AdiIRC - Bug #2258

Decryption fails with $decrypt

10/16/2015 08:21 PM - jon chris

Status:	Closed	**Start date:**	10/16/2015
Priority:	Normal	**Due date:**	
Assignee:	Per Amundsen	**% Done:**	0%
Category:	Scripting	**Estimated time:**	0.00 hour
Target version:	3.3		
Operative System:	Windows 10	**Regression:**	No

Description

When I run this on the betabuild portable 32 and 64bit
var %text $encrypt(Hello World, test)
echo -ag $decrypt(%text, test)
I get this :
0f ~ò.trD

before I found $encrypt and $decrypt I was using the blowfish fork.
And I have gotten similar issues with cbc decryption there too.

History

#1 - 10/17/2015 02:25 AM - Per Amundsen

Thanks this is fixed for next beta.

The blowfish dll is not related to this, I will try update it from upstream.

#2 - 10/17/2015 02:25 AM - Per Amundsen

- Status changed from New to Resolved

#3 - 10/17/2015 06:26 AM - Per Amundsen

mirc fish is updated now, using next AdiIRC beta, encoding should be more reliable.

https://dev.adiirc.com/projects/adiirc/wiki/Blowfish

#4 - 10/18/2015 03:25 AM - jon chris

Per Amundsen wrote:

> mirc fish is updated now, using next AdiIRC beta, encoding should be more reliable.
>
> https://dev.adiirc.com/projects/adiirc/wiki/Blowfish

Thanks for the quickfix, btw does $encrypt use cbc mode?

#5 - 10/18/2015 04:56 AM - Per Amundsen

No it uses EBC.

#6 - 12/03/2018 03:54 AM - Per Amundsen

- Status changed from Resolved to Closed

- Target version changed from 1.9.9 to 3.3

Was keeping this open in case I figured out how to do CBC, but I just learned even ECB is not working properly so $encrypt is gonna be disabled in 3.3, consider using the blowfish plugin instead https://dev.adiirc.com/projects/adiirc/wiki/Blowfish, it also supports CBC.