

KEYPHRENE ' S BLOG

Digest & HMAC

Digest

```
from org.keyphrene.crypto import Digest, HMAC
```

```
#####  
# SHA 1  
d = Digest("sha1")  
print "SHA1 Size: %d" % d.get_size()  
d.update("naja")  
print "SHA1: %s" % d.digest()
```

```
#####  
# MD5 1  
d = Digest("md5")  
print "MD5 Size: %d" % d.get_size()  
d.update("naja")  
print "MD5: %s" % d.digest()
```

List of Digests: sha, sha1, md5, md4, md2, mdc2, rmd160

HMAC

```
from org.keyphrene.crypto import Digest, HMAC
```

```
key = "a key"  
digestmod = "md5"  
hmac = HMAC(key, digestmod)  
hmac.update("your data")  
print hmac.final()
```

List of digestmod: md5, sha, sha1