decimal(s)
K' = sha512(K' & salt)
permutate K'
K = K & K'
fi
rof
```

Re: triple algorithms