Archivematica - Bug #1002

Replace md5 with sha

01/04/2011 12:00 AM - Evelyn McLellan

Status:	Verified	**Start date:**	
Priority:	High	**Due date:**	
Assignee:	Joseph Perry	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	Release 0.7		
Google Code Legacy ID:	archivematica-347	**Pull Request:**	
Sponsored:		**Requires documentation:**	

Description

More secure. Austin to research best sha. Also have to add script to check sha hash values.

[g] Legacy categories: Checksums

Related issues:

Duplicated by Archivematica - Bug # 912: Add checksum verification on ingest	**Duplicate**

History

#1 - 01/04/2011 12:00 AM - Austin Trask

did some testing with different versions of sha and compared it to md5sum one file which was 255K and the other with is 695M.. based on the tests I think sha256 should be adequate/speedy-enough.

$ ls -alh ubuntu-10.10-desktop-amd64.iso web-page-menu-01pizzas3.pdf
695M 2010-12-22 17:49 ubuntu-10.10-desktop-amd64.iso
255K 2010-12-28 17:35 web-page-menu-01pizzas3.pdf

$ time md5sum ubuntu-10.10-desktop-amd64.iso && time shasum ubuntu-10.10-desktop-amd64.iso && time sha224sum ubuntu-10.10-desktop-amd64.iso && time sha256sum ubuntu-10.10-desktop-amd64.iso && time sha512sum ubuntu-10.10-desktop-amd64.iso
1b9df87e588451d2ca4643a036020410 ubuntu-10.10-desktop-amd64.iso

real   0m2.895s
user   0m2.480s
sys   0m0.412s
ac7323b1f98d07583b59c2ace45e0e6102541467 ubuntu-10.10-desktop-amd64.iso

real   0m7.743s
user   0m7.400s
sys   0m0.340s
ea38ed73f0805c4e5a4d66dd8c532a61b640dd0c9c8097dadc799808 ubuntu-10.10-desktop-amd64.iso

real   0m11.100s
user   0m10.681s
sys   0m0.412s
3d720b4044c3f8baf14f706b09f012df82f269291b9f0ba0b3fc88e2bf07d0bd ubuntu-10.10-desktop-amd64.iso

real   0m11.110s
user   0m10.669s
sys   0m0.432s
e85db5d3384767f12505f1c6ad324428ec10fb26a4a5663d1dbd51af5c2c48a5f9ad7fecde9e6ca4ab880c7af01cf93f78db83e3135e1ac62d11ce6b519380f4 ubuntu-10.10-desktop-amd64.iso

real   1m0.086s
user   0m59.452s
sys   0m0.560s

$ time md5sum web-page-menu-01pizzas3.pdf && time shasum web-page-menu-01pizzas3.pdf && time sha224sum web-page-menu-01pizzas3.pdf && time sha256sum web-page-menu-01pizzas3.pdf && time sha512sum web-page-menu-01pizzas3.pdf
1400c15feca9e2de19e09a7ec21066a6 web-page-menu-01pizzas3.pdf

```
real    0m0.077s
user    0m0.000s
sys    0m0.004s
325ce8726f6a6327a521ca3f626fa8fb070f1c9e  web-page-menu-01pizzas3.pdf

real    0m0.054s
user    0m0.052s
sys    0m0.008s
bbf1027d49ee1d2d16698d5a02d4cf99d879ef2724b515126f4f2a03  web-page-menu-01pizzas3.pdf

real    0m0.006s
user    0m0.008s
sys    0m0.000s
3efda9ce2b32760229d8fd62709c02aa930b6f05f58a8d3030afee32f47f9998  web-page-menu-01pizzas3.pdf

real    0m0.006s
user    0m0.008s
sys    0m0.000s
9adb7f7a74c372292d8f7e826fffbaba0198af23524605c8e05aee80fe08be01ddf7eb4ba0cba687df10a4780bc2537721ec584076d6d30c8884466b3b9a
8b18  web-page-menu-01pizzas3.pdf

real    0m0.024s
user    0m0.020s
sys    0m0.004s
```

#3 - 01/04/2011 12:00 AM - Joseph Perry

Looking at doing this in python, as was done with MD5.
The python module sha module is replaced by hashlib.
http://docs.python.org/library/hashlib.html
Looks like it will do.

#4 - 01/05/2011 12:00 AM - Austin Trask

[g] New owner: Joseph Perry

#5 - 01/11/2011 12:00 AM - Joseph Perry

- Status changed from New to Verified

Committed r975.