

MIHALYA project

Encrypted Data Searching Tool

Encryption

- Uses AES 256 encryption;
- Perl + modules `Crypto::OpenSSL::AES` and `Data::Dump`;
- Javascript AES implementation;
- Generates encrypted index and encrypted data
- Example:


```
#perl mihalya.pl "user" "pass" MySourceDir MyOutputDir
```

(encrypts all the files in MySourceDir with user and pass and outputs index and data to MyOutputDir)

Local vs Server

Two versions:

Local: output data in the localstorage of the browser (sqlite) and Server: output in raw files



SELECT * FROM webappsstore2		
scope	key	value
tsohlacol.:http:6670	EDza30zILDdLIPGcyJVzAC...	kivKk6xrTSVfVr7zUHCXfq...
tsohlacol.:http:6670	EDza30zILDcWw6bNndJ6C...	cxS12cu3thkxtEWpKcjAbH...
tsohlacol.:http:6670	EDza30zILDdXguKH2ZV8C...	87QmXnRUsnds
tsohlacol.:http:6670	EDza30zILDcVxKfDmNjm...	jsXRw3mWEjZwbEu9HL8bz...
tsohlacol.:http:6670	EDza30zILDdGrvaSxjlkCzU...	Ao7Lwh42xabxc9b/H/jfh...
tsohlacol.:http:6670	EDza30zILDdBNPSa3o5zCy...	7tEcFvzHjWnBWQ==
tsohlacol.:http:6670	EDza30zILDcWw6TFksk8G...	sxWAa/Q1UlfEh35isjhyz9...
tsohlacol.:http:6670	EDza30zILDcRyqPCmtj7CD...	7joKNJa5JYtOEScWRg==
tsohlacol.:http:6670	EDza30zILDdXh+eFx5V3H...	iTRwsgUU0L0+lw5S77fLpB...
tsohlacol.:http:6670	EDza30zILDcWw6PenMw8...	9D3wZBYZvgA95MHyDNw...
tsohlacol.:http:6670	EDza30zILDdGgPKUz9jxAz...	sTib3JeLcZBW
tsohlacol.:http:6670	EDza30zILDcYqbdmtj2D...	wS0sr9GKRu8VrVp8QGm...
tsohlacol.:http:6670	EDza30zILDcQx6PCmtjxAz...	hQtGW/nCT/Fr
tsohlacol.:http:6670	EDza30zILDdSk+Sc3tjxAz...	N0AhJEtCK1PO



file4d526f55434c735073426b2f4a4a5363486d377164673d3d.txt
file4d526f55434c735073426b2f4a4a5363486d546865344373.txt
file4d526f55434c735073426b2f4a5a2b4b486d377164673d3d.txt
file4d526f55434c735073426b2f4a5a2b4b486d546865344373.txt
file4d526f55434c735073426b2f4a5a2b4c57577272494965385a673d3d.txt
file4d526f55434c735073426b2f4a5a2b4c5747376761634378656a4d3d.txt
file4d526f55434c735073426b2f4a5a2b4c575772724949323361795546.txt
file4d526f55434c735073426b2f4a5a2b4c57473767616343376354346662673d3d.txt
file4d526f55434c735073426b2f4a5a2b51586d4b675a347167.txt
file4d526f55434c735073426b2f4a5a2b51586d4b67625947746344383d.txt
file4d526f55434c735073426b2f4a5a2b4957474c3861384378656a4d3d.txt
file4d526f55434c735073426b2f4a5a2b4957474c38613843376354346662673d3d.txt
file4d526f55434c735073426b2f4a5a2b49555836675a347167.txt
file4d526f55434c735073426b2f4a5a2b5358335872494965385a673d3d.txt
file4d526f55434c735073426b2f4a5a2b6458325033494965385a673d3d.txt
file4d526f55434c735073426b2f4a5a2b4955583667625947746344383d.txt
file4d526f55434c735073426b2f4a5a2b53583358724949323361795546.txt
file4d526f55434c735073426b2f4a5a2b64583250334949323361795546.txt
file4d526f55434c735073426b2f4a5a2f5255326a37594a6f3d.txt
file4d526f55434c735073426b2f4a5a2f5257575032.txt
file4d526f55434c735073426b2f4a5a4b51586d6a34494965385a673d3d.txt

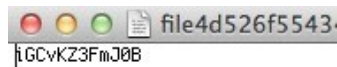
Client side

- Full webapp embedded in index.html;
- Local input of user and pass. They never travel through the Net unencrypted even without https;
- No data is travelling and stored without encryption;
- Search words are encrypted and the browser tries to retrieve the corresponding index files/localstorage;
- If index file is found, it is decrypted in RAM. Index contains only pointers to the files with data;
- Pointers are encrypted and there is a lookup for the corresponding data files;
- Files are decrypted one at a time in RAM;
- In the server version index and data are cached in localstorage in encrypted form, which speeds up and obfuscates the way it works;
- Works with tablets, iOS, Android.

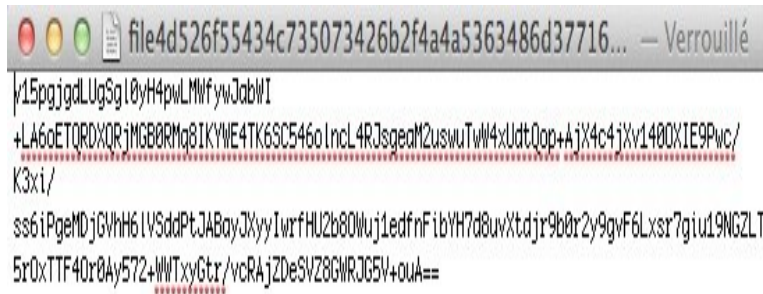
Search process

SEARCH

Search:



63279 + salt
100931
Etc.



Index

```
file4d526f55434cf35073426b2f4a4a5363486d3771f64673d3d.txt
file4d526f55434cf35073426b2f4a4a5363486d546865344373.txt
file4d526f55434cf35073426b2f4a5a2b4b486d3771f64673d3d.txt
file4d526f55434cf35073426b2f4a5a2b4b486d546865344373.txt
file4d526f55434cf35073426b2f4a5a2b4c5757727249496538a673d3d.txt
file4d526f55434cf35073426b2f4a5a2b4c574737676163437856a673d3d.txt
file4d526f55434cf35073426b2f4a5a2b4c575772724949323361795546.txt
file4d526f55434cf35073426b2f4a5a2b4c574737676163437856a673d3d.txt
file4d526f55434cf35073426b2f4a5a2b51586d4b67625947746344383d.txt
file4d526f55434cf35073426b2f4a5a2b51586d4b67625947746344383d.txt
file4d526f55434cf35073426b2f4a5a2b495747443861384378656a73d3d.txt
file4d526f55434cf35073426b2f4a5a2b495747443861384378656a73d3d.txt
file4d526f55434cf35073426b2f4a5a2b4955836675a37167.txt
file4d526f55434cf35073426b2f4a5a2b5358357249496538a673d3d.txt
file4d526f55434cf35073426b2f4a5a2b645832503449496538a673d3d.txt
file4d526f55434cf35073426b2f4a5a2b4955583667625947746344383d.txt
file4d526f55434cf35073426b2f4a5a2b535835724949323361795546.txt
file4d526f55434cf35073426b2f4a5a2b64583250344949323361795546.txt
file4d526f55434cf35073426b2f4a5a2f255326a37594a6f3d.txt
file4d526f55434cf35073426b2f4a5a2f2575032.txt
file4d526f55434cf35073426b2f4a5a4b51586d4b449496538a673d3d.txt
```

Data

```
file4d526f55434c735073426b2f4a5a4b5752474c38664947716f
file4d526f55434c735073426b2f4a5a4b5752474c38664947716f
file4d526f55434c735073426b2f4a5a4b5752474c38664947716f
file4d526f55434c735073426b2f4a5a4b5752474c38664947716f
file4d526f55434c735073426b2f4a5a4b5755326a38664a756f61
file4d526f55434c735073426b2f4a5a4b5755326a38664a756f61
file4d526f55434c735073426b2f4a5a4b5755332a76494965385f
file4d526f55434c735073426b2f4a5a4b5755633476494932336f
file4d526f55434c735073426b2f4a5a4b5756476a36613843786f
file4d526f55434c735073426b2f4a5a4b5756476a36613843376f
file4d526f55434c735073426b2f4a5a4b5757474c695a3432336f
file4d526f55434c735073426b2f4a5a4b5757474c695a3432336f
file4d526f55434c735073426b2f4a5a4b5758326e72494965385f
file4d526f55434c735073426b2f4a5a4b5758326e72494932336f
```

Data process

file4d526f55434c735073426b2f4a4a5363486d37716... — Verrouillé

y15pgjgdLgSgl0yH4pwLMWfywJabWI
+LA6oETQORDXQR1MGB0RMq8IKYWE4TK6SC546oIncL4R3sgeaM2uswuTw4xUdtQop+A;X4c4jXv1400XIE9Pwc/
K3xi/
ss6iPgeMDjGVhH6lV5ddPtJABayJXyyIwrfHU2b80Wuj1edfnFibYH7d8uvXtdjr9b0r2y9gvF6Lxsr7giu19NGZLT
5r0xTTF40r0Ay572+WWTxGtr/vcRAjZDeSVZ8GWRJG5V+ouA==



1 REFID: 06SOFIA647 DATE: 5/9/2006 10:04 ORIGIN: Embassy Sofia CLASS: SECRET//NOFORN DEST:
SUBJECT: BULGARIA'S MOST POPULAR POLITICIAN: GREAT HOPES, MURKY TIES
[Edit](#) :: [US justice assistance](#) ::

id: 63279
date: 5/9/2006 10:04
refid: 06SOFIA647
origin: Embassy Sofia
classification: SECRET//NOFORN
destination:
header:
Tim W Hayes 02/11/2009 11:09:57 AM From DB/Inbox: Search Results

Cable
Text:

S E C R E T NOFORN SOFIA 00647
CXsofia:
ACTION: POLEC
INFO: AID DCM FAS FCS DAO PAO AMB POLM RSO

Cache

Localstorage

SELECT * FROM webappsstore2

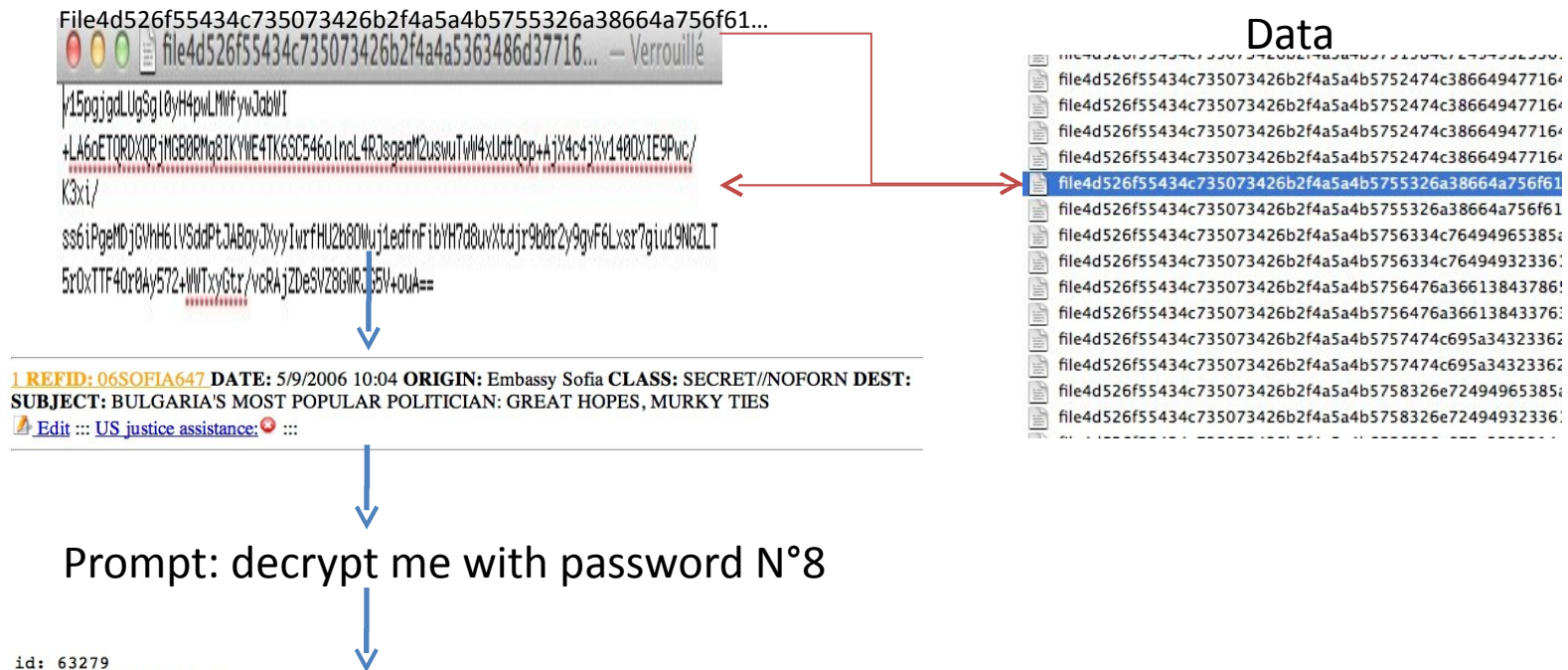
scope	key	value
tsohlacol.:http:6670	EDza30zILDdLIPGcylVzAC...	kiwKk6xrTSVfV7zUHCXf...
tsohlacol.:http:6670	EDza30zILDcWw6bNndj6C...	cxS12cu3thkxtBWpKcjAbH...
tsohlacol.:http:6670	EDza30zILDcXguK4Z2V8C...	87QmXnRUsnds
tsohlacol.:http:6670	EDza30zILDcVxkfdmNjm...	jsXRw3mWEJzwbEu9HL8bz...
tsohlacol.:http:6670	EDza30zILDdGnvaSxllkCzU...	Ao7Lwh42xabxc9b/H/jfh...
tsohlacol.:http:6670	EDza30zILDdBNpSa3o5zCy...	7tEcFvzHjWnBWQ==
tsohlacol.:http:6670	EDza30zILDcWw6TFksk8G...	sxWAA/Q1UfcEh35isjhyz9...
tsohlacol.:http:6670	EDza30zILDcRyqPCmtj7CD...	7joKNJa5jYtOEScWRg==
tsohlacol.:http:6670	EDza30zILDcXh+eFv5V3H...	iTRwsgUU0L0+kv5S77flpB...
tsohlacol.:http:6670	EDza30zILDcWw6PEmMw8...	9D3wZBYZvgA95MHYDNw...
tsohlacol.:http:6670	EDza30zILDcGgPKUz9jxAz...	sTib3JeLcZBW
tsohlacol.:http:6670	EDza30zILDcXyqbDmtj2D...	wS0sr9GKRu8VrP8QGM...
tsohlacol.:http:6670	EDza30zILDcQx6PCmtjxAz...	hQtGW/ncT/Fr
tsohlacol.:http:6670	EDza30zILDdSk+Sc3tjxAz...	N0AhEjCK1PO

Redacted version

Display & Edit

Ongoing: a more secure version

Data is encrypted with a random password from a list of 20 passwords



id: 63279
date: 5/9/2006 10:04
refid: 06SOFIA647
origin: Embassy Sofia
classification: SECRET//NOFORN
destination:
header:
Tim W Hayes 02/11/2009 11:09:57 AM From DB/Inbox: Search Results

Cable
Text:

S E C R E T NOFORN SOFIA 00647
CXsofia:
ACTION: POLEC
INFO: AID DCM FAS FCS DAO PAQ AMB POLM RSO