struct sdesc {  
 struct shash\_desc shash;  
 char ctx[];  
};  
  
static struct sdesc init\_sdesc(struct crypto\_shash \*alg)  
{  
 struct sdesc sdesc;  
 int size;  
  
 size = sizeof(struct shash\_desc) + crypto\_shash\_descsize(alg);  
 sdesc = kmalloc(size, GFP\_KERNEL);  
 if (!sdesc)  
 return ERR\_PTR(-ENOMEM);  
 sdesc->shash.tfm = alg;  
 sdesc->shash.flags = 0x0;  
 return sdesc;  
}  
  
static int calc\_hash(struct crypto\_shashalg,  
 const unsigned chardata, unsigned int datalen,  
 unsigned chardigest) {  
 struct sdesc sdesc;  
 int ret;  
  
 sdesc = init\_sdesc(alg);  
 if (IS\_ERR(sdesc)) {  
 pr\_info("trusted\_key: can't alloc %s\n", hash\_alg);  
 return PTR\_ERR(sdesc);  
 }  
  
 ret = crypto\_shash\_digest(&sdesc->shash, data, datalen, digest);  
 kfree(sdesc);  
 return ret;  
}

<https://www.kernel.org/doc/html/v4.12/crypto/api-samples.html#code-example-for-symmetric-key-cipher-operation>