



Blizzhackers

Home of the Dupe since 2001

[Login](#) [Register](#) [FAQ](#) [Search](#)

Join us on IRC: #bh@irc.synirc.net (or Mibbit Web IRC)

It is currently Sat Jun 23, 2018 1:01 pm

[View unanswered posts](#) | [View active topics](#)

[Board index](#) » [Diablo II](#) » [Diablo II Hacking Development](#)

All times are UTC [[DST](#)]


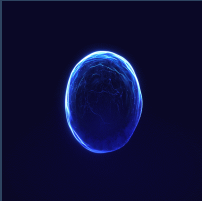
Trying to predict IDs in game. How do you convert...

Moderator: [Diablo Mods](#)

[newtopic](#) [postreply](#) Page 1 of 1 [11 posts]

[Print view](#)

[Previous topic](#) | [Next topic](#)

Author	Message
kleinerhuso2000	Post subject: Trying to predict IDs in game. How do you convert... Posted: Fri Mar 02, 2018 12:08 am
<div>User   Joined: Mon Aug 21, 2017 9:27 am Location: Frankfurt</div>	<p>There are several reasons why I asked myself how you could predict an ID in game. Mainly because an item might be somewhere where it's not possible to read its ID. In these cases, it might be very helpful if you knew what the item ID (or object ID or whatever) will be if the item is there. I know, sometimes something is not generated (for example an object in another Act when nobody is in this Act) which means that there is no way to make use of the ID because there is no such ID.</p> <p>But let's look at simple cases. We trade another player and we reset trade - our item IDs change. But before the trade resets, I like to know what ID my item will have when the trade resets which should be very possible.</p> <p>We have a DWORD in hexadecimal. Let's say we have the DWORD: 3c b0 1f 43 How do you convert this correctly into a decimal? There are different formats and I don't know which one is used in D2. Do we have that 3c b0 1f 43 in decimal is 1018175299 ?</p>

I need decimals because it will be easier for me to find the pattern which is used.
After that I like to try if there are different patterns for different cases (as example, if you reset trade, sell an item to NPC, gear your merc with an item, die, drop an item somewhere and let it update,...).

Top



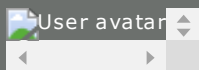
noah~

Post subject: Re: Trying to predict IDs in game. How do you convert...**Posted:** Fri Mar 02, 2018 2:07 am

D2BS Dev



Mod

**Joined:** Sun Jun 22, 2008
7:00 pm

If you are looking for a pattern, does it matter as long as you are doing the conversion consistently?

For example if this is byte addressable little endian memory you can interpret it as 0x431fb03c (1126150204)
if it is byte addressable big endian, 0x3cb01f43
nibble addressable little endian 0x34f10bc3
etc

either way, if you are looking for a 'pattern' the bit/nibble/byte/word ordering probably won't make much of a difference as long as you apply it consistently
you can try your 'pattern' at any arbitrary start point (for example if you thought either the lsb or msb was a parity bit or something idk)

However, if you want to confirm how it is interpreted, you can look at the id based on contents of the packet vs what the game returns as an id when you call the game lib function, it is likely byte addressable little endian.

NipCheck -- An offline .nip checker

PhotoGrid Sharp -- An image collage maker with formatting features

d2bot# with kolbot -- For live support: <irc://irc.synirc.net/d2bs>

Top



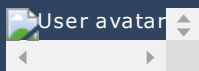
dzik

Post subject: Re: Trying to predict IDs in game. How do you convert...**Posted:** Fri Mar 02, 2018 6:22 am

User



User

**Joined:** Tue Jul 20, 2004
7:44 pm
Location: this.location

You can always collect item ids before and after trade for like couple hours of trading and see if there is any pattern in it.
As far as i know there is even algorithm used in machine learning to solve such problems.
Neural Network seems to be good option to solve such problem.

You can feed then all data into this algo and maybe you get some results. More test data you get more precise results will be.

Maybe something interesting:

D2Bot - CDKeyMaker.js by kolton

Top

 profile

Vampirewolve

Post subject: Re: Trying to predict IDs in game. How do you convert...

Posted: Fri Mar 02, 2018 9:24 am

User

Joined: Tue Mar 01, 2005
8:31 pm

Conversion depends on the used endianness.

Even when could correctly predict or already know item IDs you need to have access to them.



Top

 profile

catvir

Post subject: Re: Trying to predict IDs in game. How do you convert...

Posted: Fri Mar 02, 2018 3:04 pm

User

Joined: Thu Jul 17, 2003
12:23 pmBattle.net D2 servers use a very simple LFSR (https://en.wikipedia.org/wiki/Linear-feedback_shift_register).

Code: Select all

```
(id) -> (id >> 1) ^ (-(id & 1) & 0x90000000) ^ (-(id >> 15) & 1) & 0x0006000)
```

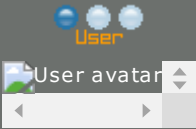

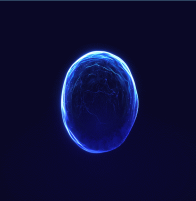
You can also easily generate previous ID with this formula:

Code: Select all

```
(id) -> (id << 1) ^ (-(id >> 13) & 1) & 0x000C000) ^ (-(id >> 31) & 0x20000001)
```

Top

 profile

<p>dzik</p> <p>User</p>  <p>Joined: Tue Jul 20, 2004 7:44 pm Location: this.location</p>	<p>Post subject: Re: Trying to predict IDs in game. How do you convert... Posted: Fri Mar 02, 2018 5:45 pm</p> <p>catvir » 2018.03.02 14:04:25 wrote:</p> <p>Battle.net D2 servers use a very simple LFSR (https://en.wikipedia.org/wiki/Linear-feedback_shift_register).</p> <div>Code: Select all <pre>(id) -> (id >> 1) ^ (-(id & 1) & 0x90000000) ^ (-(id >> 15) & 1) & 0x0006000)</pre></div> <p>You can also easily generate previous ID with this formula:</p> <div>Code: Select all <pre>(id) -> (id << 1) ^ (-(id >> 13) & 1) & 0x0000C000) ^ (-(id >> 31) & 0x20000001)</pre></div> <p>Thanks for sharing this formula.</p> <p>Maybe something interesting: D2Bot - CDKeyMaker.js by kolton</p>
<p>Top</p>	<p> profile</p>
<p>kleinerhuso2000</p> <p>User</p>  <p>Joined: Mon Aug 21, 2017</p>	<p>Post subject: Re: Trying to predict IDs in game. How do you convert... Posted: Fri Mar 02, 2018 10:55 pm</p> <p>catvir » Fri Mar 02, 2018 2:04 pm wrote:</p> <p>Battle.net D2 servers use a very simple LFSR (https://en.wikipedia.org/wiki/Linear-feedback_shift_register).</p> <div>Code: Select all <pre>(id) -> (id >> 1) ^ (-(id & 1) & 0x90000000) ^ (-(id >> 15) & 1) & 0x0006000)</pre></div> <p>You can also easily generate previous ID with this formula:</p> <div>Code: Select all</div>

9:27 am
Location: Frankfurt

```
(id) -> (id << 1) ^ (-((id >> 13) & 1) & 0x0000C000) ^ (- (id >> 31) & 0x20000001)
```

Thank you very much for posting the formula and the article which was very nice to read!
There were many good things mentioned but the most interesting one for me (regarding D2) was that LFSR include the generation of pseudo-random numbers and sequences, too.
From the formula you have posted, we can clearly see that this is the case (a PRNG is used for generating IDs and we now know its state).
Now it would be interesting to know where else those PRNGs are used in this game and what their state is.
After all the information posted in this topic, I wouldn't be too much surprised if they were also used to generate an items stats.
In plain terms, one should also be able to predict an items stats and it seems to be most efficient to use it on the imbue quest.
In theory, it should also be possible to use it on chests which sounds pretty much like chest-hack. Plainly and simply said, the main difference is
that you reset the items stats instead of resetting the objects state.

It sounds very possible and I can only hope that Blizzard fixed this already.

Top

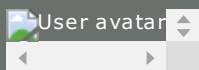
 [profile](#)

Muted

Post subject: Re: Trying to predict IDs in game. How do you convert...

Posted: Sat Mar 03, 2018 2:52 am

Banned



Joined: Sat Sep 06, 2008
7:18 am
Location: USA, TX

kleinerhuso2000 » Fri Mar 02, 2018 4:55 pm wrote:

catvir » Fri Mar 02, 2018 2:04 pm wrote:

Battle.net D2 servers use a very simple LFSR (https://en.wikipedia.org/wiki/Linear-feedback_shift_register).

Code: Select all

```
(id) -> (id >> 1) ^ (- (id & 1) & 0x90000000) ^ (-((id >> 15) & 1) & 0x00006000)
```

You can also easily generate previous ID with this formula:

Code: Select all

```
(id) -> (id << 1) ^ (-((id >> 13) & 1) & 0x0000C000) ^ (- (id >> 31) & 0x20000001)
```

Thank you very much for posting the formula and the article which was very nice to read!
There were many good things mentioned but the most interesting one for me (regarding D2) was that LFSR include the generation of pseudo-random numbers and sequences, too.

From the formula you have posted, we can clearly see that this is the case (a PRNG is used for generating IDs and we now know its state).

Now it would be interesting to know where else those PRNGs are used in this game and what their state is.

After all the information posted in this topic, I wouldn't be too much surprised if they were also used to generate an items stats.

In plain terms, one should also be able to predict an items stats and it seems to be most efficient to use it on the imbue quest.

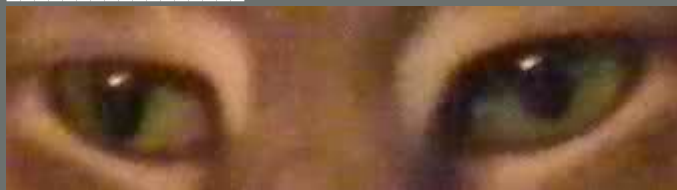
In theory, it should also be possible to use it on chests which sounds pretty much like chest-hack. Plainly and simply said, the main difference is that you reset the items stats instead of resetting the objects state.

It sounds very possible and I can only hope that Blizzard fixed this already.

In theory... If this 'pre-determined' random number generator were used in item generation... You are shooting at the floor.

If you could 'predict' what every monster in every nook and cranny of the game would drop: You'd immediately know if the game was worth staying in or not (changes based on players in game (affecting mLvl)). You would also automatically know **exactly** which monsters to kill and **where** to kill them.

I doubt it works like that (especially seeing how the model on Diablo was constructed in 1996).

[Top](#)[profile](#)**chrissybhoy****Post subject:** Re: Trying to predict IDs in game. How do you convert...**Posted:** Sat Mar 03, 2018 3:38 am

User

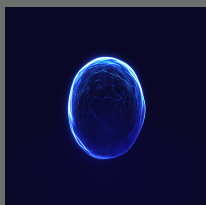


Would be epic tho.

Wishful thinkin here lol

Joined: Sat Jan 29, 2011
4:45 pm[Top](#)[profile](#)**kleinerhuso2000****Post subject:** Re: Trying to predict IDs in game. How do you convert...**Posted:** Sat Mar 03, 2018 11:29 am

User



Joined: Mon Aug 21, 2017
9:27 am
Location: Frankfurt

Muted » Sat Mar 03, 2018 1:52 am wrote:

If you could 'predict' what every monster in every nook and cranny of the game would drop: You'd immediately know if the game was worth staying in or not (changes based on players in game (affecting mLvl)). You would also automatically know **exactly** which monsters to kill and **where** to kill them.

I doubt it works like that (especially seeing how the model on Diablo was constructed in 1996).

Are you consciously trying to make it all look more complicated?

There is absolutely no need to do one thing on thousands of other things simultaneously and all at once.

As it was possible to predict item IDs, it should also be possible to predict item stats and I would start my research at some simple Quest such as Charsi's Imbue Quest where you exactly have one source and one destination.

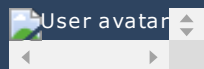
Unlike your seemingly dramatic description with thousands of complicated sources and corresponding other thousands of destinations. (Anyway, keep in mind that I assume this has worked but doesn't anymore. I will try to figure out how it worked though and when it might got fixed.)

I recommend others to ignore his post(s).

Last edited by kleinerhuso2000 on Sat Mar 03, 2018 11:56 am, edited 1 time in total.

[Top](#)[profile](#)**catvir****Post subject:** Re: Trying to predict IDs in game. How do you convert...**Posted:** Sat Mar 03, 2018 11:41 am

User



Joined: Thu Jul 17, 2003
12:23 pm

For random numbers D2 uses https://en.wikipedia.org/wiki/Lehmer_random_number_generator with $g = 0x6AC690C5$, $n = g * 2^{32} - 1$.
Unluckily, Battle.Net games differ in how they toss items.

[Top](#)[profile](#)

Display posts from previous: All posts ▼ Sort by Post time ▼ Ascending ▼ Go

[newtopic](#)[postreply](#)**Page 1 of 1** [11 posts][Board index](#) » [Diablo II](#) » [Diablo II Hacking Development](#)

All times are UTC [DST]

Who is online

Users browsing this forum: No registered users and 1 guest

You **cannot** post new topics in this forum
You **cannot** reply to topics in this forum
You **cannot** edit your posts in this forum
You **cannot** delete your posts in this forum

Search for: Jump to: 